HUAWEI

Huawei Certification

Ricardo Morschbacher

has successfully completed the Huawei certification requirements and is recognized as a

HCIA-Storage

Issue Date Feb 28, 2019

Validate this certificate's authenticity at
http://support.huawei.com/learning/verifycertificate
Certificate No. 02010090111380762317140 9

CEO
Huawei Technologies Co., Ltd.

HUAWEI

Huawei Certification

Ricardo Morschbacher

has successfully completed the Huawei certification requirements and is recognized as a

HCIE-Storage

HUAWEI Systems Instructor

Issue Date Mar 12, 2021

Validate this certificate's authenticity at
https://e.huawei.com/cn/talent/#/cert/certificate-verification
Certificate No. 02030090111380842653140 9

CEO
Huawei Technologies Co., Ltd.

HUAWEI

Huawei Certification

Joao Marcos Leite

has successfully completed the Huawei certification requirements and is recognized as a

HCIP-Storage

Issue Date Mar 06, 2020

Validate this certificate's authenticity at
http://support.huawei.com/learning/verifycertificate
Certificate No. 02020090111380802629140 9

CEO
Huawei Technologies Co., Ltd.

São Paulo, 18 de novembro de 2022

À
COMPWIRE INFORMÁTICA LTDA
Ref.:
PREGÃO ELETRÔNICO Nº 011/2022 – LOTE 2 PRODERJ (Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro)
PROCESSO Nº SEI-150016/000460/2021 (“Licitação”)

DECLARAÇÃO

Em referência à Licitação, a **HUAWEI DO BRASIL TELECOMUNICAÇÕES LTDA.**, doravante denominada “Huawei”, uma empresa registrada sob as leis da República Federativa do Brasil, inscrita no CNPJ/ME sob o nº **02.975.504/0001-52**, com sede na Rua Arquiteto Olavo Redig de Campos, 105, conjuntos 211, 212, 221, 222, 231, 232, 241 e 242, Edifício EZ Towers, Vila São Francisco, CEP 04711-904, Cidade e Estado de São Paulo, como fabricante de hardware e software, declara que a empresa **COMPWIRE INFORMÁTICA LTDA.**, doravante denominada “Compwire” inscrita no CNPJ nº: **01.181.242/0007-87**, localizada na Avenida Nossa Senhora de Copacabana, 599, Sala 604, Copacabana, Rio de Janeiro/RJ, é uma revenda autorizada e está apta a comercializar os produtos e serviços marca Huawei ofertados no âmbito da Licitação.

Adicionalmente, a Huawei declara que:

- Os equipamentos e os softwares ofertados serão suportados, pela garantia e o serviço de assistência técnica Huawei, durante toda a vigência do contrato.
- Todos os equipamentos ou componentes a serem fornecidos serão novos, e estarão em linha de produção e fabricação, e serão fornecidos com a embalagem original de fábrica e lacrada. O equipamento está na linha de produção atual do fabricante, e não consta na lista de “end-of-sale" e “end-of-life".
- Permite a expansão de desempenho e capacidade através da interconexão com outros appliances do mesmo tipo e fabricante, aumentando o conjunto de armazenamento total de backup e mantendo a desduplicação global;
- Suporta o protocolo NDMP, tanto em redes SAN quanto LAN;
- Possui funcionalidade de automatização ("scripting") de ações.
- Suporta a implementação das funções de agregação de portas (trunking) e VLAN, conforme padrões IEEE 802.3ad e IEEE 802.1Q e suporte a Jumbo Frames nas interfaces Ethernet.
- Suporta o envio automático de alertas/notificações (e-mails e outros) em caso de falhas, provendo, inclusive, o ajuste de níveis de alerta do crescimento de volumes;
- Permite monitoramento através de SNMP versão 2 e/ou 3, com função de TRAP e POOL, possibilitando que sistema de monitoramento SNMP externo consiga consultar o status de, no mínimo, os seguintes componentes do Storage: tamanho e utilização de volumes e/ou LUNs, aggregates/RAID pools e/ou RAID groups e utilização de CPU. Caso o equipamento não suporte TRAP e POOL, será entregue software de gerência e monitoramento adicional sem custo para a contratante;
- Quaisquer softwares agregados ao hardware fornecido terão duração “Life time”, permitindo a utilização de todos os recursos de software do sistema indefinidamente, independentemente do tempo de garantia contratado;
- Durante o período de garantia de 60 (sessenta) meses, será possível atualizar o software do equipamento sempre

que houver nova atualização disponibilizada pelo fabricante;

- Não haverá nenhuma perda de funcionalidade operacional da solução, e não serão cobrados quaisquer valores adicionais pelo seu uso completo - durante e após o término do contrato
- Será ofertada a versão mais atual do software da solução, liberada oficialmente pelo fabricante.
- Aplicará pacotes de correção, em data e horário a serem definidos pelo CONTRATANTE, sempre que forem encontradas falhas de laboratório (bugs) ou falhas comprovadas de segurança no software que integra o objeto do contrato.
- O suporte técnico será prestado em português do Brasil (PT-BR).

Por fim, a Huawei informa que esta declaração não cria relação de responsabilidade de qualquer tipo, incluindo solidária, *joint venture*, agente principal ou relações similares entre a Huawei e a Compwire, bem como nenhuma atividade conduzida pela Compwire deverá criar quaisquer responsabilidades para a Huawei.

A presente declaração permanecerá válida pelo período de 06 (seis) meses contados da sua emissão.

FERNANDA NUNES CALANDRINO PRATES:27765319825

Digitally signed by FERNANDA NUNES CALANDRINO PRATES:27765319825
Date: 2022.11.22 11:10:55 -03'00'

Por e em nome de: **HUAWEI DO BRASIL TELECOMUNICAÇÕES LTDA.**

FusionCube

Technical White Paper

Issue	**02**
Date	**2021-01-30**

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: https://e.huawei.com

About This Document

Overview

This document introduces FusionCube for virtualization in terms of benefits, architecture, performance, scalability, security, and reliability.

Intended Audience

This document is intended for:

- Marketing engineers
- Technical support engineers
- Maintenance engineers

Symbol Conventions

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

Symbol	Description
DANGER	Indicates a hazard with a high level of risk which, if not avoided, will result in death or serious injury.
WARNING	Indicates a hazard with a medium level of risk which, if not avoided, could result in death or serious injury.
CAUTION	Indicates a hazard with a low level of risk which, if not avoided, could result in minor or moderate injury.
NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
NOTE	Supplements the important information in the main text. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

Change History

Issue	Date	Description
03	2021-03-30	This issue is the third official release.
02	2021-01-30	The issue is the second official release.
01	2020-08-15	This issue is the first official release.

Contents

1 Cabinet (optional)

1.1 Cabinet Appearance

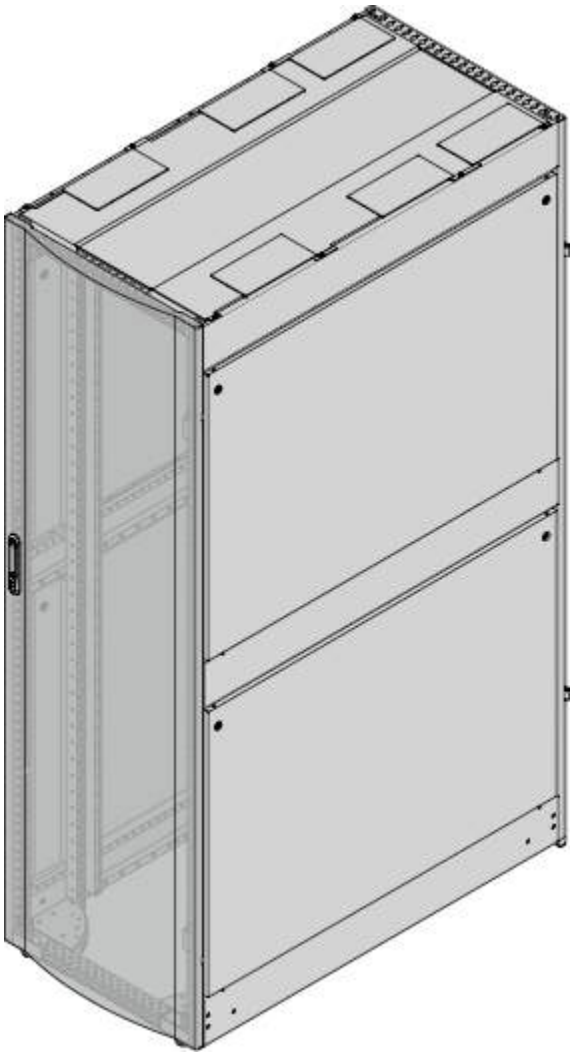
This section describes the function, exterior, physical structure, ESD jack, and technical specifications of the cabinet

The cabinet complies with International Electrotechnical Commission (IEC) 60297-1 and is an assembled cabinet for ease of expansion, which is compliant with ANSI / EIA 310. The distance between front and rear mounting bars in the cabinet can be adjusted at a minimum unit of 25 mm. The cabinet has the following functions:

- Delivers space for accommodating components that can be interconnected.
- Is equipped with castors to facilitate movement on a flat floor or a gradient that slopes to less than or equal to 10 degrees.
- Protects components from dust.
- Prevents components from being damaged.

The appearance of the cabinet is in sand texture black, the following figure shows the cabinet.

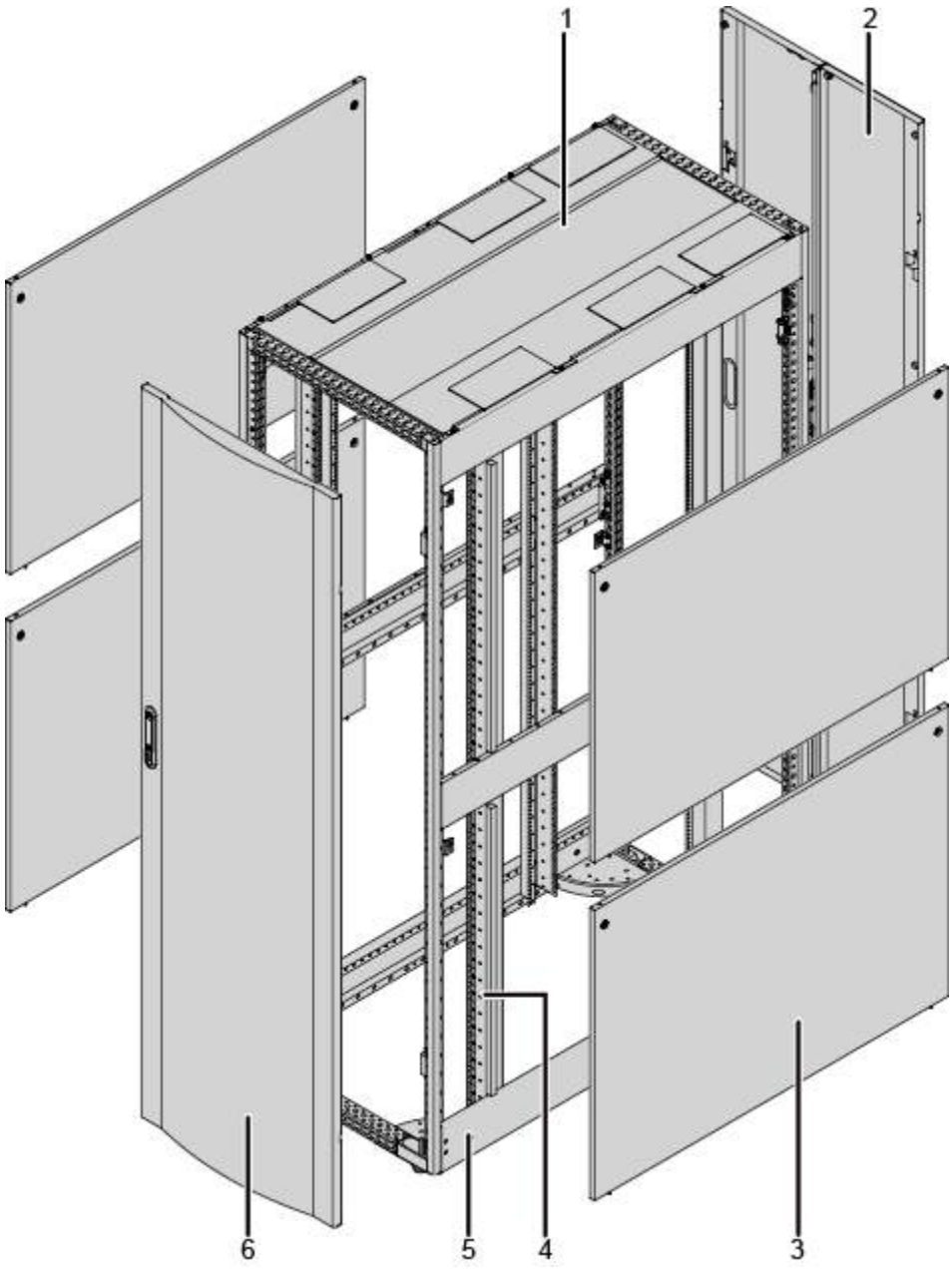
Figure 1-1 Appearance of the cabinet



1.2 Physical Structure

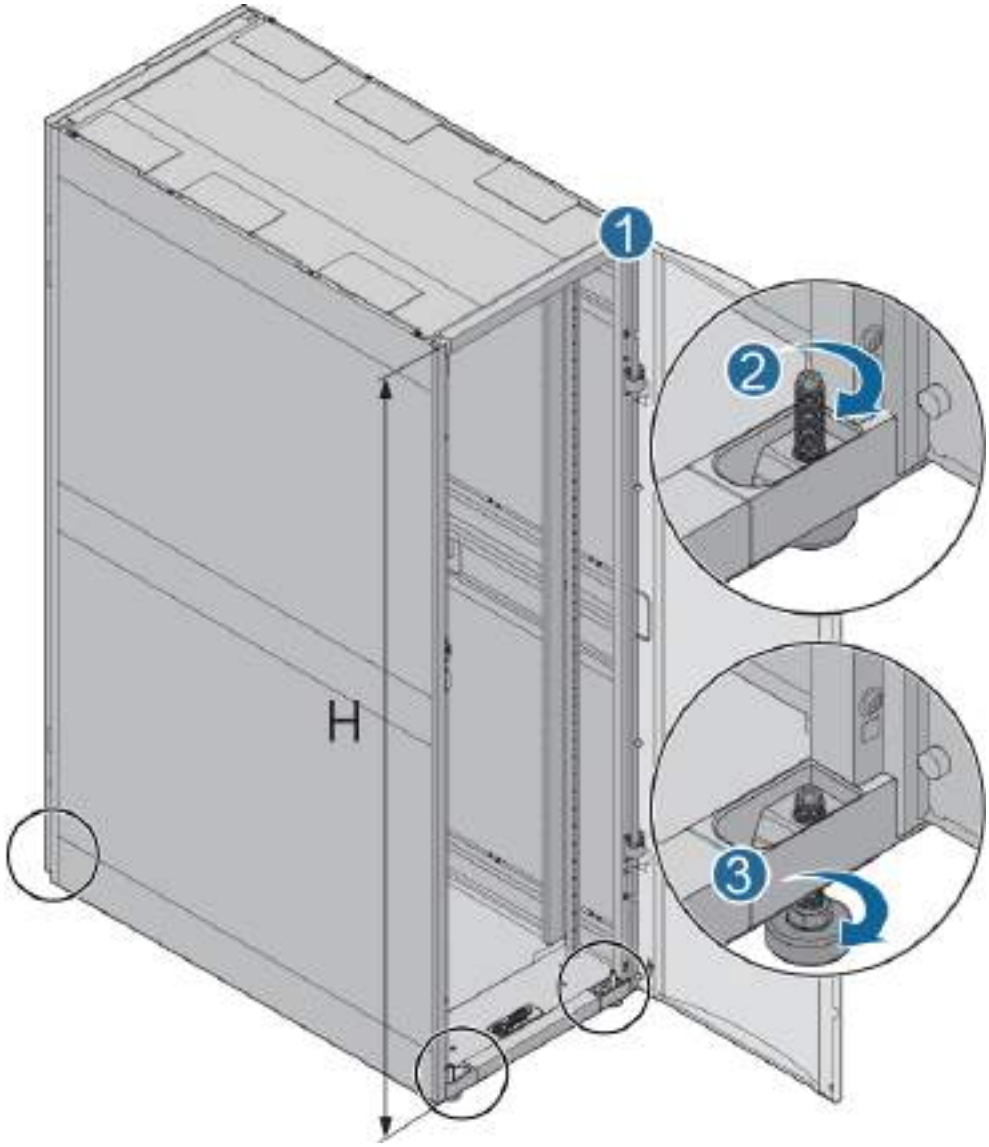
The cabinet consists of the racks, front doors, back doors, side panels, cover, and mounting bars, as shown in the following figure.

Figure 1-2 Cabinet structure



1	Cover	2	Rear door
3	Side panel	4	Mounting bar
5	Rack	6	Front door

Figure 1-3 Securing a cabinet



NOTE:

Spin the castors by using a Phillips screwdriver. If the castors rotate freely, they are hanging in the air.

H indicates the height from the cabinet top to the ground. The adjustable height range of the support foots is 1995 mm to 2005 mm. The height of the support foots can be adjustable.

1.3 Cabinet Technical Specifications

The cabinet complies with International Electrotechnical Commission (IEC) 60297-1 standards. Space for installing power distribution units (PDUs) is reserved in the rear of the cabinet. The cabinet has abundant fittings and features high reliability, easy installation, high compatibility, and environmental friendliness.

High Reliability

Cabinet

- High mechanical strength and corrosion resistance
  - The cabinet is welded with high-strength structural steel to ensure mechanical strength.
  - The cabinet adopts high-strength cold-rolled steel sheet and hot-dip zinc-coated sheet to ensure mechanical strength and corrosion resistance.
- Secure and reliable structure design
  - The nonmetallic parts of the cabinet have passed the restriction of the use of certain hazardous substances (RoHS) test to ensure no leaks or pollution during usage and disposing.
- Intelligent management
  - Supports front door and rear door locks with keys to help customers achieve equipment security management.

Easy Installation

- Castors are installed on 2 m high cabinets for easy movement, reducing the installation time.
- Cabinets can be easily combined without removing cabinet doors.
- Cabinets can be installed on bases or directly on a floor.
- Cabinets can be installed with protective earthing conductor
- Side panels are installed on the cabinet to seal cabinet sides and prevent dust. One side panel consists of two side panels, each side panel can be installed and removed with screws, so it can be easy to remove side panels
- A power distribution unit (PDU) must be installed to provide power for the components in a cabinet. It can support different position to install, it is better to install the PDU vertically on the PDU installation plate on either side at the rear of the cabinet.

High Compatibility

The cabinet can host Huawei servers, storage devices, as well as third-party 19-inch standard servers, storage devices, and network devices.

Abundant Cabinet Fittings

- Adopts simple installation and removal design for cabinet fittings to reduce installation, adjustment, and maintenance time.
- Abundant hardware fittings are provided, which can be installed based on requirements and are easy to operate and manage.

Environmental Friendliness

The cabinet provides an environmentally-friendly and energy-saving telecommunications level equipment room solution where:

- The cabinet meets RoHS requirements.

Table 1-1 lists the technical specifications of the cabinet

Parameter	Value
Dimensions (height x width x depth)	2000 mm x 600 mm x 1200 mm
Capacity	42 U of internal space
Weight	120 kg (only with the front and rear doors)
Load-bearing weight	1000 kg
Cabling mode	Overhead and underfloor cabling
Installation mode	Fastening installation and non-fastening installation The two modes are applicable both to the concrete ground and ESD floor.
Material	High-intensity G-A quality carbon cold-rolled steel plates and galvanized sheets that comply with Restriction of the Use of Certain Hazardous Substances (RoHS) and Underwriter Laboratories (UL)
Heat dissipation	Perforated doors, front-to-rear cooling, and underfloor air intake
Operating temperature	Long-term: 0°C to 50°C Short term: -5°C to +50°C
Operating humidity	Long term: 5% RH to 85% RH Short term: 5% RH to 95% RH
Power supply and power distribution	The cabinet supports single-phase PDU and three-phase PDU. Each cabinet must be equipped with multiple PDUs of the same type, provide N + N redundancy.

1.4 Power distribution unit

This section describes the functions and technical specifications of different PDUs

1.4.1 PDU (PDU2000-32-1PH-11/2-B1)

The power distribution unit (PDU) distributes AC power to cabinets, the input and output power capacity specifications are marked in the PDU label. It has the following features:

- Provides 13 outlets:

- 11 IEC60320 C13 outlets. The maximum output current of a single outlet is 10 A.
- 2 IEC60320 C19 outlets. The maximum output current of a single outlet is 16 A.

- Provides output overcurrent protection with circuit breakers.

Table 1-2 Technical specifications

Category	Item	Technical Specifications
Mechanical specifications	Dimensions (H x W x D)	876 mm x 50 mm x 44.45 mm
	Color	Black
	Weight	10 kg
	Input cable specifications	➢ Length: 3 m ➢ Model: Rvv 3 x 6 mm2
	Input connector model	IEC 60309 AC connector
Environmental specifications	Temperature	➢ Operating temperature: –5°C to +55°C ➢ Storage temperature: –40°C to +70°C
	Humidity (non-condensing)	➢ Operating humidity: 5% RH to 85% RH ➢ Storage humidity: 5% RH to 95% RH
	Altitude	0 m to 3000 m
	Atmospheric pressure	70 kPa to 106 kPa
Input power specifications	Input voltage range	200 V AC to 240 V AC at 50 Hz or 60 Hz
	Maximum input current	32 A
Output power specifications	Output voltage range	200 V AC to 240 V AC at 50 Hz or 60 Hz
	Rated output current	13 outlets: ➢ 11 IEC60320 C13 outlets. The maximum output current of a single outlet is 10 A. ➢ 2 IEC60320 C19 outlets. The maximum output current of a single outlet is 16 A.
	Output overcurrent protection feature	The overcurrent protection feature is available for all outputs with circuit breakers.

1.4.2 PDU (PDU2000-32-1PH-20/4-B2)

The power distribution unit (PDU) distributes AC power to cabinets, the input and output power capacity specifications are marked in the PDU label. It has the following features:

- Provides 24 outlets:
  - 20 IEC60320 C13 outlets. The maximum output current of a single outlet is 10 A.
  - 4 IEC60320 C19 outlets. The maximum output current of a single outlet is 16 A.
- Provides output overcurrent protection with circuit breakers.

Table 1-3 Technical specifications

Category	Item	Technical Specifications
Mechanical specifications	Dimensions (H x W x D)	1782 mm x 50 mm x 44.45 mm
	Color	Black
	Weight	10 kg
	Input cable specifications	➢ Length: 3 m ➢ Model: Rvv 3 x 6 mm2
	Input connector model	IEC 60309 AC connector
Environmental specifications	Temperature	➢ Operating temperature: –5°C to +55°C ➢ Storage temperature: –40°C to +70°C
	Humidity (non-condensing)	➢ Operating humidity: 5% RH to 85% RH ➢ Storage humidity: 5% RH to 95% RH
	Altitude	0 m to 3000 m
	Atmospheric pressure	70 kPa to 106 kPa
Input power specifications	Input voltage range	200 V AC to 240 V AC at 50 Hz or 60 Hz
	Maximum input current	32 A
Output power specifications	Output voltage range	200 V AC to 240 V AC at 50 Hz or 60 Hz
	Rated output current	24 outlets: ➢ 20 IEC60320 C13 outlets. The maximum output current of a single outlet is 10 A. ➢ 4 IEC60320 C19 outlets. The maximum output current of a single outlet is 16 A.

Category	Item	Technical Specifications
	Output overcurrent protection feature	The overcurrent protection feature is available for all outputs with circuit breakers.

1.4.3 PDU (PDU2000-32-1PH-20/4-B2)

The power distribution unit (PDU) distributes AC power to cabinets, the input and output power capacity specifications are marked in the PDU label. It has the following features:

- Provides 21 outlets :
  - 12 IEC60320 C13 outlets. The maximum output current of a single outlet is 10 A.
  - 9 IEC60320 C19 outlets. The maximum output current of a single outlet is 16 A.
- Provides output overcurrent protection with circuit breakers.

Table 1-4 Technical specifications

Category	Item	Technical Specifications
Mechanical specifications	Dimensions (H x W x D)	1732 mm x 50 mm x 44.45 mm
	Color	Black
	Weight	10 kg
	Input cable specifications	➢ Length: 3 m ➢ Model: Rvv 5 x 6 mm2
	Input connector model	IEC 60309 AC connector
Environmental specifications	Temperature	➢ Operating temperature: –5°C to +55°C ➢ Storage temperature: –40°C to +70°C
	Humidity (non-condensing)	➢ Operating humidity: 5% RH to 85% RH ➢ Storage humidity: 5% RH to 95% RH
	Altitude	0 m to 3000 m
	Atmospheric pressure	70 kPa to 106 kPa
Input power specifications	Input voltage range	346 V AC to 415 V AC at 50 Hz or 60 Hz
	Maximum input current	32 A

Category	Item	Technical Specifications
Output power specifications	Output voltage range	200 V AC to 240 V AC at 50 Hz or 60 Hz
	Rated output current	21 outlets: ➢ 12 IEC60320 C13 outlets. The maximum output current of a single outlet is 10 A. ➢ 9 IEC60320 C19 outlets. The maximum output current of a single outlet is 16 A.
	Output overcurrent protection feature	The overcurrent protection feature is available for all outputs with circuit breakers.

1.5 Filler Panel

Both standard and non-standard filler panels are provided:

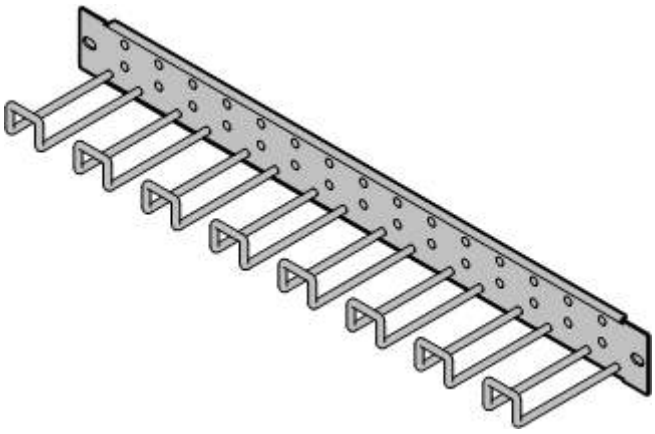
- The height of a standard filler panel is an integral multiple of U (1 U = 44.45 mm).
- The height of a non-standard filler panel is not an integral multiple of U.

Figure 1-4 Appearance (2 U filler panel)

1.6 Cable Organizer

A cable organizer is installed on the rear mounting bars in a cabinet for routing power and signal cables.

Figure 1-5 Appearance



1.7 High-Density Cable Organizer

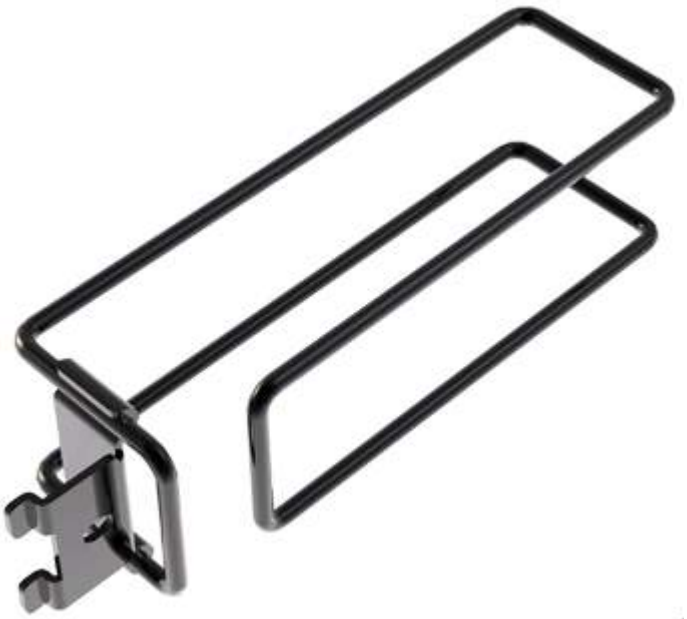
A high-density cable organizer is used for routing cables without occupying any device space.

Figure 1-6 Appearance

1.8 Vertical Cable Guide

A vertical cable guide is installed on the column in a cabinet to manage vertically-routed cables.

Figure 1-7 Appearance



OceanStor 5310/5510/5610
New-Gen Hybrid Flash Storage Systems

OceanStor 5310/5510/5610
New-Gen Hybrid Flash Storage Systems

Huawei's New-Gen OceanStor 5310/5510/5610 Hybrid Flash Storage Systems are designed for future data centers.

Designed to help users achieve their business goals, they adopt Huawei's proprietary algorithms to efficiently deploy data across media, fully utilizing the SSD space to accelerate mission-critical data. Their comprehensive convergence and value-added features deliver leading system efficiency and reliability, while the built-in Insight module provides intelligent prediction. The systems supercharged by the features provide diversified storage services to users, ideal for the finance, government, manufacturing, education, healthcare, energy, and media entertainment sectors.

Endless Evolution

- Huawei OceanStor 5310/5510/5610 storage supports hybrid workloads such as blocks, files, virtualization, and containers, which meets the users' elastic service development requirements, improves storage resource utilization, and effectively reduces the total cost of ownership (TCO). In addition, balanced SAN and NAS services, supercharged by the Hyper and Smart features, provide diversified data protection and efficiency improvement capabilities for block and file systems. This provides users with comprehensive services.
- Industry's only gateway-free active-active solution for both SAN and NAS reduces the number of faulty nodes, simplifies deployment, and improves system reliability. In addition, the active-active deployment implements load-balancing active-active mirroring and non-disruptive cross-site failover, freeing users from the worry of system breakdown. What's more, the 3DC and 4DC data recovery (DR) solutions are also optional for even higher reliability.
- The combination of private and public clouds, cloud backup, and container services have supercharged the user's smooth migration of data to the cloud.
- The ransomware protection solution that features the Air Gap technology and high-density snapshots can effectively defend against ransomware attacks and support fine-grained data restoration.*

Flash-Like Performance

- The global cold and hot data perception and data collaboration algorithms that support self-learning in all scenarios are used to detect changes in service models and cold and hot data, helping promptly locate hot data in all scenarios.
- Elastic convergence of cache and tiers resolves challenges faced in the traditional practice and fuels the hot data acceleration, which results in optimal data layout and simplified configuration.
- Redirect-on-write (ROW) large block sequential write: Multiple small block discrete writes are aggregated into one consecutive large block write, reducing write amplification and ensuring stable write performance in all RAID arrays.
- Low-latency RDMA connections among multiple controllers and fully-balanced active-active architecture enable a single LUN to deliver more than 90% of the system performance.
- End-to-end NVMe architecture: Storage supports 32Gbps FC-NVMe/25Gbps RoCE at the front end and 100Gbps RDMA at the back end, which realizes end-to-end data acceleration and enables latency as low as 0.05 ms.
- The global distributed file system distributes subdirectories on multiple controllers, which relieves the performance pressure of frequent access to a large number of small file directories. Two layouts of metadata sequence tables and hash tables improve the system OPS by 30%.

Cost Effectiveness

- Fewer SSDs and NL-SAS disks provide equivalent disk performance as SSDs + SAS or SSDs + SAS + NL-SAS.
- Data flows from edge to core across storage systems (high-end, mid-range, entry-level) and convergence of all-flash, hybrid flash, and backup storage reduce storage costs because no gateway or additional software is required.
- Predictable, scalable, and high-performance storage infrastructure meets the requirements of unpredictable business growth. Huawei OceanStor 5310/5510/5610 storage supports a maximum of 16 controllers, resulting in a linear increase of IOPS and storage capacity.
- DME interconnects with Ansible and mainstream IT Service Management platforms like ServiceNow, reducing O&M costs.

Technical Specifications

Model	OceanStor 5310	OceanStor 5510	OceanStor 5610
Hardware Specifications			
Maximum number of controllers	16	16	16
Maximum cache (dual controllers, grows with the expansion of controllers)	128 GB to 2 TB	384 GB to 4 TB	768 GB to 8 TB
Supported storage protocols	FC, iSCSI, NFS, CIFS, FC-NVMe, NVMe over RoCE, FTP*, HTTP*, NDMP, S3*		
Front-end channel port types	8/16/32 Gbps FC/FC-NVMe, 1/10/25/40/100 Gbps Ethernet, 25 Gbps NVMe over RoCE		
Back-end channel port types	100 Gbps RDMA/SAS 3.0		
Maximum number of hot-swappable I/O modules per controller enclosure	6	12	
Maximum number of front-end host ports per controller enclosure	40	48	
Hard disk types	NVMe TLC SSD, SAS TLC SSD, SAS, NL-SAS		
Supported SCMs	800 GB/1.6 TB*		
Software Specifications			
RAID levels	RAID 5, RAID 6 and RAID-TP (tolerating simultaneous failure of three disks)		
Value-added software	SmartAcceleration, SmartThin, SmartQuota, SmartMulti-Tenant, SmartQoS, SmartVirtualization, SmartMigration, SmartCompression, SmartDedupe, HyperSnap, HyperReplication, HyperClone, HyperMetro, HyperCDP, HyperLock, HyperDetect, HyperEncryption, CloudBackup*		
Storage management software	Device Manager	UltraPath	eService
Electrical Specifications			
Power supply	100 V to 240 V AC ± 10%, 192 V to 288 V DC, -38.4 V to -75 V DC		200 V to 240 V AC ± 10%, 192 V to 288 V DC
Dimensions (H x W x D)	2.5-inch controller enclosure: 86.1 mm x 447 mm x 520 mm 3.5-inch controller enclosure: 86.1 mm x 447 mm x 600 mm NVMe controller enclosure*: 86.1 mm × 447 mm × 620 mm	2.5-inch controller enclosure: 86.1 mm x 447 mm x 820 mm 3.5-inch controller enclosure: 86.1 mm x 447 mm x 900 mm NVMe controller enclosure*: 86.1 mm x 447 mm x 920 mm	
	SAS disk enclosure: 86.1 mm × 447 mm × 410 mm NVMe disk enclosure:* 86.1 mm × 447 mm × 620 mm NL-SAS disk enclosure: 175 mm x 447 mm x 488 mm		
Weight (excluding disk units)	2.5-inch controller enclosure: 23.75 kg 3.5-inch controller enclosure: 24.1 kg NVMe controller enclosure*: 21.25 kg	2.5-inch controller enclosure: 38.05 kg 3.5-inch controller enclosure: 38.5 kg NVMe controller enclosure*: 40.65 kg	
	2.5-inch SAS disk enclosure: 13.4 kg 3.5-inch SAS disk enclosure: 26.5 kg NVMe disk enclosure*: 24.95 kg		
Operating temperature	-60 m to +1800 m altitude: 5°C to 35°C (cabinet) or 40°C (enclosure) 1800 m to 3000 m altitude: The maximum temperature threshold decreases by 1°C for every altitude increase of 220 m		
Operating humidity	10% to 90% R.H.		

*Contact Huawei sales staff if you need this specification.

For More Information

To learn more about Huawei storage, please contact your local Huawei office or visit the Huawei Enterprise website: http://e.huawei.com/en/.

Huawei Enterprise Business App

Huawei IT Products & Solutions - LinkedIn

Huawei IT Products & Solutions - YouTube

Huawei Technologies Co., Ltd

Bantian Longgang District

Shenzhen 518129, P.R. China

Tel: +86-755-28780808

www.huawei.com

Trademarks and Permissions

HUAWEI, HUAWEI, and are trademarks or registered trademarks of Huawei Technologies Co., Ltd.

Other trademarks, product, service and company names mentioned are the property of their respective holders.

Disclaimer

The content of this manual is provided "as is". Except as required by applicable laws, no warranties of any kind, either express or implied, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose, are made in relation to the accuracy, reliability or contents of this manual.

To the maximum extent permitted by applicable law, in no case shall Huawei Technologies Co., Ltd be liable for any special, incidental, indirect, or consequential damages, or lost profits, business, revenue, data, goodwill or anticipated savings arising out of, or in connection with, the use of this manual.

Huawei OceanStor V5 Converged Storage Simple Interoperability Matrix

Date 10/18/2021

Huawei Technologies Co., Ltd. provides customers with comprehensive technical support and service. For any assistance, please contact our local representative office, agency, or customer service center.

Trademark Notice

 and other Huawei trademarks are trademarks or registered trademarks of Huawei Technologies Co., Ltd.
Other trademarks, products, services and company names mentioned are the property of their respective owners.

Contents

Base connectivity inter-operability matrix

Operating System	MultiPath Software			Volume Manager Software		Cluster Software			NAS[4]			
	UltraPath	Native MPIO	Veritas DMP	Native LVM	Veritas VxVM	Native Cluster	Veritas Cluster	others	SMB	NFS	FTP/FTPS	HTTP/HTTPS
Apple MAC OS X 10.7	NA	HBA Driver[1]	NA	Y	NA	X SAN	NA		Y			Y
Apple MAC OS X 10.8		HBA Driver[1,2]							Y			
Apple MAC OS X 10.9		HBA Driver[1]							Y			
Apple MAC OS X 10.10		HBA Driver[1]							Y			Y
Apple MAC OS X 10.11		HBA Driver[1]							Y			Y
Apple MAC OS X 10.12		HBA Driver[1]										
Apple MAC OS X 10.13		HBA Driver[1]							Y			
AIX 5.3 TL3 and later	Y	MPIO	5.1SP1	Y	5.1SP1	HACMP	5.1SP1		NA			
AIX 6.1			5.1SP1,6.0,6.1,6.2, 7.0,7.1		5.1SP1,6.0,6.1,6.2, 7.0,7.1	HACMP,PowerHA	5.1SP1,6.0,6.1,6.2, 7.0,7.1	GPFS[3]	NA	Y	Y	
AIX 7.1			5.1SP1,6.0,6.1,6.2		6.1 ,6.2,7.0,7.1,7.2	PowerHA	6.1, 6.2,7.0,7.1,7.2	GPFS[3]	NA	Y	Y	
AIX 7.2	Y	MPIO	6.0,6.1,6.2	Y	7.1,7.2	PowerHA	7.1,7.2		NA	Y	Y	
HP UX 11iv1	NA	PV-Links		Y		MC/SG			NA			
HP UX 11iv2									NA			
HP UX 11iv3	NA	PV-Links,NMP	5.1SP1,6.0	Y	5.1SP1,6.0	MC/SG	5.1SP1,6.0	RAC[3]	NA	Y	Y	Y
OpenVMS 8.4 update 1000 for IA64	NA	OpenVMS Multipath	NA	Y	NA	NA	NA	NA	NA	NA	NA	NA
OpenVMS 8.4 update 1200 for Alpha	NA	OpenVMS Multipath	NA	Y	NA	NA	NA	NA	NA	NA	NA	NA
RHEL 5(x86/x64)	Y	DM-Multipath	5.1SP1,6.0,6.1	Y	5.1SP1,6.0,6.1	RHCS	5.1SP1,6.0,6.1	RAC[3]	NA	Y	Y	Y
RHEL 6(x86/x64)			5.1SP1,6.0,6.1,6.2		5.1SP1,6.0,6.1,6.2, 7.0,7.1,7.2		5.1SP1,6.0,6.1,6.2, 7.0,7.1,7.2	RoseHA[3]	NA	Y	Y	Y
RHEL 7(x64)	Y	DM-Multipath	6.2	Y	6.2,7.0,7.1,7.2	RHCS	6.2,7.0,7.1,7.2	Pacemaker	NA	Y	Y	Y

RHEL 8(x64)	Y	DM-Multipath	7.x	Y	7.x	RHCS	7.x	Pacemaker	NA	Y	Y	Y
RHEL With KVM	Y	DM-Multipath	NA	Y	NA							
RedFlag Asianux 3/4(x86/x64)	Y	DM-Multipath	NA	Y	NA		NA		NA			
RedFlag Asianux 7(x64)		DM-Multipath							NA			
SLES 10(x86/x64)	Y	DM-Multipath	6.0	Y	6.0	HeartBeat	6.0	RAC[3]	NA	Y	Y	Y
SLES 11(x86/x64)			5.1SP1,6.0,6.1,6.2		5.1SP1,6.0,6.1,6.2, 7.0,7.1,7.2	HeartBeat	5.1SP1,6.0,6.1,6.2, 7.0,7.1,7.2	RAC[3],Rose HA[3],	NA	Y	Y	Y

SLES 12(x64)	Y	DM-Multipath	6.2	Y	2.1,7.0,7.1,7.2	HeartBeat	2.1,7.0,7.1,7.2		NA	Y	Y	
Windows Server 2003(x86/x64)		NA				MSCS			Y	NA		Y
Windows Server 2008(x86/x64)		MPIO	6.0,6.1		6.0,6.1	WSFC	6.0,6.1		Y	NA	Y	Y
Windows 7(x86/x64)		NA	NA		NA	NA	NA		Y	NA	Y	Y
Windows 8(x86/x64)		NA							Y	NA	Y	Y
Windows 10(x64)	Y	NA		Y					Y	NA	Y	Y
Windows Server 2008 R2(x64)		MPIO	6.0,6.1		6.0,6.1,7.0,7.1	WSFC	6.0,6.1,7.0,7.1	RoseHA[3]	Y	NA	Y	Y
Windows Server 2012(x64)			6.0,6.1		6.0,6.1,7.0,7.1,7.2		6.0,6.1,7.0,7.1,7.2		Y	NA	Y	Y
Windows Server 2012 R2(x64)			6.1		6.1,7.0,7.1,7.2		6.1,7.0,7.1,7.2		Y	NA	Y	Y
Windows Server 2016(x64)			6.1		6.1,7.0,7.1,7.2		6.1,7.0,7.1,7.2		Y	NA		
Windows Server 2019(x64)				Y								
Windows Server 2008 R2 with Hyper-V	Y	MPIO	NA	Y	NA	WSFC	NA					
Windows Server 2008 R2 SP1 with Hyper-V	Y		NA		NA		NA					
Windows Server 2012 with Hyper-V	Y		NA		NA		NA					
Windows Server 2012 R2 with Hyper-V	Y		NA		NA		NA					
Windows Server 2016 with Hyper-V	Y		NA		NA		NA					
Windows Server 2019 with Hyper-V	Y		NA		NA		NA					
Solaris 8(SPARC)	NA	STMS	NA	Y	NA				NA			
Solaris 9u9 (SPARC)			5.1SP1		5.1SP1	SUN Cluster	5.1SP1		NA			
Solaris 10u4 and later (SPARC)	Y		5.1SP1,6.0,6.1,6.2		5.1SP1,6.0,6.1,6.2, 7.0,7.1	SUN Cluster	5.1SP1,6.0,6.1,6.2, 7.0,7.1		NA	Y	Y	Y
Solaris 11(SPARC)			6.0,6.1,6.2		6.0,6.1,6.2,7.0,7.1, 7.2	SUN Cluster	6.0,6.1,6.2,7.0,7.1, 7.2		NA	Y	Y	Y
Windows Server 2008 R2 And later for Active Directory	NA	NA	NA	NA	NA	NA	NA		Y	NA	NA	NA
Solaris 10(x86)	NA	STMS		Y		SUN Cluster			NA			
Solaris 11(x86)									NA			
CentOS 5/6(x86/x64)	Y	DM-Multipath	NA	Y	NA	Pacemaker	NA		NA	Y	Y	Y
CentOS 7(x86/x64)									NA	Y	Y	Y

CentOS 8(x64)	Y	DM-Multipath	NA	Y	NA	Pacemaker	NA		NA	Y	Y	Y

Debian 7/8/9(x86/x64)	NA	DM-Multipath	NA	Y	NA		NA		NA	Y	Y	Y
NeoKylin v5/v6/v7	NA	DM-Multipath	NA	Y	NA		NA		NA			
Kylin v3/v4	Y	DM-Multipath	NA	Y	NA		NA					
Scientific Linux 6/7	NA	DM-Multipath	NA	Y	NA		NA		NA			
OEL UEK 5.7 and later (x64)	Y	DM-Multipath	NA	Y	NA	OCFS2	NA		NA	Y	Y	Y
OEL UEK 6(x64)									NA	Y	Y	Y
OEL UEK 7(x64)	Y	DM-Multipath	NA	Y	NA	OCFS2	NA		NA	Y	Y	Y
OEL UEK With KVM	Y	DM-Multipath	NA	Y	NA		NA		NA	NA	NA	NA
Rocky v4/v6	NA	DM-Multipath	NA	Y	NA		NA		NA	Y	Y	Y
Ubuntu 12.04/14.04/14.10/16.04/16.10/18.04(x86/x64)	NA	DM-Multipath	NA	Y	NA		NA		NA	Y	Y	Y
Citrix XenServer 6.x	NA	DM-Multipath	NA	Y	NA	HA(OS bundle)	NA		NA			
Citrix XenServer 7.x									NA	Y	Y	Y
Citrix XenServer 8.x									NA			
VMware ESXi 5.0/5.1/5.5	Y	NMP	NA	Y	NA	HA(OS bundle)	NA		NA	Y		
VMware ESXi 6.0									NA	Y		
VMware ESXi 6.5									NA	Y		
VMware ESXi 6.7									NA	Y		
VMware ESXi 7.0									NA	Y		
FusionCompute V100R005/V100R006	Y	DM-Multipath	NA	Y	NA	HA(OS bundle)	NA		NA	Y		
FusionCompute 6.3.0/6.3.1/8.0									NA	Y		
IBM VIOS 2.1/2.2	Y	MPIO	NA	Y	NA		NA		NA			
IBM VIOS 3.1									NA			
Oracle VM 3.1/3.2/3.3/3.4 for x86	NA	DM-Multipath	NA	Y	NA	HA(OS bundle)	NA		NA	Y		
Oracle VM 3.1/3.2/3.3 for SPARC	Y	STMS	NA	Y	NA							
RHEV 3	NA	DM-Multipath	NA	Y	NA	HA(OS bundle)	NA					
RHEV 4	NA	DM-Multipath	NA	Y	NA	HA(OS bundle)	NA					
Turbo Linux 11.3	NA	DM	NA	Y	NA	NA	NA					
Deepin 15.2	Y	DM	NA	Y	NA	NA	NA					

CloudLinux 6.7	NA	DM	NA	Y	NA	NA	NA					
iSoft v4.0	NA	DM	NA	Y	NA	NA	NA					

For more details, please refer to: http://support-open.huawei.com/ready/pages/user/compatibility/support-matrix.jsf	
Legend: 1.Blank(Not currently Supported) 2.Y(Supported) 3.NA(Not Applicable)	**Notes:** 1. ATTO multipathing driver. 2. LSI multipathing driver. 3. For detail Cluster software version, refer to: http://support-open.huawei.com/ready/pages/user/compatibility/support-matrix.jsf
Supported Switches	All FC SAN switched (2Gb/s or greater) frome Brocade and Cisco,including vendor rebranded versions. **Brocade** 12000,200E,300,3250,3850,3900,4018,4100,4140,48000,4900,5000,5100,5300,5470,6505,6510,6520,6720,7500,7500E, DCX-4S,DCX 8510,G610,G620,M5424 Embedded, VDX 6730,X6-4,X6-8 **Cisco** MDS 9120,9124,9132T,9148,9148s,9250i,9396s,9506,9509,9513,9706,9710 **Hewlett Packard** B-series 8 / 24c SAN BladeSystem c-Class for more details, please refer to:http://support-open.huawei.com/ready/pages/user/compatibility/support-matrix.jsf
Supported Hosts Adapters	All Fibre Channel HBAs from Emulex and QLogic(2Gb/s or greater) and Brocade(4Gb/s or greater),including vendor rebranded versions.for more details, please refer to: http://support-open.huawei.com/ready/pages/user/compatibility/support-matrix.jsf
Supported Servers	Apple MAC pro Workstations, Dell PowerEdge Blade Series, Dell PowerEdge Rack Servers, Fujitsu Primergy Blade Series, HP 9000 RP Series, HP Integrity Blade Series, HP Integrity RX Series, HP ProLiant Blade Series, HP ProLiant Rack Servers, Huawei E6000 Blade Series, Huawei E9000 Blade Series, Huawei RH Rack Servers, Huawei T8000 Blade Series, IBM BladeCenter HS Series, IBM BladeCenter JS Series, IBM Power Series, IBM xSeries Rack Servers, IBM Z10, Lenovo Flex System xSeries, Oracle Sun SPARC Servers. Note: For Server and Operating System inter-operability, refer to the server product vendors' support matrix. For Server and OceanStor V5 Storage System inter-operability, refer to : http://support-open.huawei.com/ready/pages/user/compatibility/support-matrix.jsf

Supported Disk Storage System	**Dell** Compellent series SC20, Compellent series SC30, Compellent series SC40,Compellent series SC4020,Compellent series SC5020,Compellent series SC5020F,Compellent series SC7020,Compellent series SC8000,Compellent series SC9000,Compellent series SCv2000,Compellent series SCv2020,Compellent series SCv2080,MD3600f,MD3620f, MD3660F,MD3800F,MD3820F,MD3860F **EMC** AX4-5,CX200,CX300,CX3-10,CX3-20,CX3-40,CX3-80,CX400,CX4-120,CX4-240,CX4-480,CX4-960,CX500,CX600,CX700,DMX3,DMX4(DMX4-1,DMX4-2,DMX4-3), DMX4-1500,DMX4-950,VMAX,VMAX10K,VMAX20K,VMAX40K,VMAX100K,VMAX200K,VMAX400K,VMAXe,VMAX250F,VMAX250FX,VMAX450F,VMAX450FX, VMAX850F,VMAX850FX,VMAX950F,VMAX950FX,VNX5100,VNX5200,VNX5300,VNX5400,VNX5500,VNX5600,VNX5700,VNX5800,VNX7500,VNX7600,VNX8000,V NXe3200, VNXe3150,VNXe3300,VPLEX,XtremIO,Unity300, Unity300F, Unity400, Unity400F, Unity500, Unity500F, Unity600, Unity600F, Unity650F, UnityVSA **Fujitsu** CX200,CX300,CX3-10,CX3-20,CX3-40,CX3-80,CX400,CX4-120,CX4-240,CX4-480,CX4-960,CX500,CX600,CX700,DX100 S3,DX200 S3,DX410 S2,DX440 S2,DX500 S3,DX60,DX600 S3,DX80,DX80 S2,DX90,DX90 S2, DX60 S2,E8000 Model 1200,E8000 Model 2200,E4000 Model 80/100,DX8700 S3,DX8900 S3,DX60 S4,DX100 S4,DX200 S4,DX500 S4,DX600 S4,DXAF250 S2,DXAF650 S2,AF250,AF650 **Hitachi** AMS1000,AMS200,AMS2100,AMS2300,AMS2500,AMS500,HUS110,HUSVM,HUS130,HUS150,HUS150DC,NSC55,USP100,USP1100,USP600,USP-V,USP-VM,VSP,VSP G1000,VSP G200,VSP G400,VSP G600,VSP G800,WMS100,VSP G350,VSP G370,VSP G700,VSP G900,VSP G1500,VSP F200, VSP F400, VSP F600, VSP F800, VSP F350, VSP F370, VSP F700, VSP F900, VSP F1500 **Huawei** OceanStor 18500,OceanStor 18500 V3,OceanStor 18800,OceanStor 18800 V3,OceanStor 18800F,OceanStor 5300 V3,OceanStor 5500 V3,OceanStor 5600 V3,OceanStor 5800 V3,OceanStor 6800 V3,OceanStor Dorado 2100,OceanStor Dorado 2100G2,OceanStor Dorado 5100,OceanStor S12100,OceanStor S12300,OceanStor S2100,OceanStor S2200T,OceanStor S2300,OceanStor S2300E,OceanStor S2600,OceanStor S2600T,OceanStor S2900,OceanStor S3100,OceanStor S3200,OceanStor S3900,OceanStor S5300,OceanStor S5500,OceanStor S5500T,OceanStor S5600,OceanStor S5600T,OceanStor S5800T,OceanStor S5900,OceanStor S6800,OceanStor S6800E,OceanStor S6800T,OceanStor S6900,OceanStor 5300V5, OceanStor 5500V5, OceanStor 5600V5, OceanStor 5800V5, OceanStor 6800V5, OceanStor 18500V5, OceanStor 18800V5 **HP** 3parF200,3parF400,3parT400,3parT800,3par10400,3par10800,3par20450,3par20800,3par20840,3par20850,3par7200,3par7200c,3par7400,3par7400c,3par7440c,3par7450,3par7450c,3par8200,3par8400,3par8440,3par8450,EVA3000,EVA4000,EVA4100,EVA4400,EVA5000,EVA6000 ,EVA6100,EVA6400,EVA8000,EVA8100,EVA8400,MSA1040,MSA2040,MSA2312fc,MSA2324fc,MSA2012fc,MSA2212fc,P2000 G3,P6300,P6350,P6500,P6550,P9500,SVS200,XP10000,XP12000,XP20000,XP24000,XP7

	IBM DCS3700,DS3400,DS3512,DS3524,DS3950,DS4100,DS4200,DS4300,DS4300\turbo,DS4400,DS4500,DS4700,DS4800,DS5020,DS5100,DS5300,DS6000\Series,DS8100,DS8300,DS8700,DCS3860,DS8880,DS8884,DS8886,DS8888,DS8884F,DS8886F,DS8888F,SVC,V3500,V3700,V5000,V7000,DS8800,DS8870,N3220,N3240,N3300,N3400,N3600,N6040,N6060,N6070,N6210,N6240,N6270,XIV Gen2,Flash System 840,Flash System 900, Flash System 710, Flash System 720, Flash System 810, Flash System 820, Flash System A9000, Flash System A9000R **Netapp** E2612,E2624,E2660,E2712,E2724,E2760,E5412,E5424,E5460,E5512,E5524,E5560,E5612,E5624,E5660FAS2552,FAS2554,FAS2020,FAS2040,FAS2050,FAS2240-2,FAS2240-4 ,FAS3140,FAS3160,FAS3170,FAS3210,FAS3220,FAS3240,FAS3250,FAS3270,FAS6210,FAS6220,FAS6240,FAS6250,FAS6280,FAS6290,FAS8020,FAS8040,FAS8060,FAS8080,v3140,v3160,v3170,v3210,V3220,v3240,V3250,v3270,V6210,V6220,V6240,V6250,V6280,V6290, E5612,E5624,E5660,FAS2620,FAS2650,FAS8200,FAS9000, AFF A200,AFF A300,AFF A700,AFF A700S **SUN** 9985,9985v,9990,9990v,ST2540,ST2540-M2ST6130,ST6140,ST6180,ST6540,ST6580,ST6780 **TMS** RamSan620, RamSan630 Note: 1. ISCSI and FC are supported when Huawei Storage Systems are connected. Only FC is supported for third-party Storage System. 2. The Huawei and third-party storage system firmware requirements and limitation, refer to: http://support-open.huawei.com/ready/pages/user/compatibility/support-matrix.jsf
Supported Storage Virtualization Gateway/Array	**EMC** VPLEX **IBM** SVC/StorWize V **HUAWEI** VIS6000T **HDS** HUS-VM VSP USP-V VSP G1x00/F1500,G/Fxx0 **FalconStor** CDP/NSS **DataCore** SANsymphony For detail requirements and limitation, refer to: http://support-open.huawei.com/ready/pages/user/compatibility/support-matrix.jsf
Supported Software Define Storage	**Veritas** StorageFoundation, InforScale **FalconStor** NSS/CDP **DataCore** SANsymphony-V For detail requirements and limitation, refer to: http://support-open.huawei.com/ready/pages/user/compatibility/support-matrix.jsf
Supported Database	SQL Server 2008 or later,My SQL 5 and 8,Oracle 10 or later,DB2 9.7 and later,,MariaDB 5.x and 10.x,PostgreSQL 9 or later.
Supported VMware feature	VAAI、VASA、VVOLs、SRM 、PSA、NGC、SRM Stretch、vMSC、vRO、vROPs

Support OpenStack Driver	OceanStor V5 V500R007 support OpenStack Juno, Kilo, Liberty, Mitaka, Newton, Ocata, Pike, Red Hat OpenStack6/7/8/9/10/11/12, Mirantis OpenStack7/8/9, FusionSphere OpenStack, SUSE CLOUD 5/6/7, Ubuntu OpenStack Liberty, Mitaka, Ocata For detail requirements and limitation, refer to: http://support-open.huawei.com/ready/pages/user/compatibility/support-matrix.jsf
Support Docker and OpenShift	**Support Kubernetes (with docker)** 1.9 or later **Support OpenShift** 3.9
Storage Products and Version requirements	For detail requirements and limitation, refer to: http://support-open.huawei.com/ready/pages/user/compatibility/support-matrix.jsf
Support NAS Feature	Supported Active Directory Integration for Windows sever 2008 and later
Supported Active Directory Integration	Access Control to the Management Interface “Device Manager” supports integration with Microsoft Active Directory 2008 R2 and later for Windows customers 10 and later

HUAWEI PDU2000 series

Introduction

- PDU2000 series is a professional cabinet-level power system, providing various types of power distribution solutions

Scenarios

- PDU2000 can be widely used in the network communication, telecommunication and electric power and other industry data center of various network cabinets, server cabinet and other equipment.

Features

Reliable

- All socket assembly with good elasticity, abrasion resistant, corrosion resistant material, maintain a high reliable electric conduction
- 0-55℃ , 10-90% wide temperature and humidity environment.

Flexible

- Convenient fixed to the standard racks, occupy less space;
- Friendly LCD display, real-time status monitoring

Intelligent

- Online real-time monitoring system with dynamic visual layouts of run status and operation ;
- Supports Modbus network interfaces ;
- Supports multi-mode alarm notifications.

Specification

Items	PDU2000-16-1PH	PDU2000-32-1PH	PDU2000-16-3PH	PDU2000-63-1PH	PDU2000-32-3PH
capacity(KVA/KW)	3.7	7.3	11	14.5	22
input					
Input Wiring	Ph+N+PE	Ph+N+PE	3Ph+N+PE	Ph+N+PE	3Ph+N+PE
Input Current	16A	32A	16A	63A	32A
Rated Voltage	220~240Vac	220~240Vac	380~415Vac	220~240Vac	380~415Vac
Input Voltage range	187~276 Vac	187~276 Vac	323~477Vac	187~276 Vac	323~477Vac
Input Frequency	50/60Hz				
Interface	terminal box,IEC60309 industry connector(selected)			IEC60309 industry connector	
Input Cable	3*2.5mm^2 *1m(selected)	3*6mm^2*1m(selected)	5*2.5mm^2*1m (selected)	3*16mm^2 *1m	5*6mm2*1m
Output					
Output Wiring	Ph+N+PE				
Output Voltage	220~240Vac				
Output Frequency	50/60Hz				
Output Socket Spec	IEC60320 C13/C19				
Output Configuration	8*C13	2* (10*C13+2*C19)	3* (8*C13+2*C19)	2*(4*C13+2*C19)+ 2*(3*C13+3*C19)	3*(2*C13+1*C19)+ 3*(2*C13+2*C19)
Output Protection	NA	1pcs 16A/1P MCB for each group			
Indicator Light	1pcs	1pcs for each group			
Monitoring Function					
Type	Basic	Basic& Monitoring		Basic	
Monitoring	NA	Operating Voltage/Current/Power/Consumption		NA	
Communication	NA	MODBUS		NA	
Environmental					
Operating Temperature	0-55℃				
Storage Temperature	-20-70℃				
Relative Humidity	10%-90%				
Others					
Height ×Width × Depth (mm)	476 * 44.5 * 44.5 (1U in-cabinet)	1732 * 50 * 44.5 (Full height) 876 * 50 * 44.5 (Half height)	1732 * 50 * 44.5 (Full height)		
Install	Hangers	Hangers + Fixed			
Weight	3kg	7kg/4kg	7kg		
Certification	CE				

OceanStor 5x10 Series
6.1.x

Product Description

Issue	02
Date	2022-08-25

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: https://e.huawei.com

About This Document

Purpose

This document describes the positioning, highlights, typical applications, architecture, specifications, environmental requirements, standards compliance, and granted certifications of the OceanStor storage systems.

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

Product Model	Product Version
OceanStor 5310	6.1.3 6.1.5
OceanStor 5510	
OceanStor 5610	

Intended Audience

This document is intended for all readers.

Symbol Conventions

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

Symbol	Description
DANGER	Indicates a hazard with a high level of risk which, if not avoided, will result in death or serious injury.
WARNING	Indicates a hazard with a medium level of risk which, if not avoided, could result in death or serious injury.
CAUTION	Indicates a hazard with a low level of risk which, if not avoided, could result in minor or moderate injury.

Symbol	Description
NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
NOTE	Supplements the important information in the main text. 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 02 (2022-08-25)

This issue is the second official release.

Issue 01 (2022-01-25)

This issue is the first official release.

Contents

1 Product Positioning

OceanStor storage systems are Huawei's brand-new hybrid flash storage products designed for medium- and large-size enterprise storage environments. The storage systems provide mass data storage, fast data access, high availability, and excellent utilization in the ease-of-use and energy saving form factor.

OceanStor storage systems offer comprehensive and superb solutions by using diverse efficiency boost mechanisms to provide industry-leading performance. Those solutions help customers maximize their return on investment (ROI) and meet the requirements of different application scenarios such as online transaction processing (OLTP), online analytical processing (OLAP), high-performance computing (HPC), server virtualization, and virtual desktop infrastructure (VDI).

In addition to providing enterprise users with high-performance and efficient storage services, OceanStor storage systems support advanced data backup and disaster recovery technologies, ensuring secure and smooth operation of data services. The storage systems also offer various methods for easy management and convenient local/remote maintenance, remarkably reducing management and maintenance costs.

2 Product Highlights

OceanStor storage systems combine a cutting-edge hardware structure and an optimized software architecture with advanced data application and protection technologies, meeting medium- and large-size enterprises' storage requirements for high performance, scalability, reliability, and availability. In addition, the OceanStor storage systems integrate both SAN and NAS on one set of hardware and software without using independent NAS gateways. The systems support file access protocols such as NFS and CIFS, and block access protocols such as Fibre Channel (SCSI-port-based FC-SCSI protocol or NVMe-port-based FC-NVMe protocol), iSCSI, and NVMe over RoCE. Both SAN and NAS can scale out to multiple controllers. Hosts can access any LUN or file system from a front-end port on any controller.

NOTE

- The use of the FC-NVMe protocol is closely related to application scenarios and network ecosystem. In 6.1.5 and later versions, some interface modules do not support the FC-NVMe protocol. For details, contact Huawei technical support.

High Performance

SmartAcceleration is a key feature for performance improvement on the next-generation OceanStor hybrid flash storage. It leverages the large block sequential write mechanism of redirect-on-write (ROW) and uses a unified performance layer for cache and tier performance acceleration. This breaks the bottleneck of traditional HDDs in random IOPS performance, maximizing the performance of the hybrid flash system.

OceanStor storage systems use distributed file systems, which means the file systems are not owned by any specific controller. Directories and files in a file system are evenly distributed to all controllers by a balancing algorithm. Read and write requests are equally distributed on each controller so that one file system can fully utilize the resources of the entire storage cluster. Customers can use the file system in one namespace or multiple file systems based on their service plans. The distributed file systems apply to file sharing scenarios with coexisting mass volumes of small and large files. Data in each directory is evenly distributed to each controller for load balancing. The same controller processes the I/Os of a directory and its files to eliminate forwarding across controllers and improve performance for directory traversal, attribute traversal, and batch attribute configuration. When large files are written to a storage pool, RAID 2.0+ globally

distributes their data blocks to all SSDs in the storage pool for improved write bandwidth.

Flexible Scalability

OceanStor storage systems have an outstanding scalability. They support a wide range of the following disks and interface modules in a high density:

- Disks: SAS disks, NL-SAS disks, and SSDs.
- Interface modules: see **3.6 Interface Module**.

OceanStor storage systems support both scale-up and scale-out, achieving flexible scalability while maintaining high performance.

- Scale-up

  Increases storage capacity and improves processing capabilities of existing controllers.
- Scale-out

  Enables performance to increase linearly with the number of controllers.

High Reliability

OceanStor storage systems offer advanced data protection technologies to minimize risks of disk failures and data loss, and protect data against catastrophic disasters, ensuring continuous system running.

- Component failure protection

  Storage system components are in 1+1 redundancy and work in active-active mode. Normally, the two redundant components are working simultaneously and share loads. If one component fails or is offline, the other one takes over all loads without affecting ongoing services.
- RAID 2.0+

  The RAID 2.0+ underlying virtualization technology is used to automatically balance loads across disks. RAID 5, RAID 6, and RAID-TP are supported. RAID-TP can tolerate simultaneous failure of three disks. If a disk encounters a fault, all the other disks in the same disk domain help reconstruct the faulty disk's service data, achieving a 20-fold faster reconstruction speed than traditional RAID and significantly reducing the possibility of multi-disk failure. RAID 2.0+ supports dynamic RAID and flexible data layout, accelerating SSD reconstruction.
- Power failure protection

  Built-in backup battery units (BBUs) supply power to controller enclosures in the event of unexpected power failures. This enables the storage system to write cache data to built-in disks of controllers to prevent data loss.
- Global wear leveling and anti-wear leveling
  - Global wear leveling: If data is unevenly distributed to SSDs, certain SSDs may be used more frequently and wear faster than others. As a result, they may fail much earlier than expected, increasing the maintenance costs. OceanStor storage systems address this problem by using global wear leveling that levels the wear degree among all SSDs, improving SSD reliability.

  - Global anti-wear leveling: When the wear degree of multiple SSDs is reaching the threshold, the system preferentially writes data to specific SSDs. In this way, these SSDs wear faster than the others. This prevents multiple SSDs from failing at a time.
- Disk data pre-copy

  The disk data pre-copy technology enables the storage system to routinely check hardware status and migrate data from any failing disk to minimize the risks of data loss.
- Advanced data protection
  - HyperSnap supports writable snapshots. Snapshot creation and activation have no impact on performance.
  - HyperReplication backs up local data to a remote storage system for disaster recovery.
  - HyperClone generates a full copy of the source data in the local storage system for data backup or use by other applications, ensuring local data security.
  - HyperCDP achieves continuous data protection at an interval of several seconds, generating more intensive recovery points on storage devices.
  - HyperMetro enables real-time data synchronization and access between two storage systems. If data access fails in either storage system, HyperMetro implements seamless service switchover to ensure data security and service continuity.

High Availability (HA)

OceanStor storage systems use TurboModule, online capacity expansion, and disk roaming to ensure service continuity during routine maintenance.

- TurboModule enables hot swap of controllers, power modules, interface modules, BBUs, fan modules, and disks.
- Online capacity expansion allows you to add disks to the system online with ease.
- Disk roaming enables the storage system to automatically identify relocated disks and resume their services.

OceanStor storage systems use multiple resource application technologies to flexibly manage resources and maximize customers' ROI.

- SmartVirtualization allows a local storage system to centrally manage resources of third-party storage systems, simplifying management and reducing maintenance costs.
- SmartMigration migrates LUNs in or between storage systems, adjusting and allocating resources along with business development.
- SmartQoS categorizes service data based on its characteristics (each category represents a type of application) and sets a priority and performance objective for each category. In this way, resources can be preferentially allocated to services with high priorities to guarantee their performance.
- SmartQuota is a file system quota technology. It controls the storage resources for directories, users, and user groups to prevent overuse of storage resources by specific users.

High System Security

- Storage network security
  - Secure management channel

    All management operations from physical ports are controlled by the access authentication mechanism of the storage system, and only authorized users are allowed to manage the storage system.
  - Secure protocols and ports

    The storage system provides only necessary external connections for system operations and maintenance. All the ports used are listed in the Communication Matrix. Dynamic listening ports are functioning in a proper scope, and no undisclosed ports exist.
  - Isolation between service and management ports

    The access control list (ACL) is used to isolate Ethernet ports from internal heartbeat network ports, management network ports, and maintenance ports.

  NOTE

  Internal heartbeat links exist between the controllers in a storage system and are used to check the operating status of the controllers. No additional links are required.
- Storage management security

  Management permissions are controlled by enabling or disabling users. All management operations are logged.

Virtualization, Intelligence, and Efficiency

OceanStor storage systems adopt cutting-edge storage designs in terms of virtualization, intelligence, and efficiency. Compared with traditional storage systems, OceanStor storage systems use the following technologies to provide higher storage space utilization, faster data reconstruction, smarter performance allocation, and finer service quality control:

- RAID 2.0+ underlying virtualization

  Divides disk storage space into small-sized data blocks and uses the blocks to create RAID groups for fine-grained resource management. This technology enables automatic load balancing, higher storage performance, better storage space utilization, faster disk reconstruction, and delicate storage space management, serving as a basis for a number of other advanced storage technologies.
- Intelligent thin provisioning (SmartThin)

  SmartThin allocates storage space on demand rather than pre-allocating all storage space at the initial stage. It is a cost-effective solution because customers can start business operations with minimal disks and add disks based on onsite requirements. In this way, the initial purchase cost and Total Cost of Ownership (TCO) are reduced.
- Deduplication and compression (SmartDedupe and SmartCompression)

  OceanStor storage systems use SmartDedupe and SmartCompression to deduplicate and compress data to save storage space and reduce read and write operations on SSDs. This helps prolong the service life of SSDs and reduce the investment costs as well as the O&M costs.

NOTE

- A hybrid flash storage system with both SSDs and HDDs supports SmartCompression but does not support SmartDedupe.
- An all-flash storage system with only SSDs supports both SmartCompression and SmartDedupe.

Cost-Effectiveness and Ease-of-Use

OceanStor storage systems employ delicate fan speed control and SmartCompression to drive down costs. They also provide a collection of management and maintenance tools to simplify operation and maintenance.

- Cost-effectiveness

  Delicate fan speed control

  Dynamically adjusts the fan speed based on storage system temperature, lowering the noise and power consumption while saving device operation costs.
- Ease-of-use
  - DeviceManager

    A tool that is developed based on HTML5 and provides the graphical user interface (GUI) for storage management. It helps you easily manage storage systems through wizard-instructed operations.
  - Integrated management

    Supports VMware vCenter Plug-in and Hyper-V System Center for management. In addition, the storage system supports VMware vStorage APIs for Storage Awareness (VASA), vStorage APIs for Array Integration (VAAI), and Volume Shadow Copy Service (VSS) Provider to facilitate management.
  - Tablet management

    Supports flexible storage system management on a tablet.
  - Various alarm notification methods

    Supports alarm notification by sound, indicator, short message service (SMS), and email. Critical information is sent to users in a timely manner.
  - One-key upgrade tool

    Provides one-click online upgrade for controllers. This upgrade is easy and services remain online and operational during the upgrade process.

Intelligent O&M

The eService cloud intelligent management system (eService for short) improves user O&M capabilities and takes planned maintenance actions to prevent potential risks.

Being authorized by customers, eService monitors device alarms in 24/7 mode. Whenever an alarm is detected, it automatically notifies Huawei technical support center and creates service requests. Huawei service engineers will help customers solve problems in a timely manner.

- eService provides a self-service O&M system for customers, aiming for precise information services.

- Based on HUAWEI CLOUD, the eService cloud system drives O&M activities through big data analytics and artificial intelligence (AI) to identify faults in advance, reduce O&M difficulties, and improve O&M efficiency.
- Data is encrypted for secure transmission. eService can access the customer's system only after being authorized by the customer.
- eService provides 24/7 secure, reliable, and proactive O&M services. SRs can be automatically created.
- Customers can use any PC to access eService at any time and place to check device information.

eService enables the client to work with the cloud system.

- The eService client is deployed on the customer side. It collects alarms on the customer devices and sends them to the eService cloud system for remote maintenance such as remote inspection and log collection.
- The eService cloud system is deployed in Huawei technical support center. It receives device alarms from the eService client 24/7 hours and automatically notifies Huawei technical support personnel of the alarms. It also supports automatic inspection and log collection on the customer devices.

For details, see the *eService Intelligent Cloud Management System User Guide* or access eService at **http://support.eservice.huawei.com**.

Integrated Container Service

SmartContainer is a new feature provided by the OceanStor storage systems based on the current applications of storage products and the development trend of storage technologies. It meets enterprise users' requirements for converged IT applications that integrate computing and storage capabilities, and provides a stable and reliable environment for running application software on storage hosts.

By integrating the container technology on storage systems, the storage resources can be fully utilized to reduce IT infrastructure costs and simplify service configuration. The OceanStor storage systems greatly shorten the rollout period of enterprise services and improve the operation efficiency.

After SmartContainer is enabled, the storage system runs container services and basic services at the same time to combine computing, network, storage, and virtualization resources.

NOTE

OceanStor 5310 does not support SmartContainer.

3 Hardware Architecture

A storage system typically consists of controller enclosures and disk enclosures.

3.1 Device Composition

A storage system consists of controller enclosures and disk enclosures. It provides an intelligent storage platform that features robust reliability, high performance, and large capacity.

Different product models use different types of controller enclosures and disk enclosures, as listed in **Table 3-1**.

Table 3-1 Controller and disk enclosures used by different product models

Product Model	Controller Enclosure	Disk Enclosure
OceanStor 5310	• 2 U controller enclosure (12 disk slots) • 2 U SAS controller enclosure (25 disk slots) • 2 U NVMe controller enclosure (25 disk slots)	• 2 U SAS disk enclosure (25 disk slots) • 4 U SAS disk enclosure (24 disk slots) • 4 U SAS high-density disk enclosure (75 x 3.5-inch disk slots) • 2 U smart NVMe disk enclosure (36 disk slots)
OceanStor 5510 and 5610	• 2 U controller enclosure (12 disk slots) • 2 U controller enclosure (25 disk slots) • 2 U controller enclosure (36 disk slots)	

The following figures show the appearances of the storage devices.

Figure 3-1 2 U controller enclosure (12 disk slots)

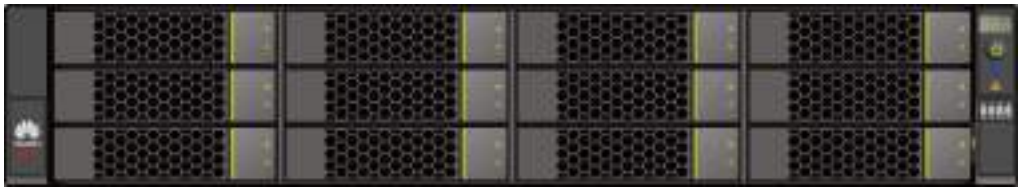


Figure 3-2 2 U SAS controller enclosure (25 disk slots)

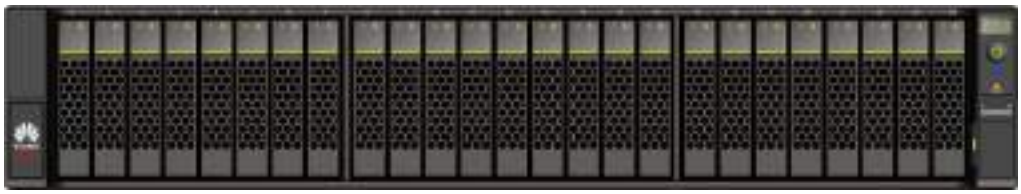


Figure 3-3 2 U NVMe controller enclosure (25 disk slots)

Figure 3-4 2 U controller enclosure (36 disk slots)

Figure 3-5 2 U SAS disk enclosure (25 disk slots)

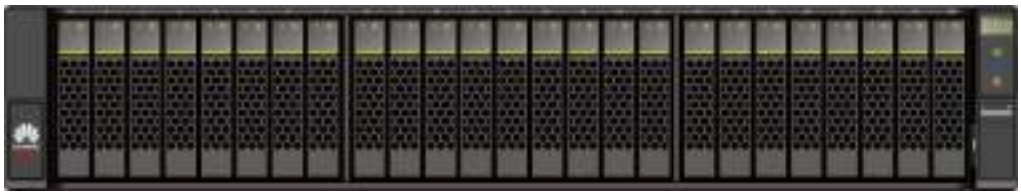


Figure 3-6 4 U SAS disk enclosure (24 disk slots)

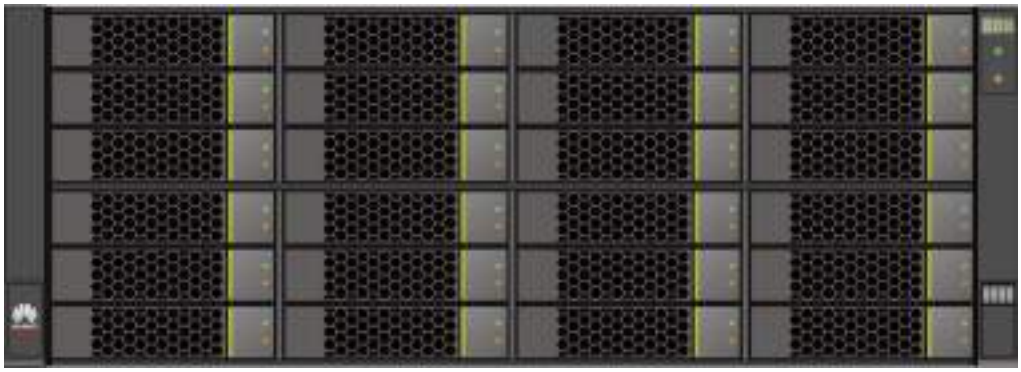


Figure 3-7 High-density disk enclosure

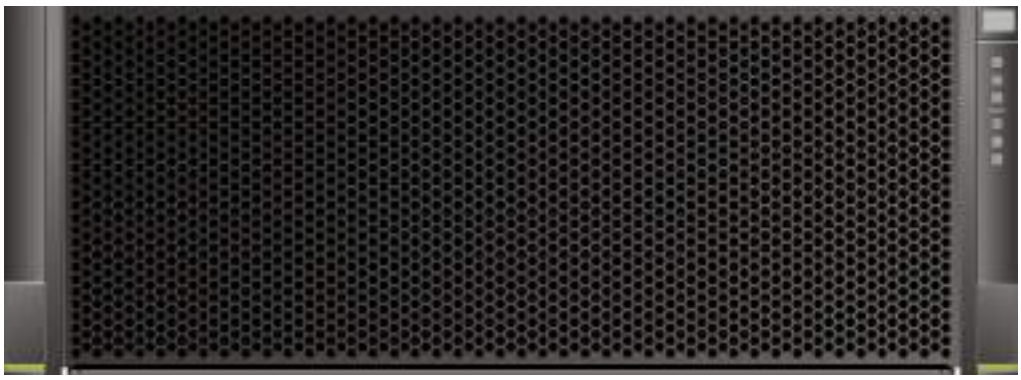


Figure 3-8 2 U smart NVMe disk enclosure (36 disk slots)

NOTE

On the front panel of a 2 U controller enclosure (25 disk slots), the function described by  is reserved, which means the rightmost four slots can house NVMe SSDs.

3.2 3D Interactive Hardware Demonstration

OceanStor storage systems provide new hardware simulation for interactive experience, which supports all-round demonstration of hardware components and manual disassembly, providing details on the internal structure. You can access the demonstration as follows:

1. Log in to **https://support.huawei.com/enterprise/**.
2. Choose **Technical Support** > **Product Support** > **Enterprise Data Center** > **Centralized Storage**.
3. Select the desired product model.
4. Click the **Video** tab and select **3D Demo** in **Type**.

Figure 3-9 Selecting **3D Demo**

5. Select the desired demonstration. A page similar to **Figure 3-10** is displayed.

Figure 3-10 3D interactive demonstration

3.3 2 U Controller Enclosure of OceanStor 5310 (SAS)

This section describes the hardware structure, component functions, front and rear views, and indicators of a controller enclosure.

3.3.1 Overview

The controller enclosure adopts a modular design and consists of a system subrack, controllers (with built-in fans), power modules, BBUs, and disk modules.

Both AC and DC power modules are supported. One controller enclosure supports two controllers.

Overall Structure

Figure 3-11 shows the overall structure and components of a 2 U 25-disk controller enclosure and **Figure 3-12** shows the overall structure and components of a 2 U 12-disk controller enclosure.

Figure 3-11 Overall structure of a 2 U 25-disk controller enclosure

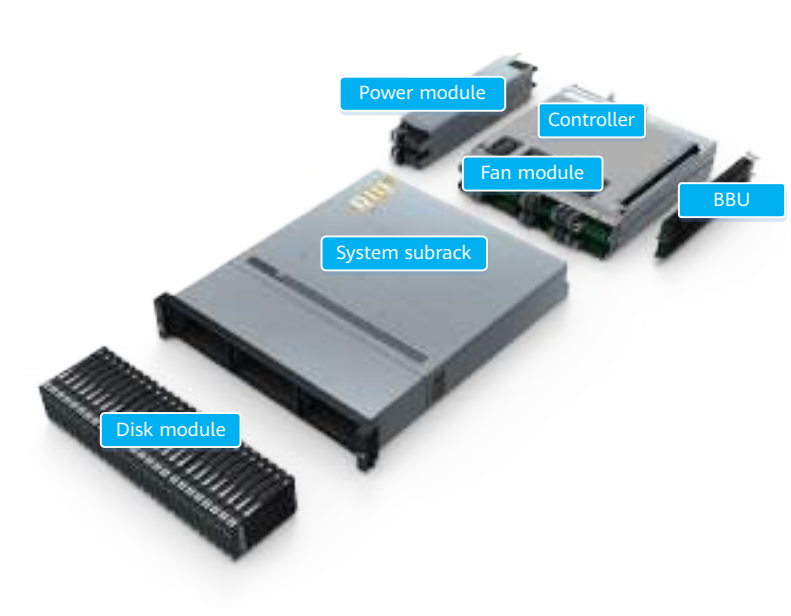
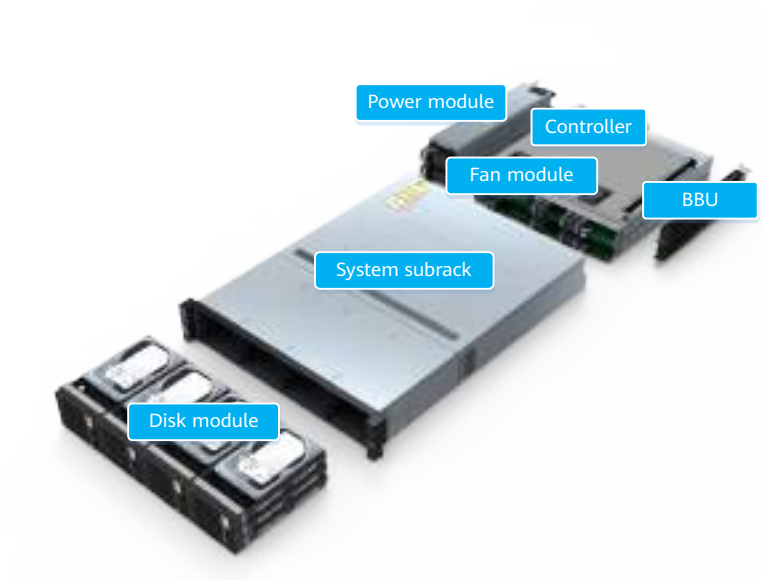


Figure 3-12 Overall structure of a 2 U 12-disk controller enclosure



NOTE

The controllers are A and B from top to bottom. Controllers communicate with each other using internal heartbeat and mirroring links and do not need cable connections.

Front View

Figure 3-13 shows the front view of a 2 U 25-disk controller enclosure and Figure 3-14 shows the front view of a 2 U 12-disk controller enclosure.

Figure 3-13 Front view of a 2 U 25-disk controller enclosure

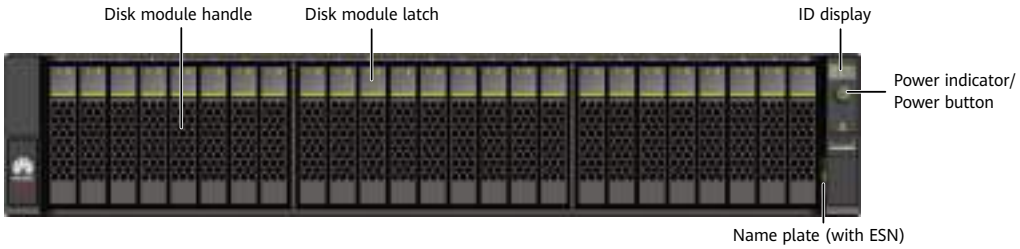


Figure 3-14 Front view of a 2 U 12-disk controller enclosure

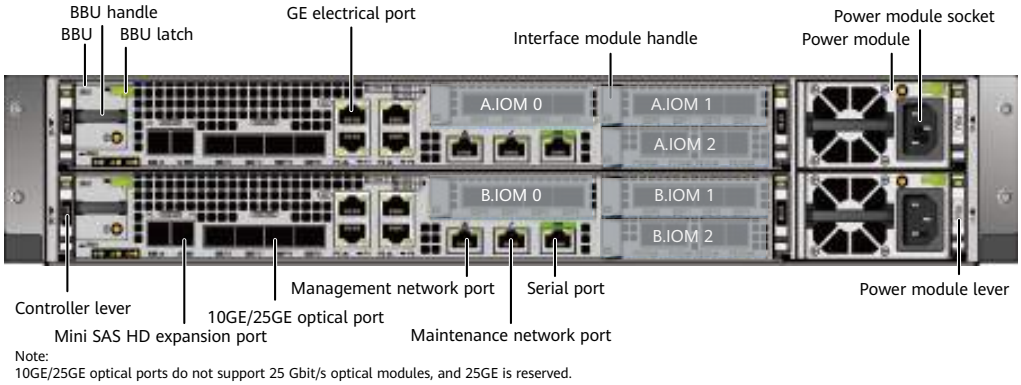
NOTE

- The disk slots of a 2 U 25-disk controller enclosure are numbered 0 to 24 from left to right.
- The disk slots of a 2 U 12-disk controller enclosure are numbered 0 to 11 from left to right and from top to bottom.
- Slots are used to accommodate and secure disks, interface modules, controllers, fan modules, and power modules.
- The nameplate records device information.

Rear View

Figure 3-15 shows the rear view of a controller enclosure.

Figure 3-15 Rear view of a controller enclosure (with AC power modules as an example)



NOTICE

- Only serial cables can be inserted into serial ports. Do not insert network cables into serial ports.
- Do not connect the management network port and maintenance network port to the same LAN or switch to prevent network loops.

NOTE

- The controllers are A and B from top to bottom. Each controller has three interface module slots, which are IOM 0, IOM 1, and IOM 2 from left to right and from top to bottom.
- The rules for installing interface modules on a controller enclosure are as follows:
  - The 12 Gbit/s SAS expansion module can be installed only in slot IOM 2 of each controller, that is, slots A.IOM 2 and B.IOM 2 in the figure.
  - The scale-out interface module must be installed in slot IOM 1.
  - Install back-end expansion modules in a sequence of IOM 2 > IOM 1 > IOM 0. Install front-end interface modules in a sequence of IOM 0 > IOM 1 > IOM 2.
- Onboard ports include GE ports, 10GE/25GE optical ports (do not support 25 Gbit/s optical modules, and 25GE is reserved), and mini SAS HD expansion ports. The storage system does not support optical modules purchased by the customer elsewhere. Use optical modules that match the storage interface modules.
- The maintenance network port is used for special management and maintenance only by Huawei technical support engineers in emergency. The initial IP address of the maintenance network port is 172.31.128.101 or 172.31.128.102. The default subnet mask is 255.255.0.0. You are advised to connect only the management network port to the network.

Hardware Specifications

Table 3-2 lists the dimensions, weight, and power specifications of the controller enclosure. For more specifications, refer to Specifications Query (**https://support-it.huawei.com/spec/#/home**).

Table 3-2 Hardware specifications

Item	Specifications
Dimensions (H x W x D)	• 86.1 mm x 447 mm x 520 mm (enclosure that uses 2.5-inch disks) • 86.1 mm x 447 mm x 600 mm (enclosure that uses 3.5-inch disks)
Weight (excluding disks and auxiliary materials such as guide rails and cables)	• 23.75 kg (enclosure that uses 2.5-inch disks) • 24.1 kg (enclosure that uses 3.5-inch disks)
AC power voltage and rated current	• 2000 W power supply (supporting 110 V dual-live-wire input (2W +PE)), 200 V to 240 V AC ±10%, 10 A, single-phase, 50/60 Hz • 900 W power supply (supporting 110 V dual-live-wire input (2W+PE) and 110 V single-live-wire input), 100 V to 240 V AC ±10%, 10 A, single-phase, 50/60 Hz
High-voltage DC (not supported in North America and Canada)	800 W power supply (240 V DC input), 192 V to 288 V, 10 A

Item	Specifications
Low-voltage DC	1200 W power supply (supporting –48 V/–60 V DC input), –38.4 V to –72 V DC, 32 A

3.3.2 Component Description

This section provides the detailed illustration and description for each component.

3.3.2.1 System Subrack

The system subrack houses a midplane that provides reliable connections for interface modules and distributes power and signals to inner modules.

Appearance

Figure 3-16 shows the appearance of a system subrack.

Figure 3-16 System subrack

3.3.2.2 Controller

A controller is the core component of a storage system. It processes storage services, receives configuration management commands, saves configuration data, connects to disks, and saves critical data onto coffer disks.

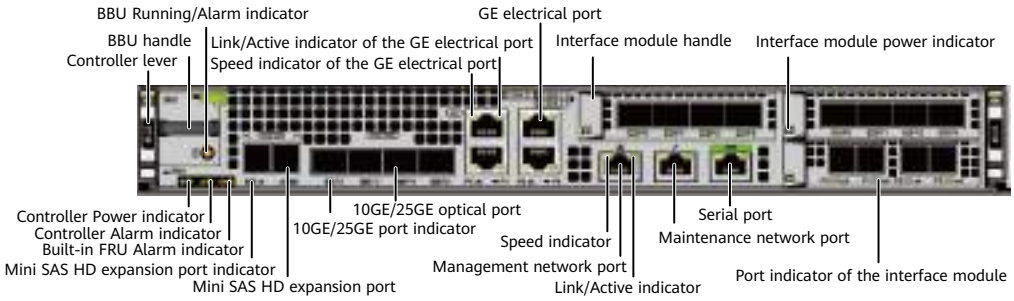
NOTE

Each controller has a built-in disk to store system data. If a power failure occurs, this disk also stores cache data. The built-in disks on different controllers are redundant for each other.

Ports

Figure 3-17 describes the ports of a controller.

Figure 3-17 Ports of a controller



NOTICE

Only serial cables can be inserted into the serial ports. Do not insert network cables into the serial ports.

Indicators

Table 3-3 describes the states and meanings of the indicators on a controller after it is powered on.

Table 3-3 Indicators on a controller

Indicator	Status and Description
10GE/25GE port indicator	• Steady blue: The speed is the highest. • Blinking blue (2 Hz): The port is transmitting data at the highest speed. • Steady green: The speed is not the highest. • Blinking green (2 Hz): The port is transmitting data, but not at the highest speed. • Steady yellow: The optical module or cable is faulty or not supported by the port. • Blinking yellow (2 Hz): The port is being located. • Off: The port is not connected.
Link/Active indicator of the management network port	• Steady green: The port is connected properly. • Blinking green (2 Hz): Data is being transmitted. • Off: The connection is abnormal.
Speed indicator of the management network port	• Steady yellow: Data is being transmitted at the highest speed. • Off: The speed is not the highest.

Indicator	Status and Description
Power indicator of the controller	• Steady green: The controller is on. • Blinking green (0.5 Hz): The controller is being powered on and booting the BIOS. • Blinking green (2 Hz): The controller is booting the operating system or being powered off. • Off: The controller is absent or powered off.
Alarm indicator of the controller	• Steady yellow: An alarm is reported on the controller. • Off: The controller is working properly.
Built-in FRU Alarm indicator	• Steady yellow: A built-in FRU (fan module) of the controller is faulty. • Off: The built-in FRUs of the controller are normal.
Indicator of the mini SAS HD expansion port	• Steady blue: The port transmission rate is 4 x 12 Gbit/s. • Steady green: The port transmission rate is 4 x 3 Gbit/s or 4 x 6 Gbit/s. • Steady yellow: The port is faulty. • Off: The port is not connected.
Link/Active indicator of the GE electrical port	• Steady green: The link to the application server is normal. • Blinking green (2 Hz): Data is being transmitted. • Off: The link to the application server is down or no link exists.
Speed indicator of the GE electrical port	• Steady yellow: The data transmission speed between the storage system and the application server is 1 Gbit/s. • Off: The data transmission speed between the storage system and the application server is lower than 1 Gbit/s.

3.3.2.3 BBU

BBUs supply power to the storage system in the event of an external power supply failure to protect data in the storage system. When the external power supplies are normal, the BBUs are standing by. If a BBU is faulty, it can be isolated without affecting the normal running of the storage system. If a power failure occurs, BBUs ensure that the storage system writes cached data to the built-in disks of the controllers, preventing data loss. After the external power supply resumes, the driver reads data from the built-in disks of the controllers to the cache. In a system using the lithium batteries, the battery capacity is updated and detected by charging and discharging the batteries. In this way, the problems can be detected

in advance that the battery capacity attenuates, the batteries fail to meet the power backup requirements of the system, and thus the data backup fails when the batteries are not used for a long time. Then, the reliability of data protection upon the system power failure can be improved.

Appearance

Figure 3-18 and Figure 3-19 show the appearance and front view of a BBU.

Figure 3-18 Appearance of a BBU

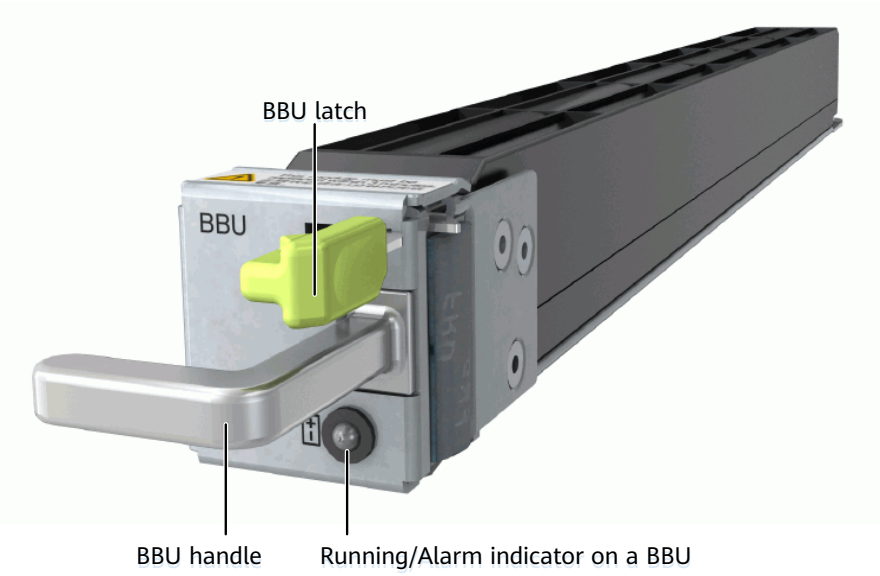
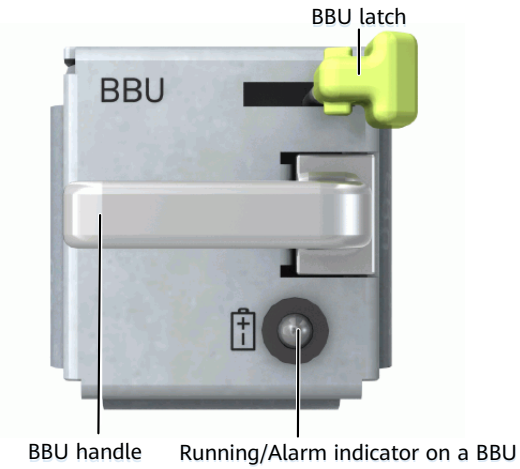


Figure 3-19 Front view of a BBU



Indicators

Table 3-4 describes the indicator on a BBU.

Table 3-4 Indicator on a BBU

Indicator	Status and Description
Running/Alarm indicator of the BBU	• Steady green: The BBU is fully charged. • Blinking green (1 Hz): The BBU is being charged. • Blinking green (4 Hz): The BBU is being discharged. • Steady yellow: The BBU is faulty. • Off: The module is powered off or hot swappable.

3.3.2.4 Fan Module

Fan modules dissipate heat from the system, allowing the controller enclosure to operate normally at maximum power.

Appearance

Figure 3-20 shows the appearance of a fan module.

Figure 3-20 Appearance of a fan module

Indicators

The fan modules are located inside controllers. You can determine the running status of the fan modules by observing the Built-in FRU Alarm indicator or checking alarm information on the management UI. For the states and meanings of the Built-in FRU Alarm indicator, see **3.3.3 Indicator Description**.

3.3.2.5 Power Module

Power modules allow the controller enclosure to work properly at maximum power. Both AC and DC power modules are supported.

Each controller enclosure has two power modules (PSU 0 and PSU 1) to supply power to controllers A and B. The two power modules form a power plane and are redundant of each other. For reliability purposes, it is recommended that you connect PSU 0 and PSU 1 to different PDUs.

Appearance

Figure 3-21 and **Figure 3-22** show the appearance of a power module.

Figure 3-21 AC power module

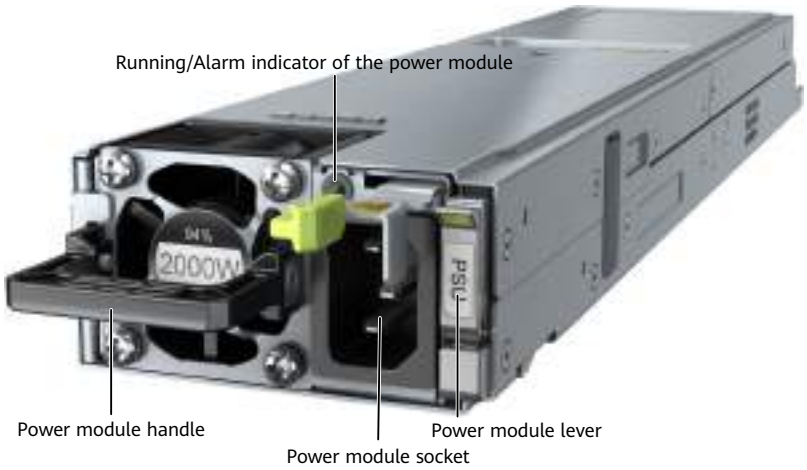


Figure 3-22 DC power module

Indicators

Table 3-5 describes the indicator on a power module.

Table 3-5 Indicator on a power module

Indicator	Status and Description
Running/Alarm indicator of the power module	• Steady green: The power input is normal. • Blinking green (1 Hz): The power input is normal but the device is powered off. • Blinking green (4 Hz): The power module is being upgraded online. • Steady yellow: The power module is faulty. • Off: There is no external power input.

3.3.2.6 Disk Module

Disk modules provide storage capacity for a storage system. Disk modules can function as system coffer disks to save service data, system data, and cache data.

Appearance

Figure 3-23 shows the appearance of a 2.5-inch disk module. **Figure 3-24** shows the appearance of a 3.5-inch disk module.

Figure 3-23 2.5-inch disk module

Figure 3-24 3.5-inch disk module

Indicators

Table 3-6 describes indicators on a disk module.

Table 3-6 Indicators on a disk module

Indicator	Status and Description
Running indicator of the disk module	• Steady green: The disk module is working properly. • Blinking green (4 Hz or higher): Data is being read and written on the disk module. • Off: The disk module is powered off or incorrectly powered on.
Alarm/Location indicator of the disk module	• Steady yellow: The disk module is faulty. • Blinking yellow (2 Hz): The disk module is being located. • Off: The disk module is working properly or hot swappable.

3.3.3 Indicator Description

After a controller enclosure is powered on, you can check the current operating status of the controller enclosure by observing its indicators.

Indicators on the Front Panel

Figure 3-25 shows the indicators on the front panel of a 2 U 25-disk controller enclosure and Figure 3-26 shows the indicators on the front panel of a 2 U 12-disk controller enclosure.

Figure 3-25 Indicators on the front panel of a 2 U 25-disk controller enclosure

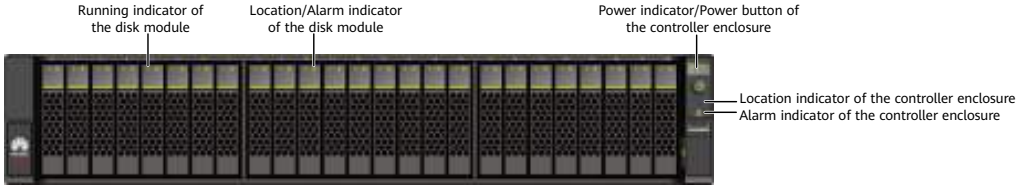


Figure 3-26 Indicators on the front panel of a 2 U 12-disk controller enclosure

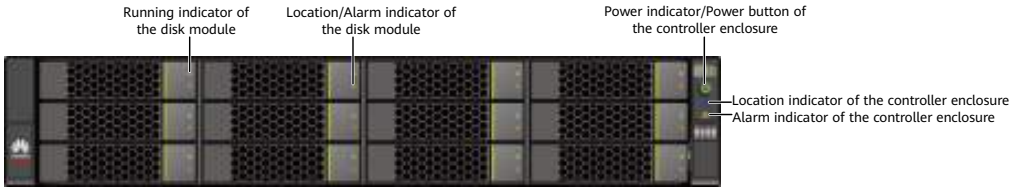


Table 3-7 describes the meanings of the indicators on the front panel of a controller enclosure.

Table 3-7 Meanings of the indicators on the front panel of a controller enclosure

Module	Indicator	Status and Description
Disk module	Running indicator of the disk module	• Steady green: The disk module is working properly. • Blinking green (4 Hz or higher): Data is being read and written on the disk module. • Off: The disk module is powered off or incorrectly powered on.
	Alarm/Location indicator of the disk module	• Steady yellow: The disk module is faulty. • Blinking yellow (2 Hz): The disk module is being located. • Off: The disk module is working properly or hot swappable.
System subrack	Location indicator of the controller enclosure	• Blinking blue (2 Hz): The controller enclosure is being located. • Off: The controller enclosure is not located.

Module	Indicator	Status and Description
	Alarm indicator of the controller enclosure	• Steady yellow: A major or critical alarm is reported on the storage system. • Off: The storage system is running properly.
	Power indicator/Power button of the controller enclosure	• Steady green: The controller enclosure is on. • Blinking green (0.5 Hz): The controller enclosure is being powered on. • Blinking green (1 Hz): The controller enclosure is in the burn-in state. • Blinking green (2 Hz): The controller enclosure is booting the operating system or being powered off. • Off: The controller enclosure is off or powered by the BBUs.

Indicators on the Rear Panel

Figure 3-27 shows the indicators on the rear panel of a controller enclosure.

Figure 3-27 Indicators on the rear panel of a controller enclosure (with AC power modules as an example)

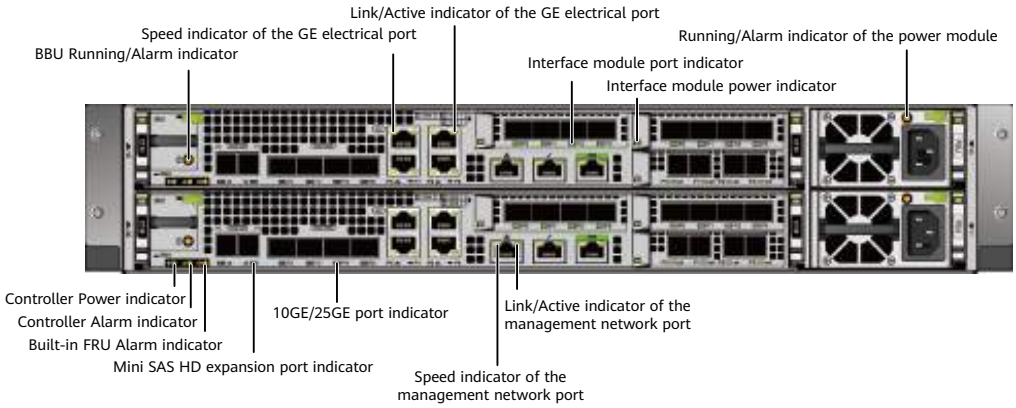


Table 3-8 describes the meanings of the indicators on the rear panel of a controller enclosure.

Table 3-8 Meanings of the indicators on the rear panel of a controller enclosure

Module	Indicator	Status and Description
Interface module	Power indicator of the interface module	For the states and meanings of the indicators on the interface modules supported by a controller, see **3.6 Interface Module**.
	Port indicator	
Power module	Running/ Alarm indicator of the power module	• Steady green: The power input is normal. • Blinking green (1 Hz): The power input is normal but the device is powered off. • Blinking green (4 Hz): The power module is being upgraded online. • Steady yellow: The power module is faulty. • Off: There is no external power input.
Controller	10GE/25GE port indicator	• Steady blue: The speed is the highest. • Blinking blue (2 Hz): The port is transmitting data at the highest speed. • Steady green: The speed is not the highest. • Blinking green (2 Hz): The port is transmitting data, but not at the highest speed. • Steady yellow: The optical module or cable is faulty or not supported by the port. • Blinking yellow (2 Hz): The port is being located. • Off: The port is not connected.
	Link/Active indicator of the management network port	• Steady green: The port is connected properly. • Blinking green (2 Hz): Data is being transmitted. • Off: The connection is abnormal.
	Speed indicator of the management network port	• Steady yellow: Data is being transmitted at the highest speed. • Off: The speed is not the highest.
	Power indicator of the controller	• Steady green: The controller is on. • Blinking green (0.5 Hz): The controller is being powered on and booting the BIOS. • Blinking green (2 Hz): The controller is booting the operating system or being powered off. • Off: The controller is absent or powered off.

Module	Indicator	Status and Description
	Alarm indicator of the controller	• Steady yellow: An alarm is reported on the controller. • Off: The controller is working properly.
	Built-in FRU Alarm indicator	• Steady yellow: A built-in FRU (fan module) of the controller is faulty. • Off: The built-in FRUs of the controller are normal.
	Indicator of the mini SAS HD expansion port	• Steady blue: The port transmission rate is 4 x 12 Gbit/s. • Steady green: The port transmission rate is 4 x 3 Gbit/s or 4 x 6 Gbit/s. • Steady yellow: The port is faulty. • Off: The port is not connected.
	Link/Active indicator of the GE electrical port	• Steady green: The link to the application server is normal. • Blinking green (2 Hz): Data is being transmitted. • Off: The link to the application server is down or no link exists.
	Speed indicator of the GE electrical port	• Steady yellow: The data transmission speed between the storage system and the application server is 1 Gbit/s. • Off: The data transmission speed between the storage system and the application server is lower than 1 Gbit/s.
BBU	Running/ Alarm indicator of the BBU	• Steady green: The BBU is fully charged. • Blinking green (1 Hz): The BBU is being charged. • Blinking green (4 Hz): The BBU is being discharged. • Steady yellow: The BBU is faulty. • Off: The module is powered off or hot swappable.

3.4 2 U Controller Enclosure of OceanStor 5310 (NVMe)

This section describes the hardware structure, component functions, front and rear views, and indicators of a controller enclosure.

3.4.1 Overview

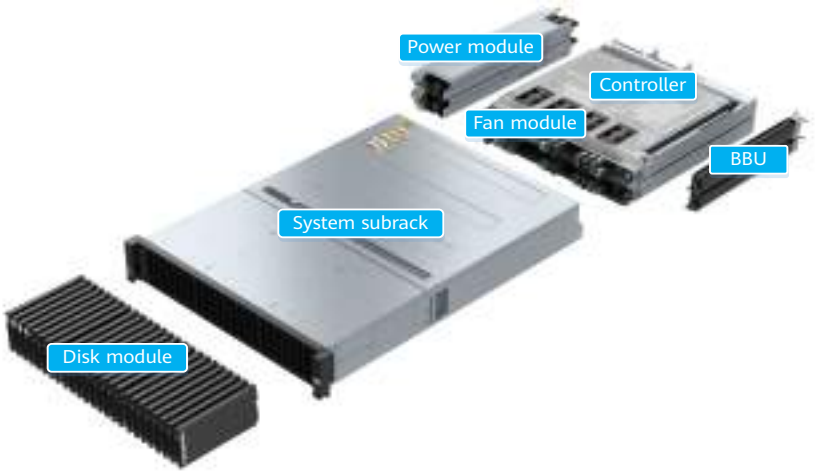
The controller enclosure adopts a modular design and consists of a system subrack, controllers (with built-in fans), power modules, BBUs, and disk modules.

Both AC and DC power modules are supported. One controller enclosure supports two controllers.

Overall Structure

Figure 3-28 shows the overall structure and components of a controller enclosure.

Figure 3-28 Overall structure of a controller enclosure



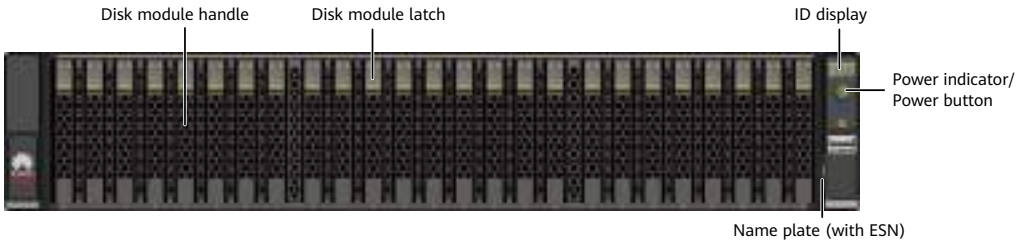
NOTE

The controllers are A and B from top to bottom. Controllers communicate with each other using internal heartbeat and mirroring links and do not need cable connections.

Front View

Figure 3-29 shows the front view of a controller enclosure.

Figure 3-29 Front view of a controller enclosure



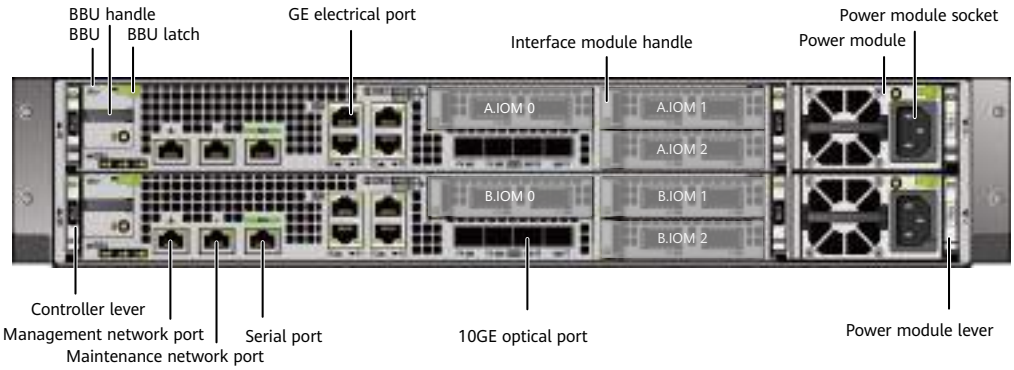
NOTE

- The disk slots of a 2 U 25-disk controller enclosure are numbered 0 to 24 from left to right.
- Slots are used to accommodate and secure disks, interface modules, controllers, fan modules, and power modules.
- The nameplate records device information.

Rear View

Figure 3-30 shows the rear view of a controller enclosure.

Figure 3-30 Rear view of a controller enclosure (with AC power modules as an example)



NOTICE

- Only serial cables can be inserted into the serial ports. Do not insert network cables into the serial ports.
- Do not connect the management network port and maintenance network port to the same LAN or switch to prevent network loops.

NOTE

- The controllers are A and B from top to bottom. Each controller has three interface module slots, which are IOM 0, IOM 1, and IOM 2 from left to right and from top to bottom.
- The rules for installing interface modules on a controller enclosure are as follows:
  - The 12 Gbit/s SAS expansion module can be installed only in slot IOM 2 of each controller, that is, slots A.IOM 2 and B.IOM 2 in the figure.
  - The scale-out interface module must be installed in slot IOM 1.
  - Install back-end expansion modules in a sequence of IOM 2 > IOM 1 > IOM 0. Install front-end interface modules in a sequence of IOM 0 > IOM 1 > IOM 2.
- Onboard ports include GE and 10GE ports. The storage system does not support optical modules purchased by the customer elsewhere. Use optical modules that match the storage interface modules.
- The maintenance network port is used for special management and maintenance only by Huawei technical support engineers in emergency. The initial IP address of the maintenance network port is 172.31.128.101 or 172.31.128.102. The default subnet mask is 255.255.0.0. You are advised to connect only the management network port to the network.

Hardware Specifications

Table 3-9 lists the dimensions, weight, and power specifications of the controller enclosure. For more specifications, refer to Specifications Query (**https://support-it.huawei.com/spec/#/home**).

Table 3-9 Hardware specifications

Item	Specifications
Dimensions (H x W x D)	86.1 mm x 447 mm x 620 mm
Weight (excluding disks and auxiliary materials such as guide rails and cables)	21.25 kg
AC power voltage and rated current	• 2000 W power supply (supporting 110 V dual-live-wire input (2W +PE)), 200 V to 240 V AC ±10%, 10 A, single-phase, 50/60 Hz • 900 W power supply (supporting 110 V dual-live-wire input (2W+PE) and 110 V single-live-wire input), 100 V to 240 V AC ±10%, 10 A, single-phase, 50/60 Hz
High-voltage DC (not supported in North America and Canada)	800 W power supply (240 V DC input), 192 V to 288 V, 10 A
Low-voltage DC	1200 W power supply (supporting –48 V/–60 V DC input), –38.4 V to –72 V DC, 32 A

3.4.2 Component Description

This section provides the detailed illustration and description for each component.

3.4.2.1 System Subrack

The system subrack houses a midplane that provides reliable connections for interface modules and distributes power and signals to inner modules.

Appearance

Figure 3-31 shows the appearance of a system subrack.

Figure 3-31 System subrack

3.4.2.2 Controller

A controller is the core component of a storage system. It processes storage services, receives configuration management commands, saves configuration data, connects to disks, and saves critical data onto coffer disks.

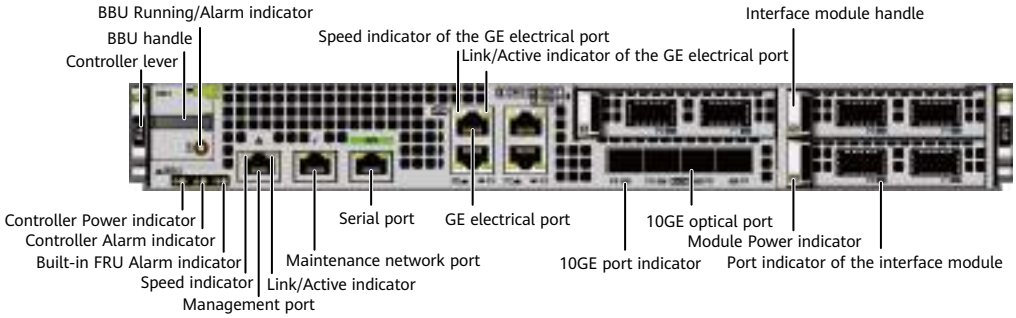
NOTE

Each controller has a built-in disk to store system data. If a power failure occurs, this disk also stores cache data. The built-in disks on different controllers are redundant for each other.

Ports

Figure 3-32 describes the ports of a controller.

Figure 3-32 Ports of a controller



NOTICE

Only serial cables can be inserted into the serial ports. Do not insert network cables into the serial ports.

Indicators

Table 3-10 describes the states and meanings of the indicators on a controller after it is powered on.

Table 3-10 Indicators on a controller

Indicator	Status and Description
10GE port indicator	• Steady green: The speed is the highest. • Blinking green (2 Hz): The port is transmitting data at the highest speed. • Steady yellow: The optical module or cable is faulty or not supported by the port. • Blinking yellow (2 Hz): The port is being located. • Off: The port is not connected.

Indicator	Status and Description
Link/Active indicator of the management network port	• Steady green: The port is connected properly. • Blinking green (2 Hz): Data is being transmitted. • Off: The connection is abnormal.
Speed indicator of the management network port	• Steady yellow: Data is being transmitted at the highest speed. • Off: The speed is not the highest.
Power indicator of the controller	• Steady green: The controller is on. • Blinking green (0.5 Hz): The controller is being powered on and booting the BIOS. • Blinking green (2 Hz): The controller is booting the operating system or being powered off. • Off: The controller is absent or powered off.
Alarm indicator of the controller	• Steady yellow: An alarm is reported on the controller. • Off: The controller is working properly.
Built-in FRU Alarm indicator	• Steady yellow: A built-in FRU (fan module) of the controller is faulty. • Off: The built-in FRUs of the controller are normal.
Link/Active indicator of the GE electrical port	• Steady green: The link to the application server is normal. • Blinking green (2 Hz): Data is being transmitted. • Off: The link to the application server is down or no link exists.
Speed indicator of the GE electrical port	• Steady yellow: The data transmission speed between the storage system and the application server is 1 Gbit/s. • Off: The data transmission speed between the storage system and the application server is lower than 1 Gbit/s.

3.4.2.3 BBU

BBUs supply power to the storage system in the event of an external power supply failure to protect data in the storage system. When the external power supplies are normal, the BBUs are standing by. If a BBU is faulty, it can be isolated without affecting the normal running of the storage system. If a power failure occurs, BBUs ensure that the storage system writes cached data to the built-in disks of the controllers, preventing data loss. After the external power supply resumes, the driver reads data from the built-in disks of the controllers to the cache. In a

system using the lithium batteries, the battery capacity is updated and detected by charging and discharging the batteries. In this way, the problems can be detected in advance that the battery capacity attenuates, the batteries fail to meet the power backup requirements of the system, and thus the data backup fails when the batteries are not used for a long time. Then, the reliability of data protection upon the system power failure can be improved.

Appearance

Figure 3-33 and **Figure 3-34** show the appearance and front view of a BBU.

Figure 3-33 Appearance of a BBU

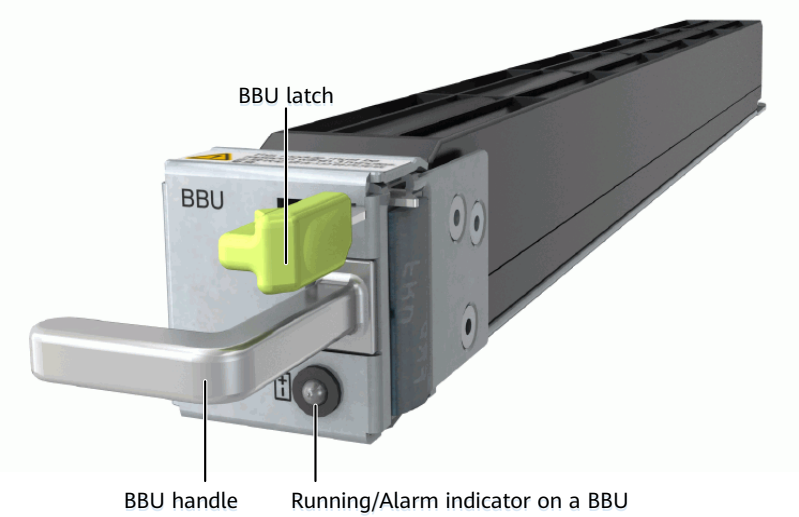
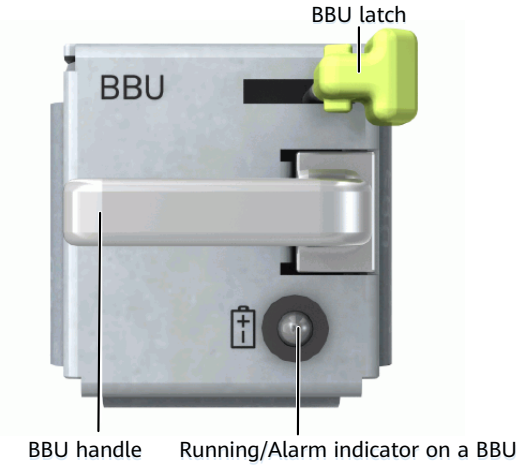


Figure 3-34 Front view of a BBU



Indicators

Table 3-11 describes the indicator on a BBU.

Table 3-11 Indicator on a BBU

Indicator	Status and Description
Running/Alarm indicator of the BBU	• Steady green: The BBU is fully charged. • Blinking green (1 Hz): The BBU is being charged. • Blinking green (4 Hz): The BBU is being discharged. • Steady yellow: The BBU is faulty. • Off: The module is powered off or hot swappable.

3.4.2.4 Fan Module

Fan modules dissipate heat from the system, allowing the controller enclosure to operate normally at maximum power.

Appearance

Figure 3-35 shows the appearance of a fan module.

Figure 3-35 Appearance of a fan module

Indicators

The fan modules are located inside controllers. You can determine the running status of the fan modules by observing the Built-in FRU Alarm indicator or checking alarm information on the management UI. For the states and meanings of the Built-in FRU Alarm indicator, see **3.4.3 Indicator Description**.

3.4.2.5 Power Module

Power modules allow the controller enclosure to work properly at maximum power. Both AC and DC power modules are supported.

Each controller enclosure has two power modules (PSU 0 and PSU 1) to supply power to controllers A and B. The two power modules form a power plane and are redundant of each other. For reliability purposes, it is recommended that you connect PSU 0 and PSU 1 to different PDUs.

Appearance

Figure 3-36 and **Figure 3-37** show the appearance of a power module.

Figure 3-36 AC power module

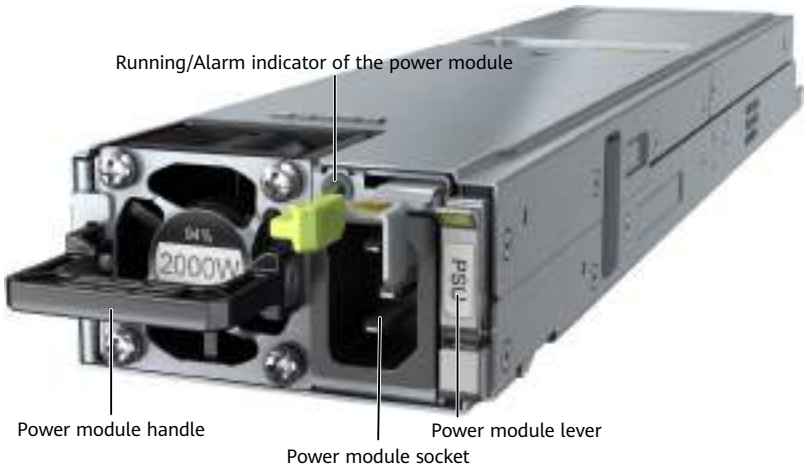


Figure 3-37 DC power module

Indicators

Table 3-12 describes the indicator on a power module.

Table 3-12 Indicator on a power module

Indicator	Status and Description
Running/Alarm indicator of the power module	• Steady green: The power input is normal. • Blinking green (1 Hz): The power input is normal but the device is powered off. • Blinking green (4 Hz): The power module is being upgraded online. • Steady yellow: The power module is faulty. • Off: There is no external power input.

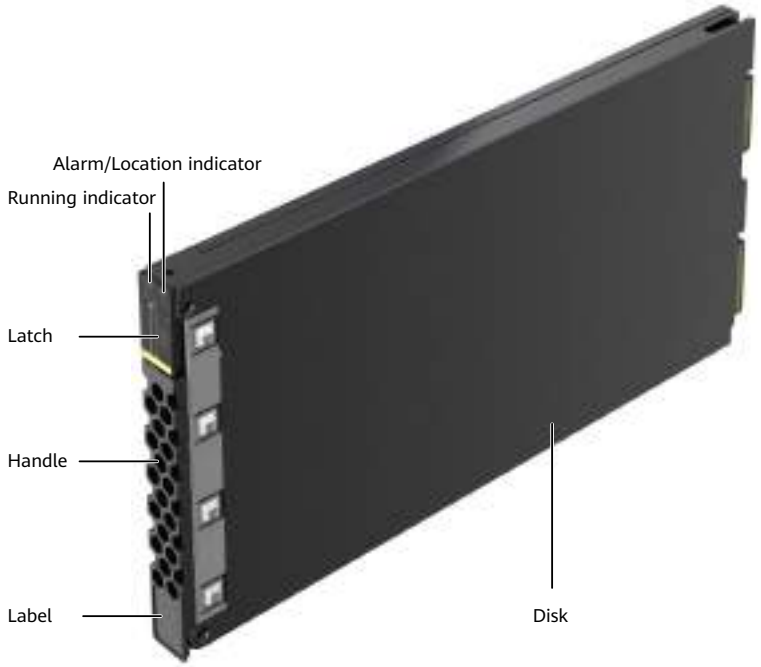
3.4.2.6 Disk Module

Disk modules provide storage capacity for a storage system. Disk modules can function as system coffer disks to save service data, system data, and cache data.

Appearance

Figure 3-38 shows the appearance of a palm-sized NVMe SSD.

Figure 3-38 Palm-sized NVMe SSD



Indicators

Table 3-13 describes indicators on a disk module.

Table 3-13 Indicators on a disk module

Indicator	Status and Description
Running indicator of the disk module	• Steady green: The disk module is working properly. • Blinking green (4 Hz or higher): Data is being read and written on the disk module. • Off: The disk module is powered off or incorrectly powered on.
Alarm/Location indicator of the disk module	• Steady yellow: The disk module is faulty. • Blinking yellow (2 Hz): The disk module is being located. • Off: The disk module is working properly or hot swappable.

3.4.3 Indicator Description

After a controller enclosure is powered on, you can check the current operating status of the controller enclosure by observing its indicators.

Indicators on the Front Panel

Figure 3-39 shows the indicators on the front panel of a controller enclosure.

Figure 3-39 Indicators on the front panel of a controller enclosure

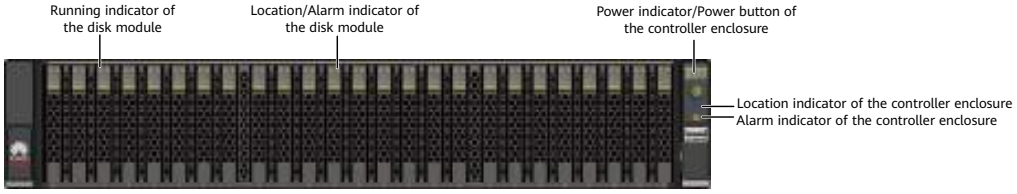


Table 3-14 describes the meanings of the indicators on the front panel of a controller enclosure.

Table 3-14 Meanings of the indicators on the front panel of a controller enclosure

Module	Indicator	Status and Description
Disk module	Running indicator of the disk module	• Steady green: The disk module is working properly. • Blinking green (4 Hz or higher): Data is being read and written on the disk module. • Off: The disk module is powered off or incorrectly powered on.

Module	Indicator	Status and Description
	Alarm/Location indicator of the disk module	• Steady yellow: The disk module is faulty. • Blinking yellow (2 Hz): The disk module is being located. • Off: The disk module is working properly or hot swappable.
System subrack	Location indicator of the controller enclosure	• Blinking blue (2 Hz): The controller enclosure is being located. • Off: The controller enclosure is not located.
	Alarm indicator of the controller enclosure	• Steady yellow: A major or critical alarm is reported on the storage system. • Off: The storage system is running properly.
	Power indicator/Power button of the controller enclosure	• Steady green: The controller enclosure is on. • Blinking green (0.5 Hz): The controller enclosure is being powered on. • Blinking green (1 Hz): The controller enclosure is in the burn-in state. • Blinking green (2 Hz): The controller enclosure is booting the operating system or being powered off. • Off: The controller enclosure is off or powered by the BBUs.

Indicators on the Rear Panel

Figure 3-40 shows the indicators on the rear panel of a controller enclosure.

Figure 3-40 Indicators on the rear panel of a controller enclosure (with AC power modules as an example)

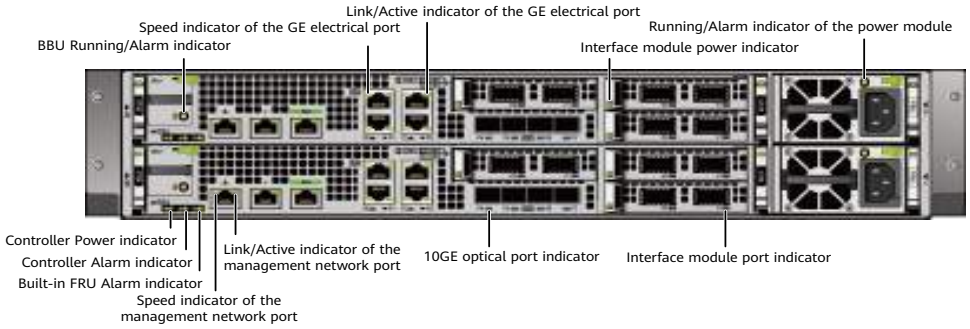


Table 3-15 describes the meanings of the indicators on the rear panel of a controller enclosure.

Table 3-15 Meanings of the indicators on the rear panel of a controller enclosure

Module	Indicator	Status and Description
Interface module	Power indicator of the interface module	For the states and meanings of the indicators on the interface modules supported by a controller, see 3.4.3 Indicator Description.
	Port indicator	
Power module	Running/ Alarm indicator of the power module	• Steady green: The power input is normal. • Blinking green (1 Hz): The power input is normal but the device is powered off. • Blinking green (4 Hz): The power module is being upgraded online. • Steady yellow: The power module is faulty. • Off: There is no external power input.
Controller	10GE optical port indicator	• Steady green: The speed is the highest. • Blinking green (2 Hz): The port is transmitting data at the highest speed. • Steady yellow: The optical module or cable is faulty or not supported by the port. • Blinking yellow (2 Hz): The port is being located. • Off: The port is not connected.
	Link/Active indicator of the management network port	• Steady green: The port is connected properly. • Blinking green (2 Hz): Data is being transmitted. • Off: The connection is abnormal.

Module	Indicator	Status and Description
	Speed indicator of the management network port	• Steady yellow: Data is being transmitted at the highest speed. • Off: The speed is not the highest.
	Power indicator of the controller	• Steady green: The controller is on. • Blinking green (0.5 Hz): The controller is being powered on and booting the BIOS. • Blinking green (2 Hz): The controller is booting the operating system or being powered off. • Off: The controller is absent or powered off.
	Alarm indicator of the controller	• Steady yellow: An alarm is reported on the controller. • Off: The controller is working properly.
	Built-in FRU Alarm indicator	• Steady yellow: A built-in FRU (fan module) of the controller is faulty. • Off: The built-in FRUs of the controller are normal.
	Link/Active indicator of the GE electrical port	• Steady green: The link to the application server is normal. • Blinking green (2 Hz): Data is being transmitted. • Off: The link to the application server is down or no link exists.
	Speed indicator of the GE electrical port	• Steady yellow: The data transmission speed between the storage system and the application server is 1 Gbit/s. • Off: The data transmission speed between the storage system and the application server is lower than 1 Gbit/s.
BBU	Running/ Alarm indicator of the BBU	• Steady green: The BBU is fully charged. • Blinking green (1 Hz): The BBU is being charged. • Blinking green (4 Hz): The BBU is being discharged. • Steady yellow: The BBU is faulty. • Off: The module is powered off or hot swappable.

3.5 2 U Controller Enclosure of OceanStor 5510 and 5610

This section describes a controller enclosure in terms of its hardware structure, component functions, front and rear views, and indicators.

3.5.1 Overview

The controller enclosure adopts a modular design and consists of a system subrack, controllers (with built-in fans), power-BBU modules, and disk modules.

Both AC and DC power modules are supported. One controller enclosure supports two controllers.

Overall Structure

Figure 3-41, **Figure 3-42**, and **Figure 3-43** show the overall structures and components of a 2 U 25-disk controller enclosure, a 2 U 12-disk controller enclosure, and a 2 U 36-disk controller enclosure respectively.

Figure 3-41 Overall structure of a 2 U 25-disk controller enclosure

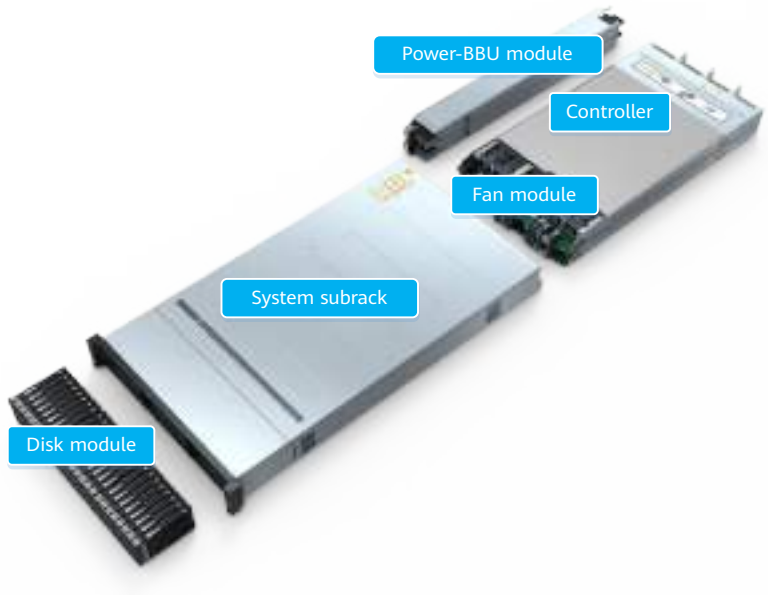


Figure 3-42 Overall structure of a 2 U 12-disk controller enclosure

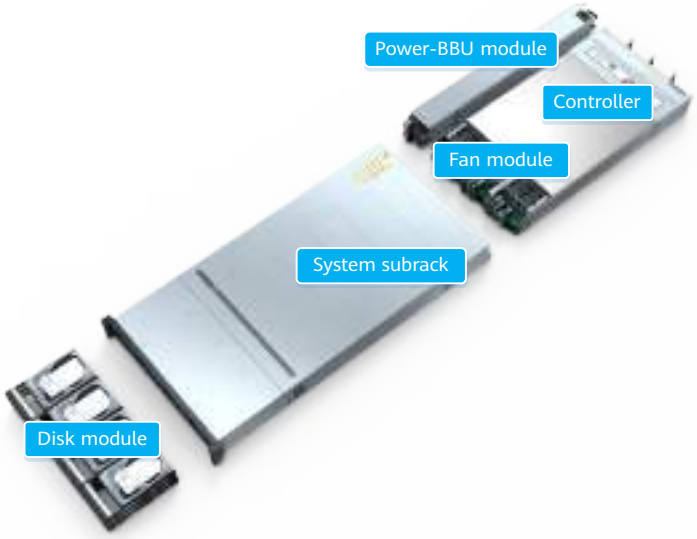
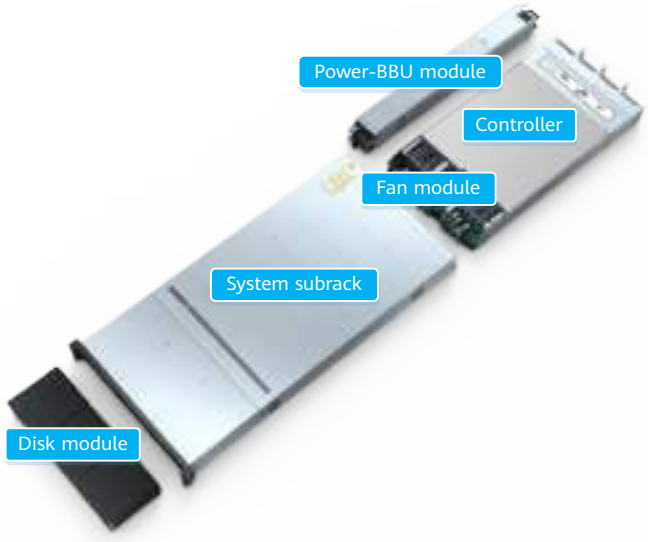


Figure 3-43 Overall structure of a 2 U 36-disk controller enclosure



NOTE

The controllers are A and B from top to bottom. Controllers communicate with each other using internal heartbeat and mirroring links and do not need cable connections.

Front View

Figure 3-44, Figure 3-45, and Figure 3-46 show the front views of a 2 U 25-disk controller enclosure, a 2 U 12-disk controller enclosure, and a 2 U 36-disk controller enclosure respectively.

Figure 3-44 Front view of a 2 U 25-disk controller enclosure

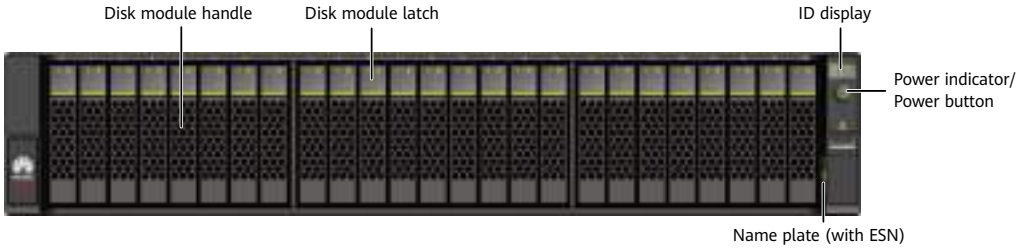
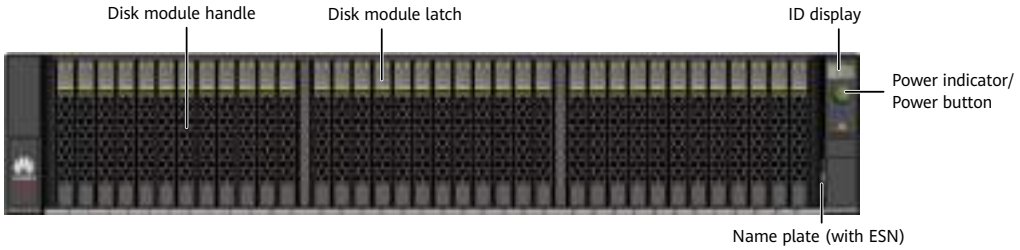


Figure 3-45 Front view of a 2 U 12-disk controller enclosure

Figure 3-46 Front view of a 2 U 36-disk controller enclosure



NOTE

- The disk slots of a 2 U 25-disk controller enclosure are numbered 0 to 24 from left to right.
- The disk slots of a 2 U 12-disk controller enclosure are numbered 0 to 11 from left to right and from top to bottom.
- The disk slots of a 2 U 36-disk controller enclosure are numbered 0 to 35 from left to right.
- Slots are used to accommodate and secure disks, interface modules, controllers, fan modules, and power modules.
- The nameplate records device information.

Rear View

Figure 3-47 and Figure 3-48 show the rear views of controller enclosures.

Figure 3-47 Rear view of a controller enclosure (with onboard SAS expansion ports and AC power modules)

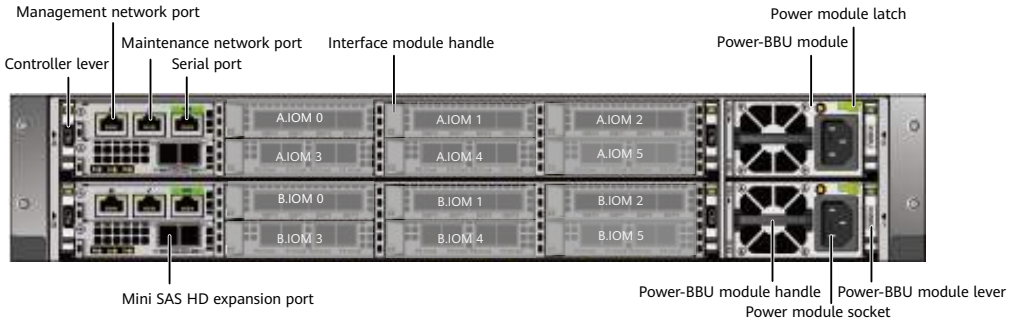
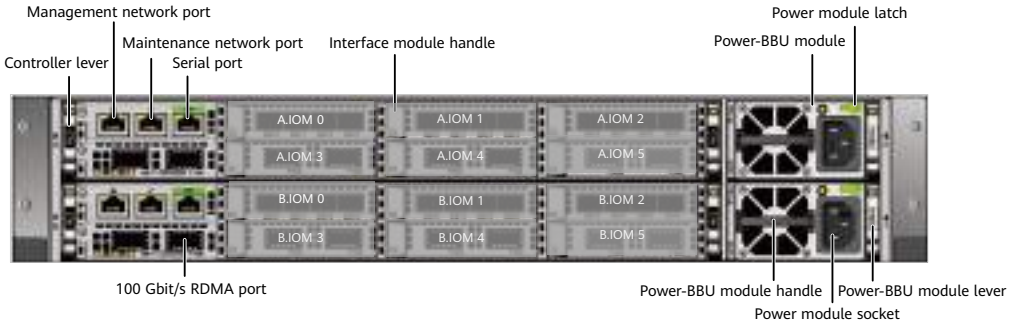


Figure 3-48 Rear view of a controller enclosure (with onboard 100 Gbit/s RDMA ports and AC power modules)



NOTICE

- Only serial cables can be inserted into the serial ports. Do not insert network cables into the serial ports.
- Do not connect the management network port and maintenance network port to the same LAN or switch to prevent network loops.

NOTE

- The controllers are A and B from top to bottom. Each controller has six interface module slots, which are numbered IOM 0, IOM 1, IOM 2, IOM 3, IOM 4, and IOM 5 from left to right and from top to bottom.
- Onboard ports include mini SAS HD expansion ports and 100 Gbit/s RDMA ports.
- The rules for installing interface modules on a controller enclosure are as follows:
  - The scale-out interface module must be installed in slot IOM 2 of each controller.
  - A maximum of three 12 Gbit/s SAS expansion modules can be installed in a sequence of IOM 5 > IOM 4 > IOM 3 (only for controller enclosures with onboard mini SAS HD expansion ports). A maximum of six 100 Gbit/s RDMA interface modules can be installed in a sequence of IOM 5 > IOM 4 > IOM 3 > IOM 1 > IOM 0 > IOM 2 (only for controller enclosures with onboard 100 Gbit/s RDMA ports).
  - Install front-end interface modules in a sequence of IOM 0 > IOM 1 > IOM 3 > IOM 4 > IOM 5 > IOM 2.
- The maintenance network port is used for special management and maintenance only by Huawei technical support engineers in emergency. The initial IP address of the maintenance network port is 172.31.128.101 or 172.31.128.102. The default subnet mask is 255.255.0.0. You are advised to connect only the management network port to the network.

Hardware Specifications

Table 3-16 lists the dimensions, weight, and power specifications of the OceanStor 5510 controller enclosure. For more specifications, refer to Specifications Query (**https://support-it.huawei.com/spec/#/home**).

Table 3-16 Hardware specifications

Item	Specifications
Dimensions (H x W x D)	• 86.1 mm x 447 mm x 820 mm (with 2.5-inch disks) • 86.1 mm x 447 mm x 900 mm (with 3.5-inch disks) • 86.1 mm x 447 mm x 920 mm (with palm-sized NVMe SSDs)
Weight (excluding auxiliary materials such as guide rails and cables)	• 38.05 kg (with 2.5-inch disks) • 38.5 kg (with 3.5-inch disks) • 40.65 kg (with palm-sized NVMe SSDs)
AC power voltage and rated current	• 2000 W power supply, 200 V to 240 V AC, 10 A, single-phase, 50/60 Hz. Supports 110 V dual-live-wire input (2W +PE). • 3000 W power supply (supporting 110 V dual-live-wire input (2W+PE) and 110 V single-live-wire input; currently used only in 110 V single-live-wire input scenarios), 100 V to 240 V AC ±10%, 16 A, single-phase, 50/60 Hz

Item	Specifications
High-voltage DC	• 2000 W DC power supply (240 V DC input), 192 V to 288 V DC, 10 A • 2200 W DC power supply (336 V DC input), 260 V to 400 V DC, 10 A
Low-voltage DC	2000 W power supply (–48 V/–60 V DC input), –40 V to –72 V DC, 50 A

Table 3-17 lists the dimensions, weight, and power specifications of the OceanStor 5610 controller enclosure. For more specifications, refer to Specifications Query (**https://support-it.huawei.com/spec/#/home**).

Table 3-17 Hardware specifications

Item	Specifications
Dimensions (H x W x D)	• 86.1 mm x 447 mm x 820 mm (with 2.5-inch disks) • 86.1 mm x 447 mm x 900 mm (with 3.5-inch disks) • 86.1 mm x 447 mm x 920 mm (with palm-sized NVMe SSDs)
Weight (excluding auxiliary materials such as guide rails and cables)	• 38.05 kg (with 2.5-inch disks) • 38.5 kg (with 3.5-inch disks) • 40.65 kg (with palm-sized NVMe SSDs)
AC power voltage and rated current	2000 W power supply (supporting 110 V dual-live-wire input (2W+PE)), 200 V to 240 V AC, 10 A, single-phase, 50/60 Hz
High-voltage DC	2000 W power supply (240 V DC input), 192 V to 288 V DC, 10 A
Low-voltage DC	2000 W power supply (–48 V/–60 V DC input), –40 V to –72 V DC, 50 A

3.5.2 Component Description

This section provides the detailed illustration and description for each component.

3.5.2.1 System Subrack

The system subrack houses a midplane that provides reliable connections for interface modules and distributes power and signals to inner modules.

Appearance

Figure 3-49 shows the appearance of a system subrack.

Figure 3-49 System subrack

3.5.2.2 Controller

A controller is the core component of a storage system. It processes storage services, receives configuration management commands, saves configuration data, connects to disks, and saves critical data onto coffer disks.

NOTE

Each controller has a built-in disk to store system data. If a power failure occurs, this disk also stores cache data. The built-in disks on different controllers are redundant for each other.

Ports

Figure 3-50 and **Figure 3-51** describe the ports of a controller.

Figure 3-50 Ports of a controller (with onboard mini SAS HD expansion ports)

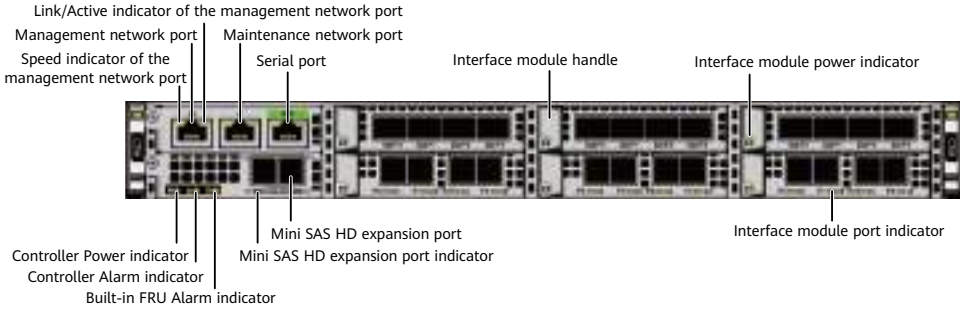
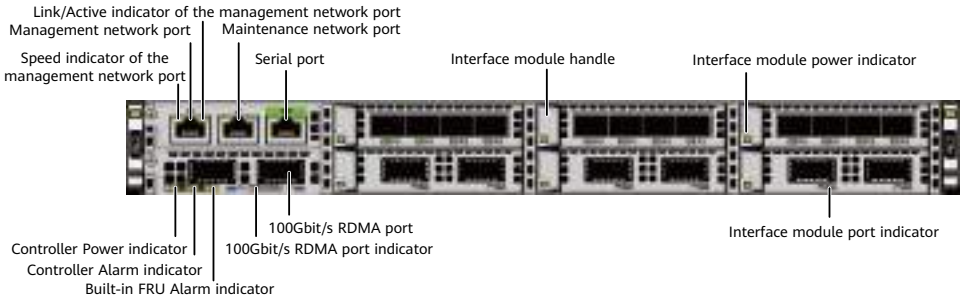


Figure 3-51 Ports of a controller (with onboard 100 Gbit/s RDMA ports)



NOTICE

Only serial cables can be inserted into the serial ports. Do not insert network cables into the serial ports.

Indicators

Table 3-18 describes the states and meanings of the indicators on a controller after it is powered on.

Table 3-18 Indicators on a controller

Indicator	Status and Description
Link/Active indicator of the management network port	• Steady green: The port is connected properly. • Blinking green (2 Hz): Data is being transmitted. • Off: The connection is abnormal.
Speed indicator of the management network port	• Steady yellow: Data is being transmitted at the highest speed. • Off: The speed is not the highest.
Power indicator of the controller	• Steady green: The controller is on. • Blinking green (0.5 Hz): The controller is being powered on and booting the BIOS. • Blinking green (2 Hz): The controller is booting the operating system or being powered off. • Off: The controller is absent or powered off.
Alarm indicator of the controller	• Steady yellow: An alarm is reported on the controller. • Off: The controller is working properly.
Built-in FRU Alarm indicator	• Steady yellow: A built-in FRU (fan module) of the controller is faulty. • Off: The built-in FRUs of the controller are normal.

Indicator	Status and Description
Indicator of the mini SAS HD expansion port	• Steady blue: The port transmission rate is 4 x 12 Gbit/s. • Steady green: The port transmission rate is 4 x 3 Gbit/s or 4 x 6 Gbit/s. • Steady yellow: The port is faulty. • Off: The port is not connected.
100 Gbit/s RDMA port indicator	• Steady blue: The speed is the highest. • Blinking blue (2 Hz): The port is transmitting data at the highest speed. • Steady green: The speed is not the highest. • Blinking green (2 Hz): The port is transmitting data, but not at the highest speed. • Steady yellow: The optical module or cable is faulty or not supported by the port. • Blinking yellow (2 Hz): The port is being located. • Off: The port is not connected.

3.5.2.3 Fan Module

Fan modules dissipate heat from the system, allowing the controller enclosure to operate normally at maximum power.

Appearance

Figure 3-52 shows the appearance of a fan module.

Figure 3-52 Appearance of a fan module

Indicators

The fan modules are located inside controllers. You can determine the running status of the fan modules by observing the Built-in FRU Alarm indicator or checking alarm information on the management UI. For the states and meanings of the Built-in FRU Alarm indicator, see **3.5.3 Indicator Description**.

3.5.2.4 Power-BBU Module

A Power-BBU module consists of a power module and a BBU. Both AC and DC power modules are supported and they allow the controller enclosure to work properly at maximum power. BBUs provide enough power to ensure that any data in flight is de-staged to the vault area in the event of a power failure. If a BBU is faulty, it can be isolated without affecting the normal running of the storage system. If a power failure occurs, BBUs ensure that the storage system writes cached data to the built-in disks of the controllers, preventing data loss. After the external power supply resumes, the driver reads data from the built-in disks of the controllers to the cache. In a system using the lithium batteries, the battery capacity is updated and detected by charging and discharging the batteries. In this way, the problems can be detected in advance that the battery capacity attenuates, the batteries fail to meet the power backup requirements of the system, and thus the data backup fails when the batteries are not used for a long time. Then, the reliability of data protection upon the system power failure can be improved.

Each controller enclosure has two power modules (PSU 0 and PSU 1) to supply power to controllers A and B. The two power modules form a power plane and are redundant of each other. For reliability purposes, it is recommended that you connect PSU 0 and PSU 1 to different PDUs.

Appearance

Figure 3-53, **Figure 3-54**, and **Figure 3-55** show the appearance and front view of the Power-BBU module.

Figure 3-53 Appearance of a Power-BBU module (using the AC module as an example)

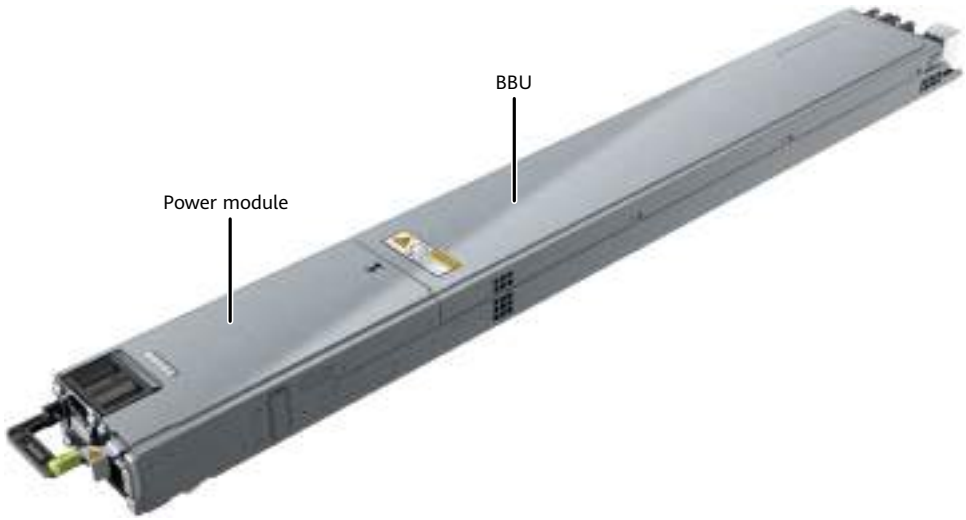


Figure 3-54 Front view of an AC Power-BBU module

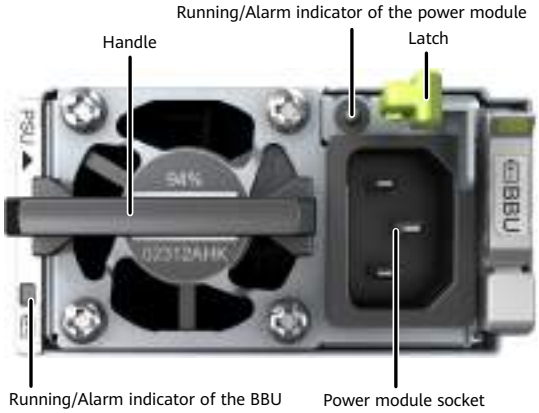
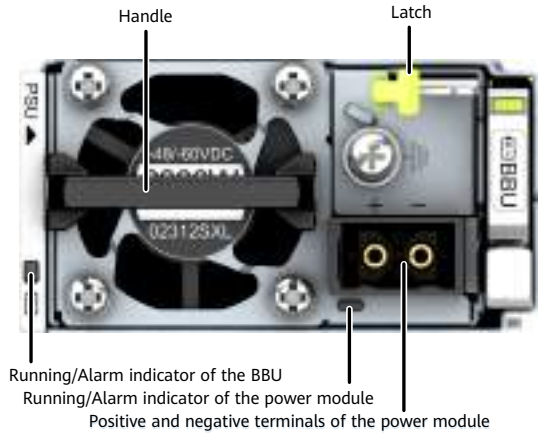


Figure 3-55 Front view of a DC Power-BBU module



Indicators

For details about the indicators on a Power-BBU module, see **3.5.3 Indicator Description**.

3.5.2.5 Disk Module

Disk modules provide storage capacity for a storage system. Disk modules can function as system coffer disks to save service data, system data, and cache data.

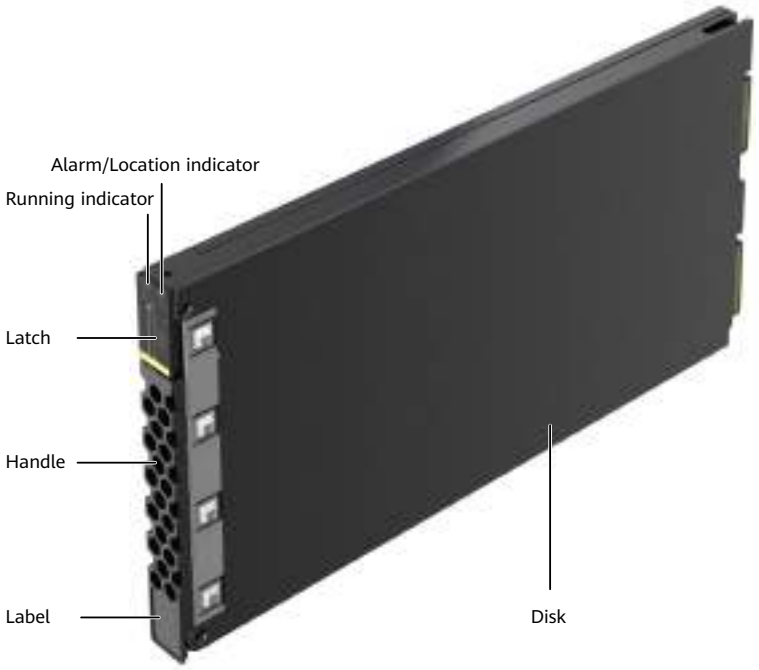
Appearance

Figure 3-56, **Figure 3-57**, and **Figure 3-58** show the appearance of a 2.5-inch disk module, a 3.5-inch disk module, and a palm-sized NVMe SSD.

Figure 3-56 2.5-inch disk module

Figure 3-57 3.5-inch disk module

Figure 3-58 Palm-sized NVMe SSD



Indicators

Table 3-19 describes indicators on a disk module.

Table 3-19 Indicators on a disk module

Indicator	Status and Description
Running indicator of the disk module	• Steady green: The disk module is working properly. • Blinking green (4 Hz or higher): Data is being read and written on the disk module. • Off: The disk module is powered off or incorrectly powered on.
Alarm/Location indicator of the disk module	• Steady yellow: The disk module is faulty. • Blinking yellow (2 Hz): The disk module is being located. • Off: The disk module is working properly or hot swappable.

3.5.3 Indicator Description

After a controller enclosure is powered on, you can check the current operating status of the controller enclosure by observing its indicators.

Indicators on the Front Panel

Figure 3-59, Figure 3-60, and Figure 3-61 show the indicators on the front panels of a 2 U 25-disk controller enclosure, a 2 U 12-disk controller enclosure, and a 2 U 36-disk controller enclosure respectively.

Figure 3-59 Indicators on the front panel of a 2 U 25-disk controller enclosure

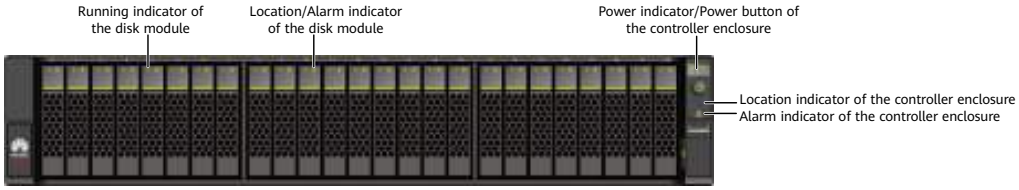


Figure 3-60 Indicators on the front panel of a 2 U 12-disk controller enclosure

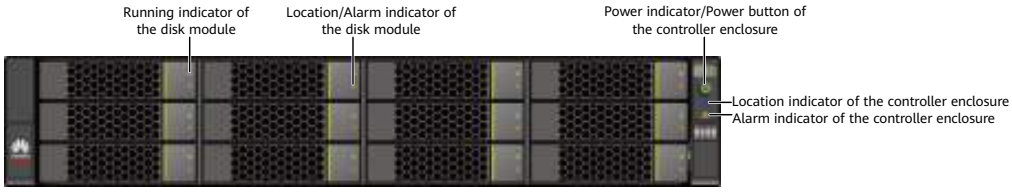


Figure 3-61 Indicators on the front panel of a 2 U 36-disk controller enclosure

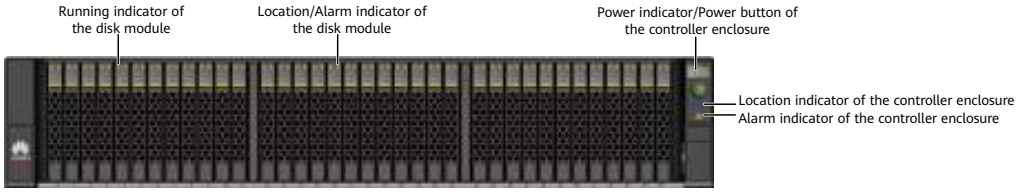


Table 3-20 describes the meanings of the indicators on the front panel of a controller enclosure.

Table 3-20 Meanings of the indicators on the front panel of a controller enclosure

Module	Indicator	Status and Description
Disk module	Running indicator of the disk module	• Steady green: The disk module is working properly. • Blinking green (4 Hz or higher): Data is being read and written on the disk module. • Off: The disk module is powered off or incorrectly powered on.
	Alarm/Location indicator of the disk module	• Steady yellow: The disk module is faulty. • Blinking yellow (2 Hz): The disk module is being located. • Off: The disk module is working properly or hot swappable.

Module	Indicator	Status and Description
System subrack	Location indicator of the controller enclosure	• Blinking blue (2 Hz): The controller enclosure is being located. • Off: The controller enclosure is not located.
	Alarm indicator of the controller enclosure	• Steady yellow: A major or critical alarm is reported on the storage system. • Off: The storage system is running properly.
	Power indicator/Power button of the controller enclosure	• Steady green: The controller enclosure is on. • Blinking green (0.5 Hz): The controller enclosure is being powered on. • Blinking green (1 Hz): The controller enclosure is in the burn-in state. • Blinking green (2 Hz): The controller enclosure is booting the operating system or being powered off. • Off: The controller enclosure is off or powered by the BBUs.

Indicators on the Rear Panel

Figure 3-63 and **Figure 3-62** show the indicators on the rear panel of a controller enclosure.

Figure 3-62 Indicators on the rear panel of a controller enclosure (with onboard mini SAS HD expansion ports)

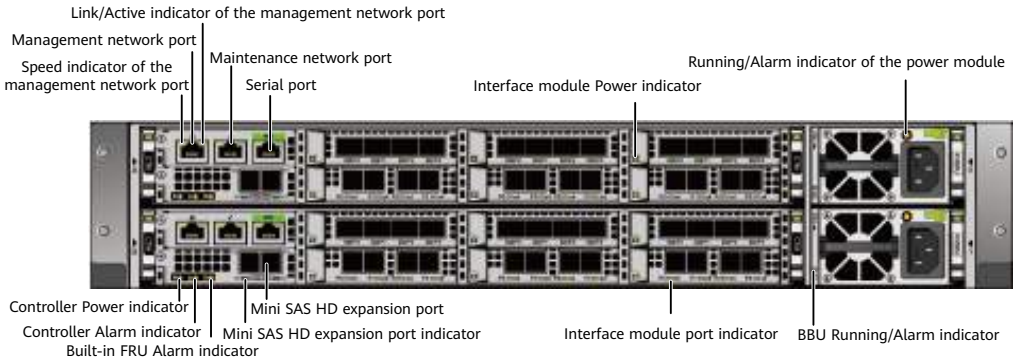


Figure 3-63 Indicators on the rear panel of a controller enclosure (with onboard 100 Gbit/s RDMA ports)

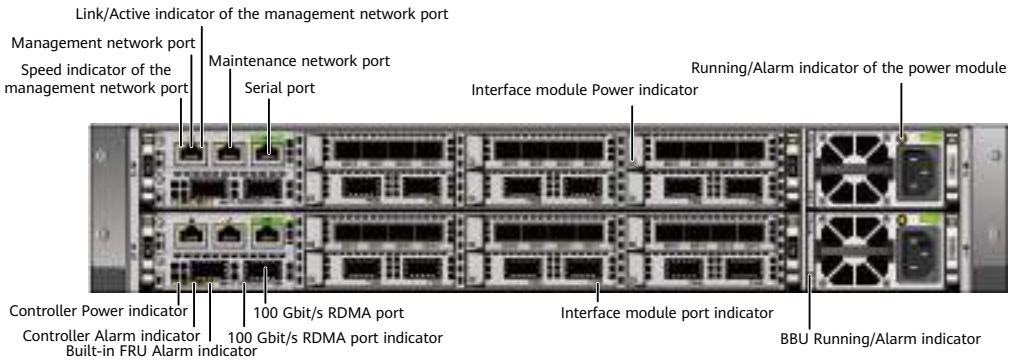


Table 3-21 describes the meanings of the indicators on the rear panel of a controller enclosure.

Table 3-21 Meanings of the indicators on the rear panel of a controller enclosure

Module	Indicator	Status and Description
Interface module	Power indicator of the interface module	For the states and meanings of the indicators on the interface modules supported by a controller, see 3.5.3 Indicator Description.
	Port indicator	
Power-BBU module	Running/ Alarm indicator of the power module	• Steady green: The power input is normal. • Blinking green (1 Hz): The power input is normal but the device is powered off. • Blinking green (4 Hz): The power module is being upgraded online. • Steady yellow: The power module is faulty. • Off: There is no external power input.
	Running/ Alarm indicator of the BBU	• Steady green: The BBU is fully charged. • Blinking green (1 Hz): The BBU is being charged. • Blinking green (4 Hz): The BBU is being discharged. • Steady yellow: The BBU is faulty. • Off: The module is powered off or hot swappable.
Controller	Link/Active indicator of the management network port	• Steady green: The port is connected properly. • Blinking green (2 Hz): Data is being transmitted. • Off: The connection is abnormal.

Module	Indicator	Status and Description
	Speed indicator of the management network port	• Steady yellow: Data is being transmitted at the highest speed. • Off: The speed is not the highest.
	Power indicator of the controller	• Steady green: The controller is on. • Blinking green (0.5 Hz): The controller is being powered on and booting the BIOS. • Blinking green (2 Hz): The controller is booting the operating system or being powered off. • Off: The controller is absent or powered off.
	Alarm indicator of the controller	• Steady yellow: An alarm is reported on the controller. • Off: The controller is working properly.
	Built-in FRU Alarm indicator	• Steady yellow: A built-in FRU (fan module) of the controller is faulty. • Off: The built-in FRUs of the controller are normal.
	Indicator of the mini SAS HD expansion port	• Steady blue: The port transmission rate is 4 x 12 Gbit/s. • Steady green: The port transmission rate is 4 x 3 Gbit/s or 4 x 6 Gbit/s. • Steady yellow: The port is faulty. • Off: The port is not connected.
	100 Gbit/s RDMA port indicator	• Steady blue: The speed is the highest. • Blinking blue (2 Hz): The port is transmitting data at the highest speed. • Steady green: The speed is not the highest. • Blinking green (2 Hz): The port is transmitting data, but not at the highest speed. • Steady yellow: The optical module or cable is faulty or not supported by the port. • Blinking yellow (2 Hz): The port is being located. • Off: The port is not connected.

3.6 Interface Module

This section describes the functions, appearance, and indicator status of interface modules.

For details about the hot-swappable interface module types supported by each product model and version, see Specifications Query (**https://support-it.huawei.com/spec/#/home**).

3.6.1 GE Electrical Interface Module

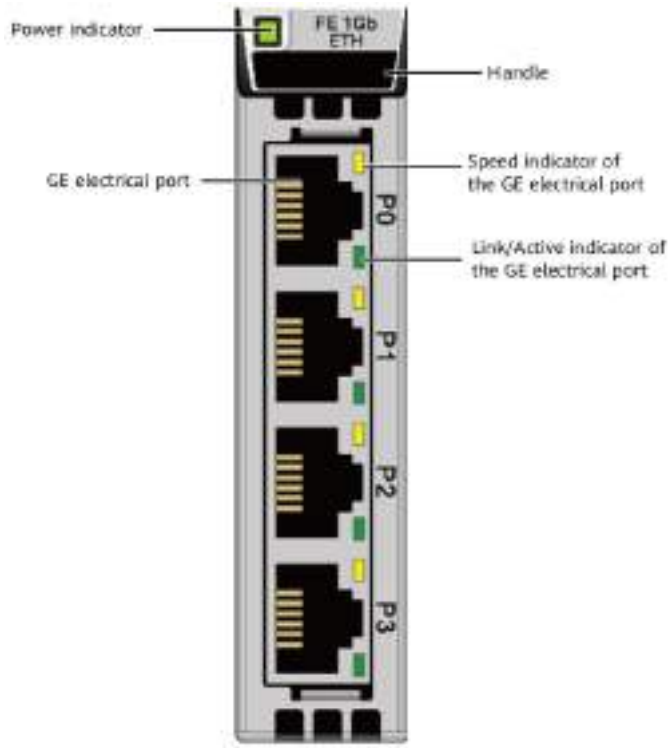
Function

A GE electrical interface module provides four 1 Gbit/s electrical ports. The rate cannot be decreased to 100 Mbit/s or 10 Mbit/s.

Ports

Figure 3-64 shows the appearance of a GE electrical interface module. FE stands for front-end.

Figure 3-64 GE electrical interface module



Indicators

Table 3-22 describes the indicators on a GE electrical interface module after the storage system is powered on.

Table 3-22 Indicators on a GE electrical interface module

Indicator	Status and Description
Power indicator	• Steady green: The module is working properly. • Blinking green (2 Hz): There is a hot swap request to the module. • Steady yellow: The module is faulty. • Off: The module is powered off or hot swappable.
Link/Active indicator of the port	• Steady green: The link to the application server is normal. • Blinking green (2 Hz): Data is being transmitted. • Off: The link to the application server is down or no link exists.
Speed indicator of the port	• Steady yellow: The speed is the highest. • Off: The speed is not the highest.

3.6.2 10GE Electrical Interface Module

The 10GE electrical interface module is used to connect storage devices to application servers.

Function

A 10GE electrical interface module provides four 10 Gbit/s electrical ports. The electrical module rate must be consistent with that on the interface module label. Otherwise, the storage system reports an alarm and this port is unavailable.

Table 3-23 describes the requirements for the electrical modules on the storage system and at the peer end of the storage system.

Table 3-23 Electrical module parameters

Electrical Module Rate on the Storage System	Type	Electrical Module Rate at the Peer End
10 Gbit/s	SFP+	10 Gbit/s

NOTE

The storage system does not support electrical modules purchased by the customer elsewhere. Use electrical modules that match the storage interface modules.

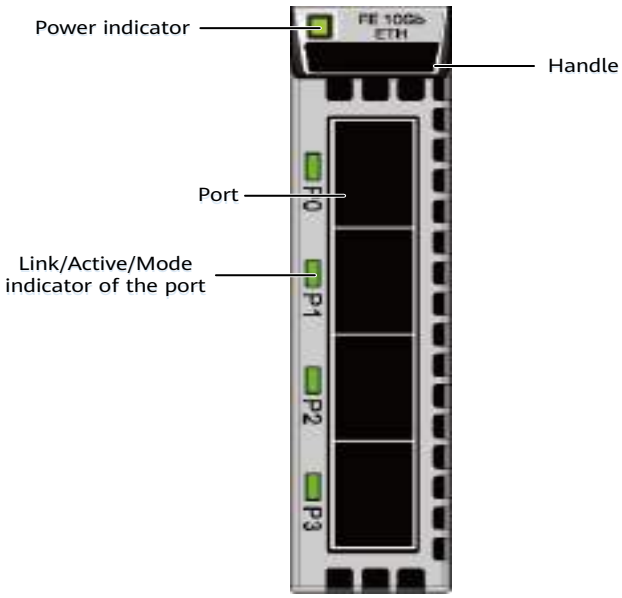
Ports

Figure 3-65 shows the appearance of a 10GE electrical interface module. FE stands for front-end.

NOTE

A 10GE electrical interface module has the same appearance as a SmartIO interface module that uses a 10 Gbit/s optical module. You can distinguish between them only by the BOM numbers on their handles. You can check the BOM number on the Spare Parts Query tool (**https://info.support.huawei.com/storage/spareparts/#/home**) to determine the interface module type.

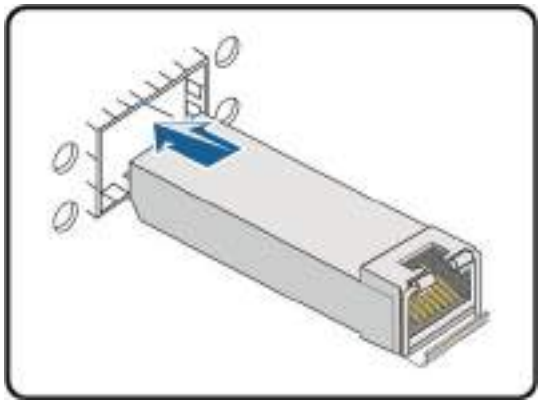
Figure 3-65 10GE electrical interface module



NOTE

You must first install electrical modules before using the 10GE electrical interface module. Figure 3-66 shows how to install an electrical module. For details about the standard cable types and length requirements for the ports, see Specifications Query (**https://info.support.huawei.com/storage/spareparts/#/home**).

Figure 3-66 Installing an electrical module



Indicators

Table 3-24 describes the indicators on a 10GE electrical interface module after the storage system is powered on.

Table 3-24 Indicators on a 10GE electrical interface module

Indicator	Status and Description
Power indicator	• Steady green: The module is working properly. • Blinking green: There is a hot swap request to the module. • Steady yellow: The module is faulty. • Off: The module is powered off or hot swappable.
Port Link/Active/Mode indicator	• Steady green: The interface module is working in Ethernet mode and the port link is up. • Blinking green (2 Hz): The interface module is working in Ethernet mode and data is being transmitted. • Steady yellow: The electrical module is faulty or does not match the port specifications. • Blinking yellow (2 Hz): The port is being located. • Off: The port is not connected.

3.6.3 25 Gbit/s RDMA Interface Module

The 25 Gbit/s RDMA interface module is used to connect two controller enclosures.

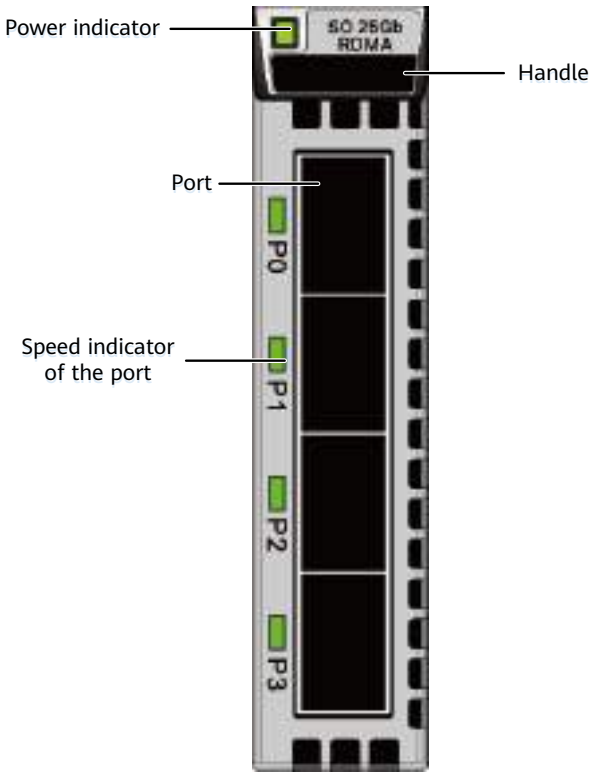
Function

A 25 Gbit/s RDMA interface module provides four 25 Gbit/s optical ports.

Ports

Figure 3-67 shows the appearance of a 25 Gbit/s RDMA interface module. SO stands for scale-out.

Figure 3-67 25 Gbit/s RDMA interface module



Indicators

Table 3-25 describes the indicators on a 25 Gbit/s RDMA interface module after the storage system is powered on.

Table 3-25 Indicators on a 25 Gbit/s RDMA interface module

Indicator	Status and Description
Power indicator	• Steady green: The interface module is working properly. • Blinking green: There is a hot swap request to the module. • Steady yellow: The module is faulty. • Off: The module is powered off or hot swappable.

Indicator	Status and Description
Speed indicator of the port	• Steady green: The speed is the highest. • Blinking green (2 Hz): The port is transmitting data at the highest speed. • Steady yellow: The optical module or cable is faulty or not supported by the port. • Off: The port is not connected.

3.6.4 25 Gbit/s RoCE Interface Module

A 25 Gbit/s RoCE interface module is used for NVMe over Fabrics connections between a storage device and an application server or for HyperMetro replication links between two storage devices.

Function

A 25 Gbit/s RoCE interface module provides four 25 Gbit/s optical ports. The optical module rate must be consistent with that on the interface module label. Otherwise, the storage system reports an alarm and this port is unavailable.

Table 3-26 describes the requirements for the optical modules on the storage system and at the peer end of the storage system.

Table 3-26 Optical module parameters

Optical Module Rate on the Storage System	Type	Optical Module Rate at the Peer End	Negotiated Rate
25 Gbit/s	SFP28	25 Gbit/s	25 Gbit/s

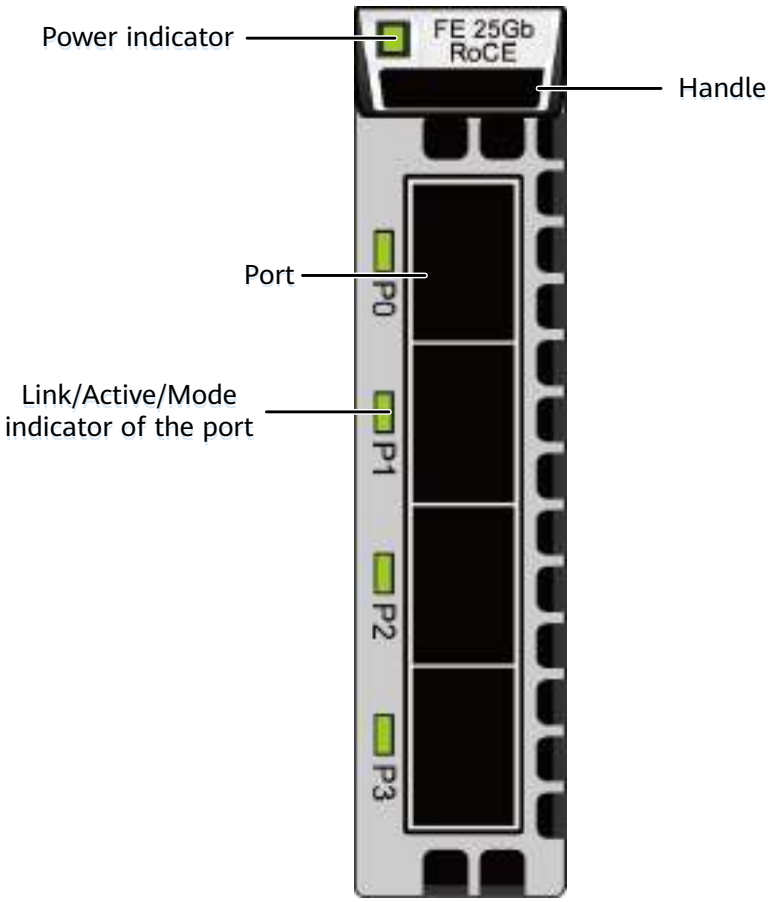
NOTE

The storage system does not support optical modules purchased by the customer elsewhere. Use optical modules that match the storage interface modules.

Ports

Figure 3-68 shows the appearance of a 25 Gbit/s RoCE interface module. FE stands for front-end.

Figure 3-68 25 Gbit/s RoCE interface module



Indicators

Table 3-27 describes the indicators on a 25 Gbit/s RoCE interface module after the storage system is powered on.

Table 3-27 Indicators on a 25 Gbit/s RoCE interface module

Indicator	Status and Description
Power indicator	• Steady green: The interface module is working properly. • Blinking green: There is a hot swap request to the module. • Steady yellow: The module is faulty. • Off: The interface module is powered off or hot swappable.

Indicator	Status and Description
Port Link/Active/Mode indicator	• Steady green: The interface module is working in Ethernet mode and the port link is up. • Blinking green (2 Hz): The interface module is working in Ethernet mode and data is being transmitted. • Steady yellow: The optical module is faulty or does not match the port specifications. • Blinking yellow (2 Hz): The port is being located. • Off: The port is not connected.

3.6.5 40GE Interface Module

The 40GE interface module is used to connect storage devices to application servers.

Function

A 40GE interface module provides two 40 Gbit/s optical ports.

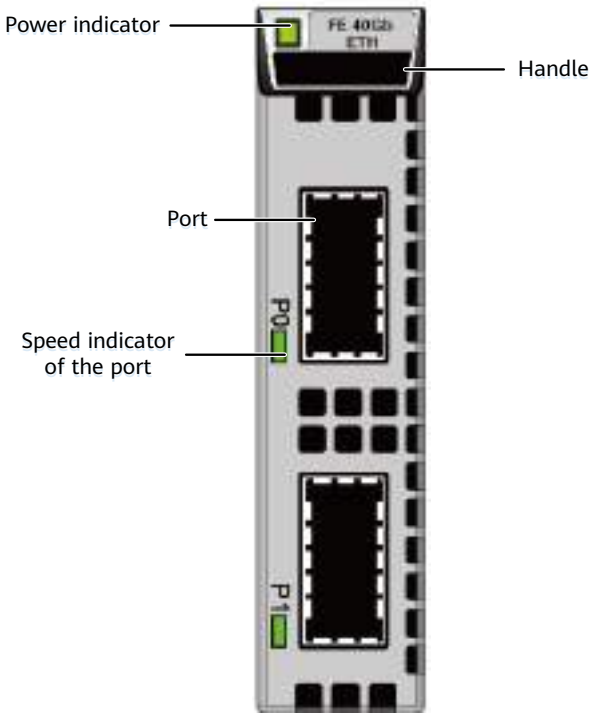
NOTE

The storage system does not support optical modules purchased by the customer elsewhere. Use optical modules that match the storage interface modules.

Ports

Figure 3-69 shows the appearance of a 40GE interface module. FE stands for front-end.

Figure 3-69 40GE interface module



Indicators

Table 3-28 describes the indicators on a 40GE interface module after the storage system is powered on.

Table 3-28 Indicators on a 40GE interface module

Indicator	Status and Description
Power indicator	• Steady green: The module is working properly. • Blinking green: There is a hot swap request to the module. • Steady yellow: The module is faulty. • Off: The module is powered off or hot swappable.
Speed indicator of the port	• Steady green: The speed is the highest. • Blinking green (2 Hz): The port is transmitting data at the highest speed. • Steady yellow: The optical module or cable is faulty or not supported by the port. • Off: The port is not connected.

3.6.6 100GE Interface Module

The 100GE interface module is used to connect storage devices to application servers.

Function

A 100GE interface module provides two 100 Gbit/s optical ports.

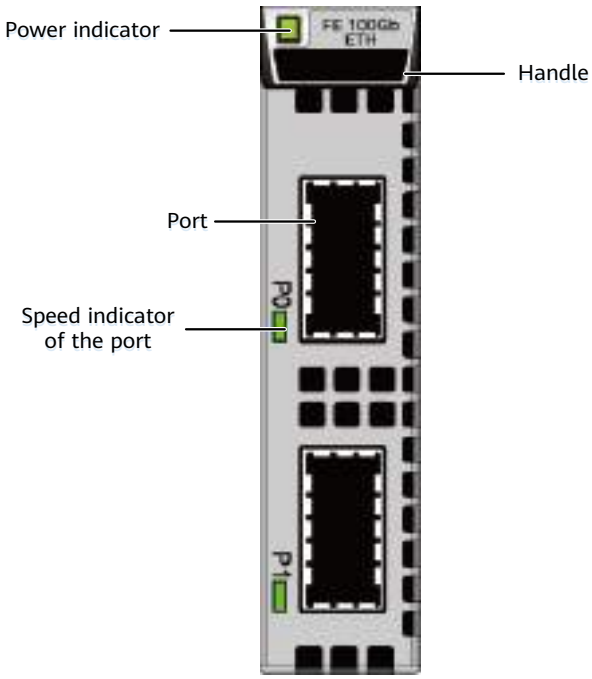
NOTE

The storage system does not support optical modules purchased by the customer elsewhere. Use optical modules that match the storage interface modules.

Ports

Figure 3-70 shows the appearance of a 100GE interface module. FE stands for front-end.

Figure 3-70 100GE interface module



Indicators

Table 3-29 describes the indicators on a 100GE interface module after the storage system is powered on.

Table 3-29 Indicators on a 100GE interface module

Indicator	Status and Description
Power indicator	• Steady green: The module is working properly. • Blinking green: There is a hot swap request to the module. • Steady yellow: The module is faulty. • Off: The module is powered off or hot swappable.
Speed indicator of the port	• Steady blue: The speed is the highest. • Blinking blue (2 Hz): The port is transmitting data at the highest speed. • Steady yellow: The optical module or cable is faulty or not supported by the port. • Off: The port is not connected.

3.6.7 100 Gbit/s RDMA Interface Module

The 100 Gbit/s RDMA interface module is used to connect a controller enclosure to another controller enclosure or a smart disk enclosure.

Function

A 100 Gbit/s RDMA interface module provides two 100 Gbit/s optical ports.

Ports

Figure 3-71 and **Figure 3-72** show the appearances of 100 Gbit/s RDMA interface modules. SO stands for scale-out and BE stands for back-end.

Figure 3-71 100 Gbit/s RDMA interface module (SO)

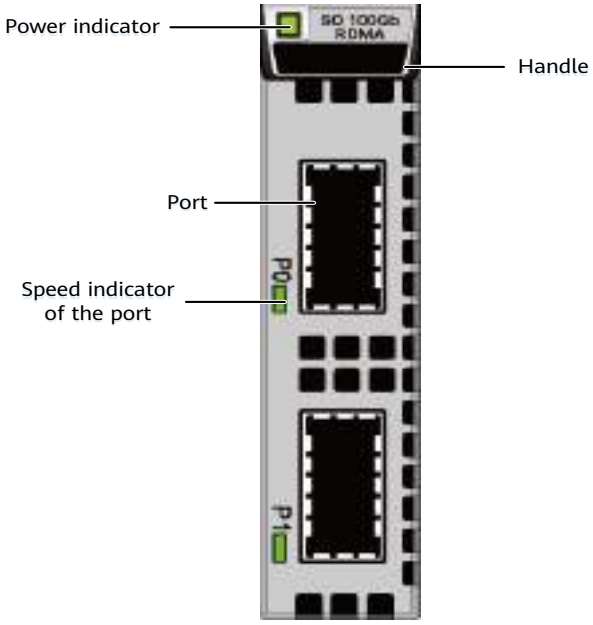
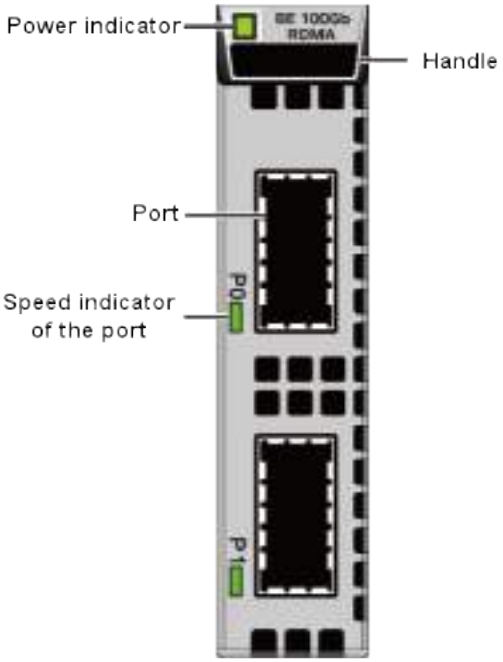


Figure 3-72 100 Gbit/s RDMA interface module (BE)



Indicators

Table 3-30 describes the indicators on a 100 Gbit/s RDMA interface module after the storage system is powered on.

Table 3-30 Indicators on a 100 Gbit/s RDMA interface module

Indicator	Status and Description
Power indicator	• Steady green: The module is working properly. • Blinking green: There is a hot swap request to the module. • Steady yellow: The module is faulty. • Off: The module is powered off or hot swappable.
Speed indicator of the port	• Steady blue: The speed is the highest. • Blinking blue (2 Hz): The port is transmitting data at the highest speed. • Steady yellow: The optical module or cable is faulty or not supported by the port. • Off: The port is not connected.

3.6.8 SmartIO Interface Module

Function

A SmartIO interface module supports 8 Gbit/s, 10 Gbit/s, 16 Gbit/s, 25 Gbit/s, and 32 Gbit/s optical modules. The optical module rate must be consistent with that on the interface module label. Otherwise, the storage system reports an alarm and this port is unavailable.

For a Fibre Channel optical module, the enabled auto-negotiation function allows it to auto-negotiate a maximum of three speeds. The Ethernet optical module does not support auto-negotiation. Table 3-31 describes the requirements for the optical modules on the storage system and at the peer end of the storage system.

Table 3-31 Optical module parameters

Optical Module Rate on the Storage System	Type	Optical Module Rate at the Peer End	Negotiated Rate
8 Gbit/s	SFP+	8 Gbit/s	8 Gbit/s
		16 Gbit/s	8 Gbit/s
		32 Gbit/s	8 Gbit/s
10 Gbit/s	SFP+	10 Gbit/s	10 Gbit/s

Optical Module Rate on the Storage System	Type	Optical Module Rate at the Peer End	Negotiated Rate
16 Gbit/s	SFP+	8 Gbit/s	8 Gbit/s
		16 Gbit/s	16 Gbit/s
		32 Gbit/s	16 Gbit/s
25 Gbit/s	SFP28	25 Gbit/s	25 Gbit/s
32 Gbit/s	SFP28	8 Gbit/s	8 Gbit/s
		16 Gbit/s	16 Gbit/s
		32 Gbit/s	32 Gbit/s

NOTE

The storage system does not support optical modules purchased by the customer elsewhere. Use optical modules that match the storage interface modules. The working mode and rate of the interface module cannot be modified. If the customer requires a different rate on the interface module, contact Huawei technical support engineers and purchase a new interface module of the required rate.

Ports

Figure 3-73, **Figure 3-74**, **Figure 3-75**, **Figure 3-76**, and **Figure 3-77** show 8 Gbit/s, 10 Gbit/s, 16 Gbit/s, 25 Gbit/s, and 32 Gbit/s SmartIO interface modules respectively. FE stands for front-end.

Figure 3-73 8 Gbit/s SmartIO interface module

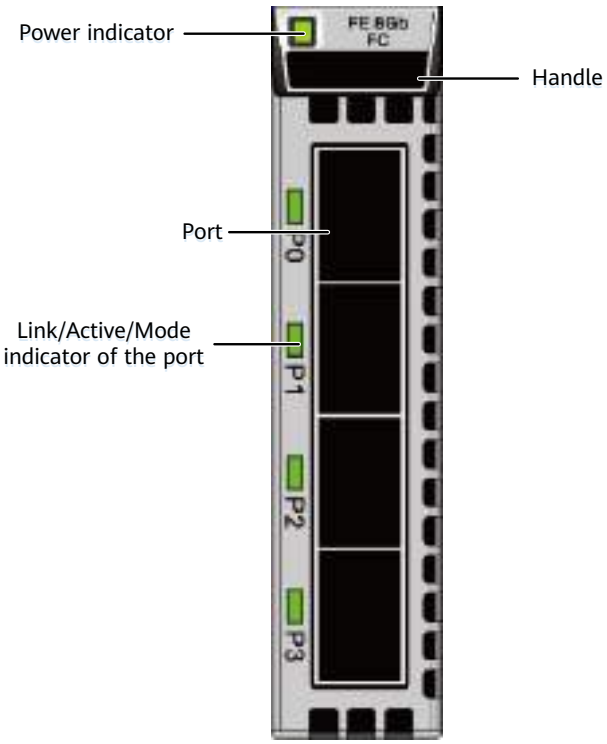


Figure 3-74 10 Gbit/s SmartIO interface module

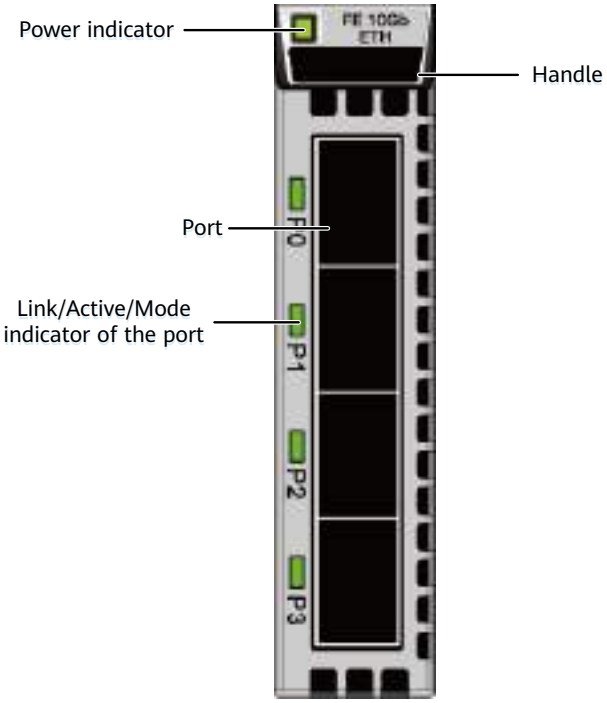


Figure 3-75 16 Gbit/s SmartIO interface module

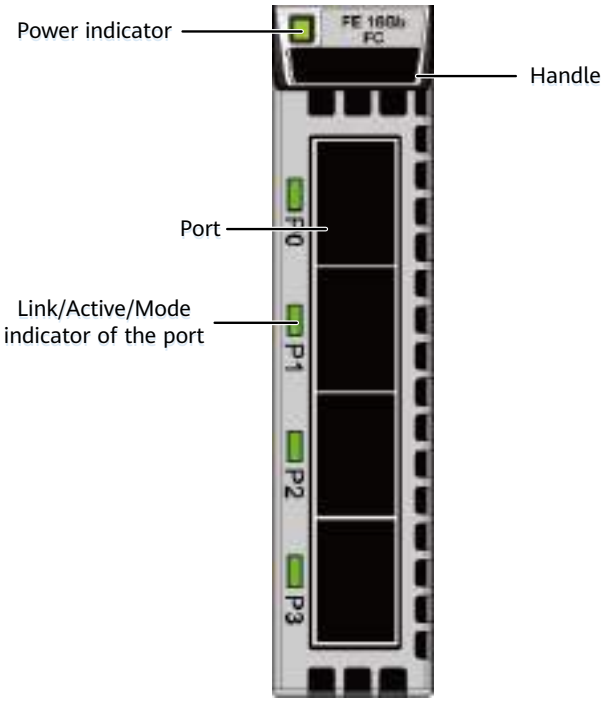


Figure 3-76 25 Gbit/s SmartIO interface module

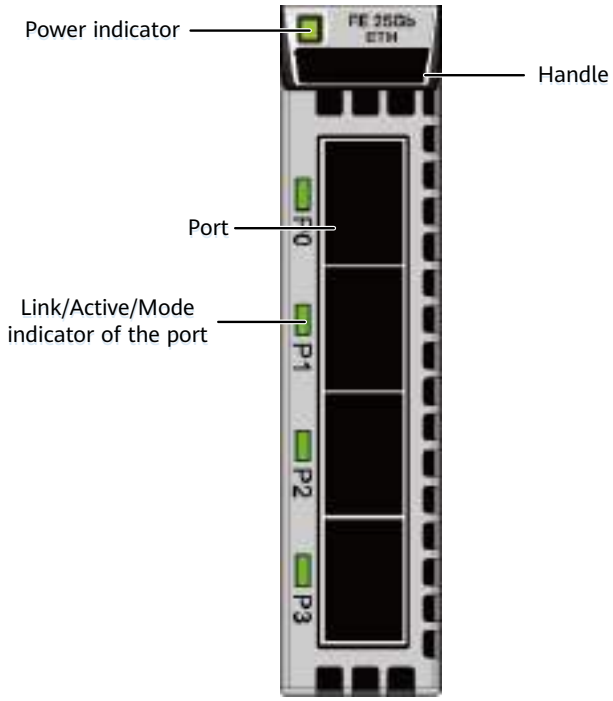
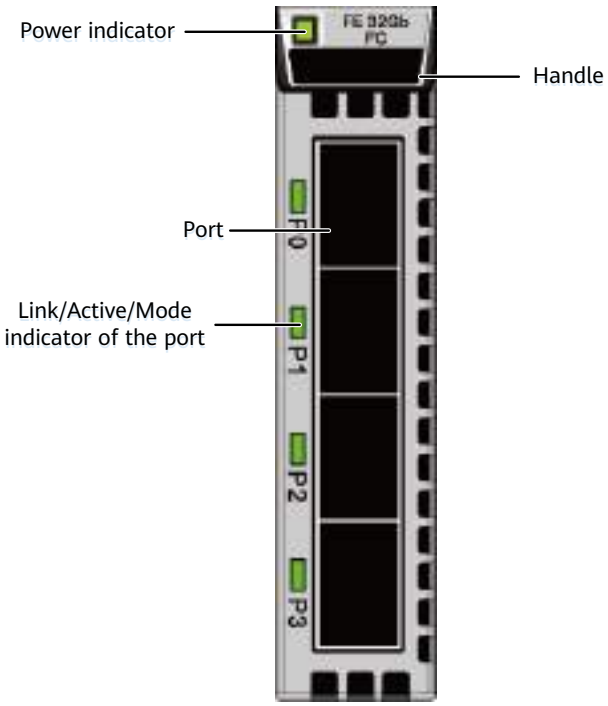


Figure 3-77 32 Gbit/s SmartIO interface module



Indicators

Table 3-32 describes the indicators on a SmartIO interface module after the storage system is powered on.

Table 3-32 Indicators on a SmartIO interface module

Indicator	Status and Description
Power indicator	• Steady green: The module is working properly. • Blinking green: There is a hot swap request to the module. • Steady yellow: The module is faulty. • Off: The module is powered off or hot swappable.

Indicator	Status and Description
Link/Active/Mode indicator of the port	• Steady blue: The interface module is working in FC mode, the port link is up, and no data is being transmitted. • Blinking blue (2 Hz): The interface module is working in FC mode and data is being transmitted. • Steady green: The interface module is working in Ethernet mode, the port link is up, and no data is being transmitted. • Blinking green (2 Hz): The interface module is working in Ethernet mode and data is being transmitted. • Steady yellow: The port is faulty. • Off: The port is not connected.

3.6.9 12 Gbit/s SAS Expansion Module

An expansion module provides expansion ports that are used for communication between a controller enclosure and a SAS disk enclosure.

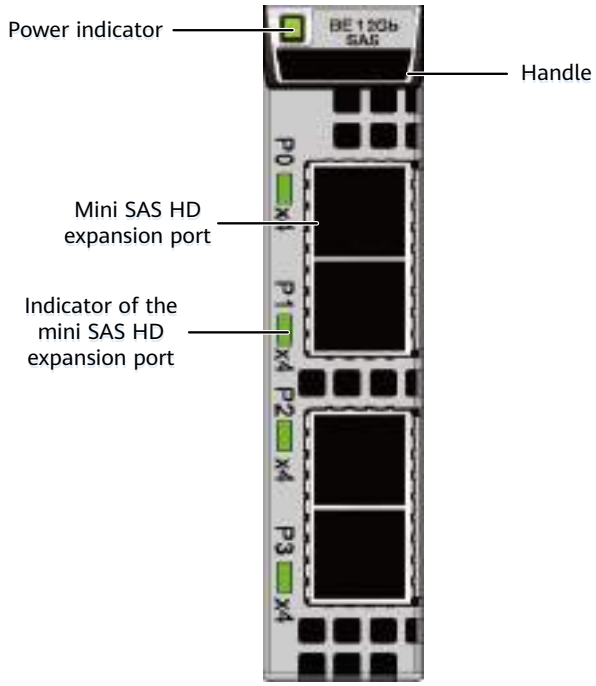
Function

A 12 Gbit/s SAS interface module provides four 4 x 12 Gbit/s mini SAS HD expansion ports that provide connectivity to disk enclosures. The SAS expansion module uses mini SAS HD cables to connect to disk enclosures. If the transmission rate of the device connected to an expansion port is lower than the port rate, the expansion port automatically adjusts the transmission rate to ensure connectivity of the data transmission channel and consistency of transmission rates.

Ports

Figure 3-78 shows the appearance of a 12 Gbit/s SAS expansion module. BE stands for back-end.

Figure 3-78 12 Gbit/s SAS expansion module



Indicators

Table 3-33 describes the indicators on a 12 Gbit/s SAS expansion module after the storage system is powered on.

Table 3-33 Indicators on a 12 Gbit/s SAS expansion module

Indicator	Status and Description
Power indicator	• Steady green: The module is working properly. • Blinking green: There is a hot swap request to the module. • Steady yellow: The module is faulty. • Off: The module is powered off or hot swappable.
Mini SAS HD expansion port indicator	• Steady blue: The port transmission rate is 4 x 12 Gbit/s. • Steady green: The port transmission rate is 4 x 3 Gbit/s or 4 x 6 Gbit/s. • Steady yellow: The port is faulty. • Off: The port is not connected.

3.7 2 U SAS Disk Enclosure (with 2.5-Inch Disks)

This section describes a disk enclosure in terms of its hardware structure, component functions, front and rear views, and indicators.

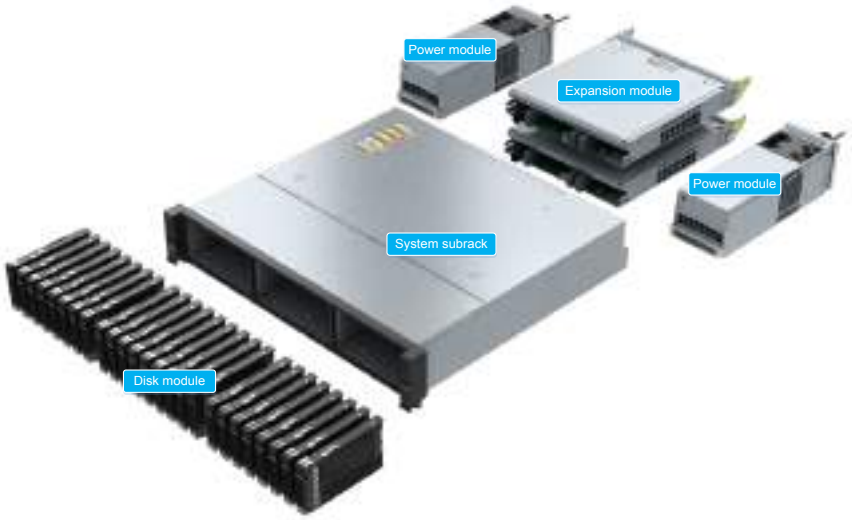
3.7.1 Overview

The disk enclosure uses a modular design and consists of a system subrack, expansion modules, disk modules, and power modules.

Overall Structure

Figure 3-79 shows the overall structure of a disk enclosure.

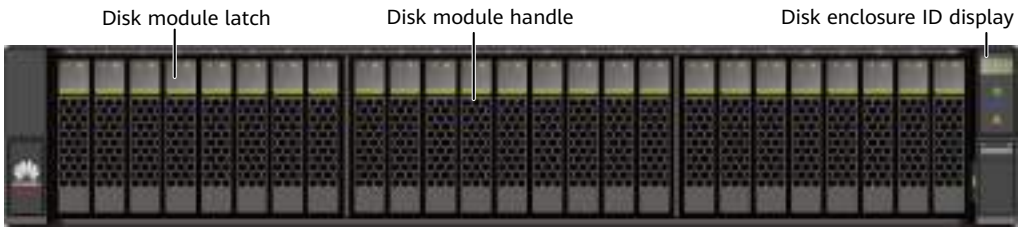
Figure 3-79 Overall structure of a disk enclosure



Front View

Figure 3-80 shows the front view of a disk enclosure.

Figure 3-80 Front view of a disk enclosure



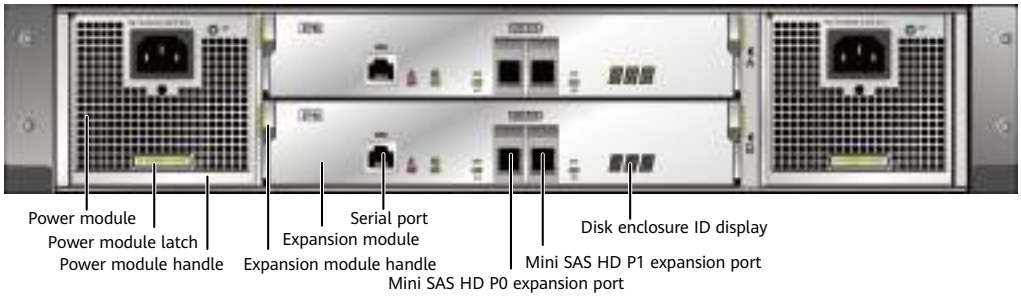
NOTE

The disk slots are numbered 0 to 24 from left to right.

Rear View

Figure 3-81 shows the rear view of a disk enclosure.

Figure 3-81 Rear view of a disk enclosure (using the AC power module as an example)



NOTICE

Only serial cables can be inserted into serial ports. Do not insert network cables into serial ports.

Hardware Specifications

Table 3-34 lists the dimensions, weight, and power specifications of the disk enclosure. For more specifications, refer to Specifications Query (**https://support-it.huawei.com/spec/#/home**).

Table 3-34 Hardware specifications

Item	Specifications
Dimensions (H x W x D)	86.1 mm x 447 mm x 410 mm
Weight (excluding disks and auxiliary materials such as guide rails and cables)	13.4 kg
AC power voltage and rated current	800 W AC power supply (supporting 110 V dual-live-wire input (2W+PE) and 110 V single-live-wire input), 100 V to 240 V AC ±10%, 10 A, single-phase, 50/60 Hz
High-voltage DC	800 W power supply (240 V DC input), 192 V to 288 V, 10 A
Low-voltage DC	600 W power supply (supporting –48 V/–60 V DC input), –38.4 V to –75 V DC, 16 A

3.7.2 Component Description

This section provides the detailed illustration and description for each component.

3.7.2.1 System Subrack

The system subrack houses a midplane that provides reliable connections for interface modules and distributes power and signals to inner modules.

Appearance

Figure 3-82 shows the appearance of a system subrack.

Figure 3-82 System subrack

3.7.2.2 Expansion Module

An expansion module provides expansion ports for communication between the disk enclosure and the controller enclosure. Each expansion module provides two expansion ports P0 and P1.

Appearance

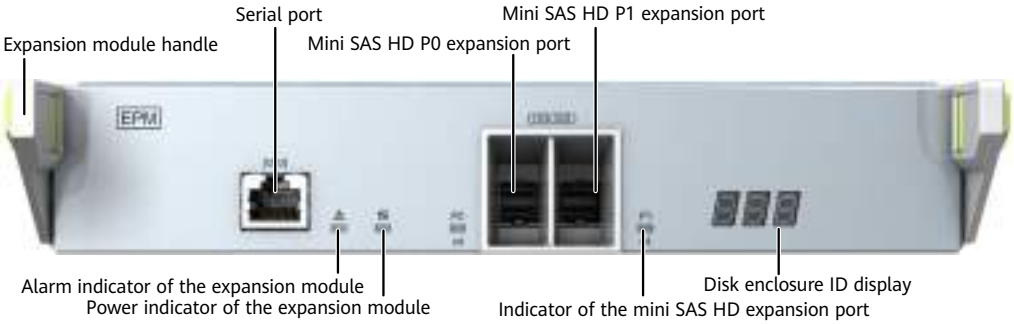
Figure 3-83 shows the appearance of an expansion module.

Figure 3-83 Expansion module

Ports

Figure 3-84 shows the ports on an expansion module.

Figure 3-84 Ports on an expansion module



NOTICE

Only serial cables can be inserted into serial ports. Do not insert network cables into serial ports.

Indicators

Table 3-35 describes the indicators on an expansion module.

Table 3-35 Indicators on an expansion module

Indicator	Status and Description
Alarm indicator of the expansion module	• Steady yellow: An alarm is reported by the expansion module. • Off: The expansion module is working properly.
Power indicator of the expansion module	• Steady green: The expansion module is powered on. • Off: The expansion module is powered off.
Mini SAS HD expansion port indicator	• Steady blue: The port transmission rate is 4 x 12 Gbit/s. • Steady green: The port transmission rate is 4 x 3 Gbit/s or 4 x 6 Gbit/s. • Steady yellow: The port is faulty. • Off: The port is not connected.

3.7.2.3 Power Module

The storage system supports AC and DC power modules. Power modules allow the disk enclosure to work properly at maximum power.

Appearance

Figure 3-85 shows the appearance of an AC power module. Figure 3-86 shows the appearance of a DC power module.

Figure 3-85 AC power module

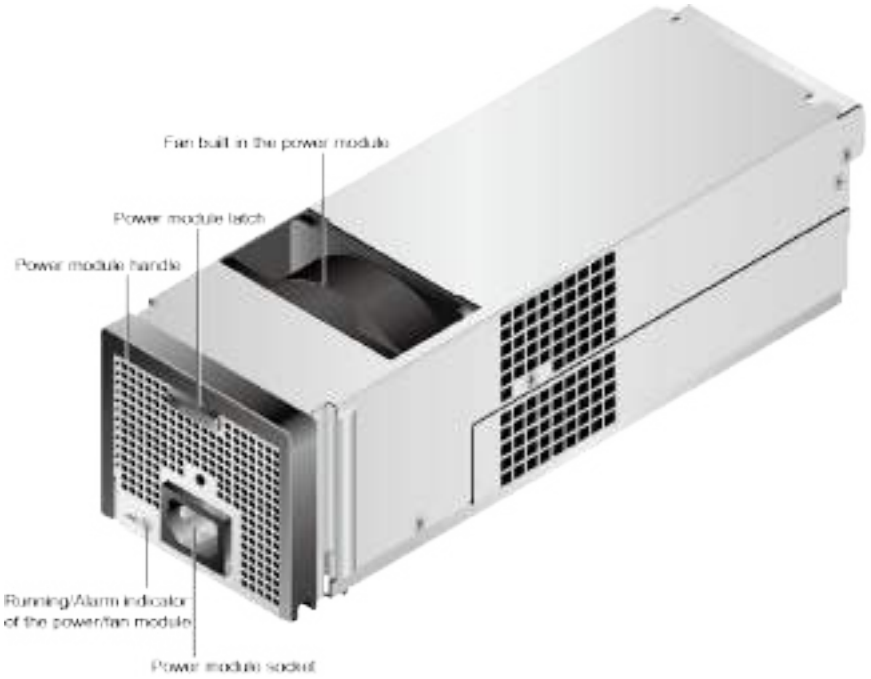
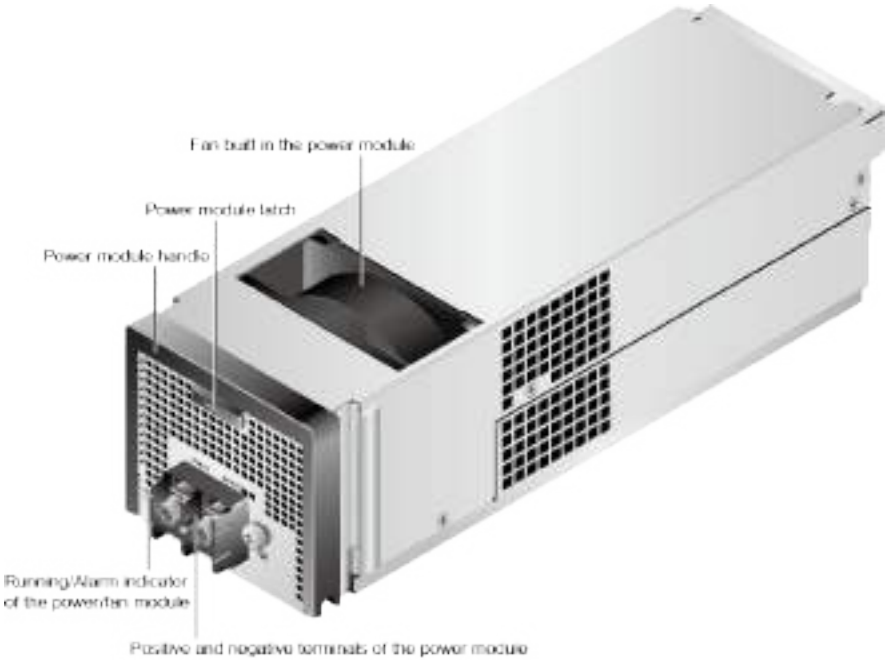


Figure 3-86 DC power module



Indicators

Table 3-36 describes indicators on a power module.

Table 3-36 Indicator on a power module

Indicator	Status and Description
Running/Alarm indicator of the power/fan module	• Steady green: The power input is normal. • Blinking green (1 Hz): The power input is normal but the device is powered off. • Blinking green (4 Hz): The power module is being upgraded online. • Steady yellow: The power module or fan module is faulty. • Off: There is no external power input.

3.7.2.4 Disk Module

Disk modules provide storage capacity for a storage system. Disk modules can function as system coffer disks to save service data, system data, and cache data.

Appearance

Figure 3-87 shows the appearance of a disk module.

Figure 3-87 Disk module

Indicators

Table 3-37 describes indicators on a disk module.

Table 3-37 Indicators on a disk module

Indicator	Status and Description
Running indicator of the disk module	• Steady green: The disk module is working properly. • Blinking green (4 Hz or higher): Data is being read and written on the disk module. • Off: The disk module is powered off or incorrectly powered on.
Alarm/Location indicator of the disk module	• Steady yellow: The disk module is faulty. • Blinking yellow (2 Hz): The disk module is being located. • Off: The disk module is working properly or hot swappable.

3.7.3 Indicator Description

After a disk enclosure is powered on, you can check the current operating status of the disk enclosure by observing its indicators.

Indicators on the Front Panel

Figure 3-88 shows the indicators on the front panel of a disk enclosure.

Figure 3-88 Indicators on the front panel of a disk enclosure

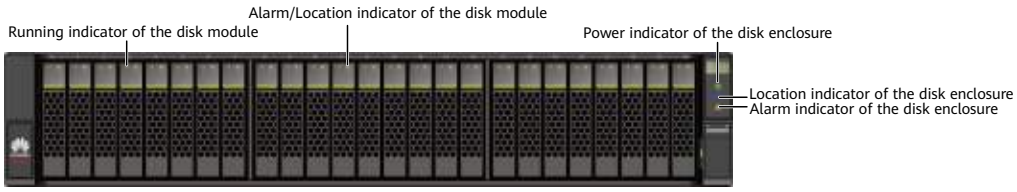


Table 3-38 describes meanings of the indicators on the front panel of a disk enclosure.

Table 3-38 Meanings of the indicators on the front panel

Module	Indicator	Status and Description
Disk module	Running indicator of the disk module	• Steady green: The disk module is working properly. • Blinking green (4 Hz or higher): Data is being read and written on the disk module. • Off: The disk module is powered off or incorrectly powered on.

Module	Indicator	Status and Description
	Alarm/Location indicator of the disk module	• Steady yellow: The disk module is faulty. • Blinking yellow (2 Hz): The disk module is being located. • Off: The disk module is working properly or hot swappable.
System subrack	Location indicator of the disk enclosure	• Blinking blue (2 Hz): The disk enclosure is being located. • Off: The disk enclosure is not located.
	Alarm indicator of the disk enclosure	• Steady yellow: An alarm is reported by the disk enclosure. • Off: The disk enclosure is working properly.
	Power indicator of the disk enclosure	• Steady green: The disk enclosure is powered on. • Off: The disk enclosure is powered off.

Indicators on the Rear Panel

Figure 3-89 shows the indicators on the rear panel of a disk enclosure.

Figure 3-89 Indicators on the rear panel of a disk enclosure (using the AC power module as an example)

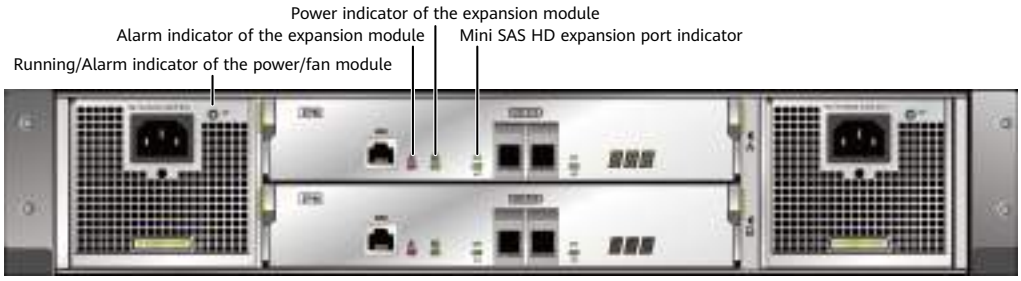


Table 3-39 describes meanings of the indicators on the rear panel of a disk enclosure.

Table 3-39 Meanings of the indicators on the rear panel

Module	Indicator	Status and Description
Expansion module	Alarm indicator of the expansion module	• Steady yellow: An alarm is reported by the expansion module. • Off: The expansion module is working properly.
	Power indicator of the expansion module	• Steady green: The expansion module is powered on. • Off: The expansion module is powered off.
	Mini SAS HD expansion port indicator	• Steady blue: The port transmission rate is 4 x 12 Gbit/s. • Steady green: The port transmission rate is 4 x 3 Gbit/s or 4 x 6 Gbit/s. • Steady yellow: The port is faulty. • Off: The port is not connected.
Power module	Running/Alarm indicator of the power/fan module	• Steady green: The power input is normal. • Blinking green (1 Hz): The power input is normal but the device is powered off. • Blinking green (4 Hz): The power module is being upgraded online. • Steady yellow: The power module or fan module is faulty. • Off: There is no external power input.

3.8 4 U SAS Disk Enclosure (with 3.5-Inch Disks)

This section describes a disk enclosure in terms of its hardware structure, component functions, front and rear views, and indicators.

3.8.1 Overview

The disk enclosure uses a modular design and consists of a system subrack, expansion modules, power modules, fan modules, and disk modules.

Overall Structure

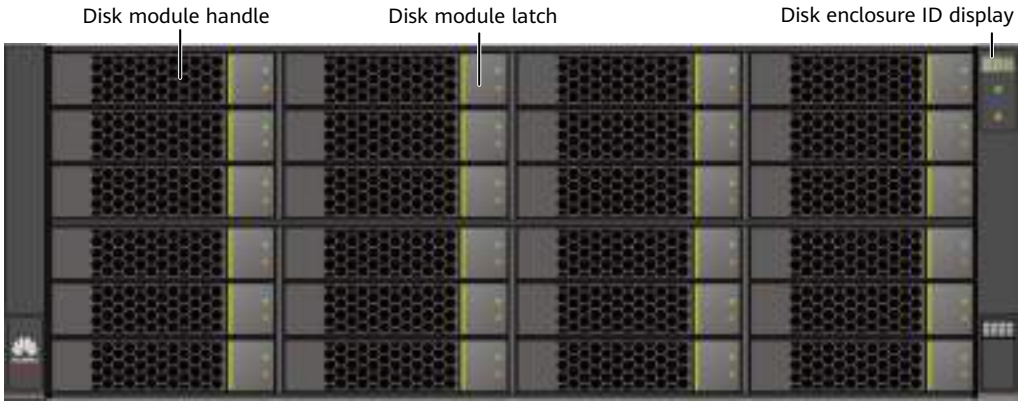
Figure 3-90 shows the overall structure of a disk enclosure.

Figure 3-90 Overall structure of a disk enclosure

Front View

Figure 3-91 shows the front view of a disk enclosure.

Figure 3-91 Front view of a disk enclosure



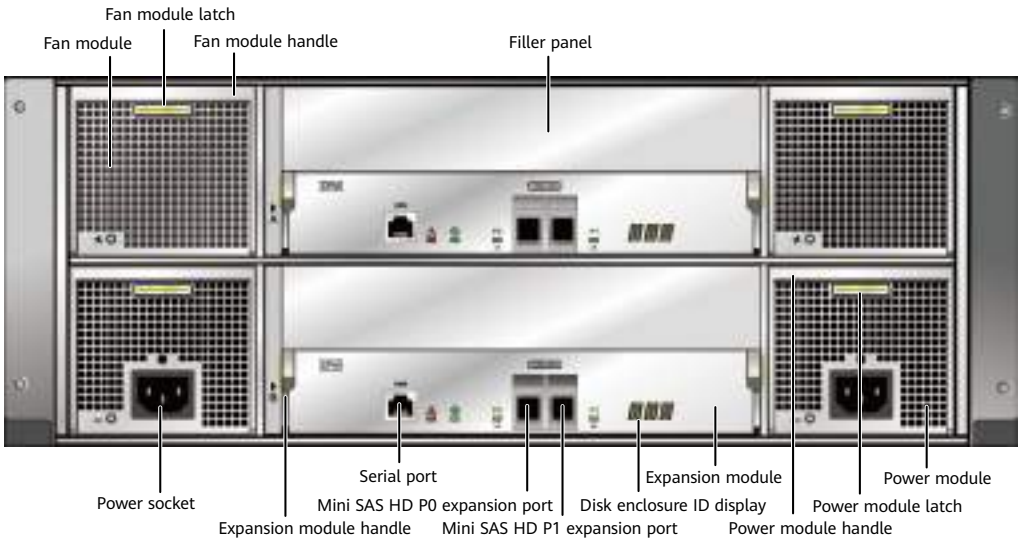
NOTE

The disk slots are numbered 0 to 23 from left to right and from top to bottom.

Rear View

Figure 3-92 shows the rear view of a disk enclosure.

Figure 3-92 Rear view of a disk enclosure (using the AC power module as an example)



NOTICE

Only serial cables can be inserted into serial ports. Do not insert network cables into serial ports.

Hardware Specifications

Table 3-40 lists the dimensions, weight, and power specifications of the disk enclosure. For more specifications, refer to Specifications Query (**https://support-it.huawei.com/spec/#/home**).

Table 3-40 Hardware specifications

Item	Specifications
Dimensions (H x W x D)	175 mm x 447 mm x 488 mm
Weight (excluding disks and auxiliary materials such as guide rails and cables)	23.95 kg
AC power voltage and rated current	800 W AC power supply (supporting 110 V dual-live-wire input (2W+PE) and 110 V single-live-wire input), 100 V to 240 V AC ±10%, 10 A, single-phase, 50/60 Hz
High-voltage DC	800 W power supply (240 V DC input), 192 V to 288 V, 10 A
Low-voltage DC	600 W power supply (supporting –48 V/–60 V DC input), –38.4 V to –75 V DC, 16 A

3.8.2 Component Description

This section provides the detailed illustration and description for each component.

3.8.2.1 System Subrack

The system subrack houses a midplane that provides reliable connections for interface modules and distributes power and signals to inner modules.

Appearance

Figure 3-93 shows the appearance of a system subrack.

Figure 3-93 System subrack

3.8.2.2 Expansion Module

An expansion module provides expansion ports for communication between the disk enclosure and the controller enclosure. Each expansion module provides two expansion ports P0 and P1.

Appearance

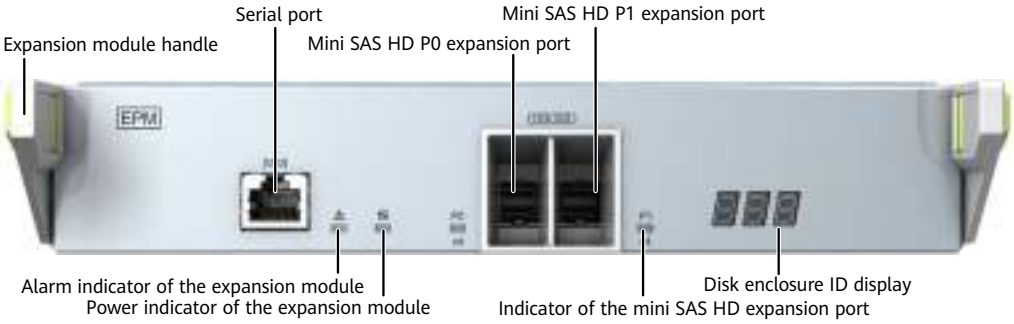
Figure 3-94 shows the appearance of an expansion module.

Figure 3-94 Expansion module

Ports

Figure 3-95 shows the ports on an expansion module.

Figure 3-95 Ports on an expansion module



NOTICE

Only serial cables can be inserted into serial ports. Do not insert network cables into serial ports.

Indicators

Table 3-41 describes the indicators on an expansion module.

Table 3-41 Indicators on an expansion module

Indicator	Status and Description
Alarm indicator of the expansion module	• Steady yellow: An alarm is reported by the expansion module. • Off: The expansion module is working properly.
Power indicator of the expansion module	• Steady green: The expansion module is powered on. • Off: The expansion module is powered off.
Mini SAS HD expansion port indicator	• Steady blue: The port transmission rate is 4 x 12 Gbit/s. • Steady green: The port transmission rate is 4 x 3 Gbit/s or 4 x 6 Gbit/s. • Steady yellow: The port is faulty. • Off: The port is not connected.

3.8.2.3 Power Module

Figure 3-96 shows the appearance of an AC power module. Figure 3-97 shows the appearance of a DC power module.

Figure 3-96 AC power module

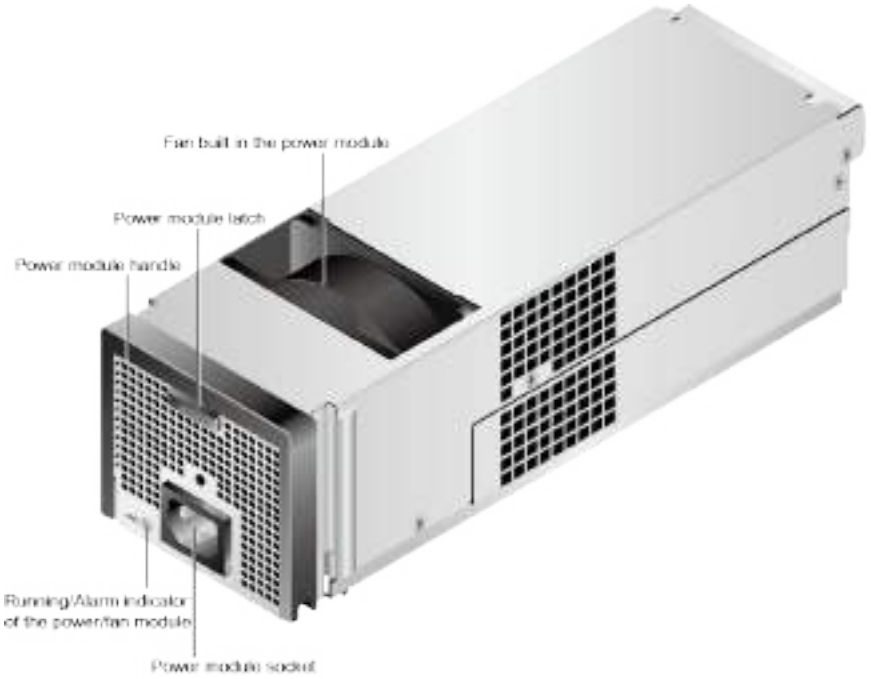
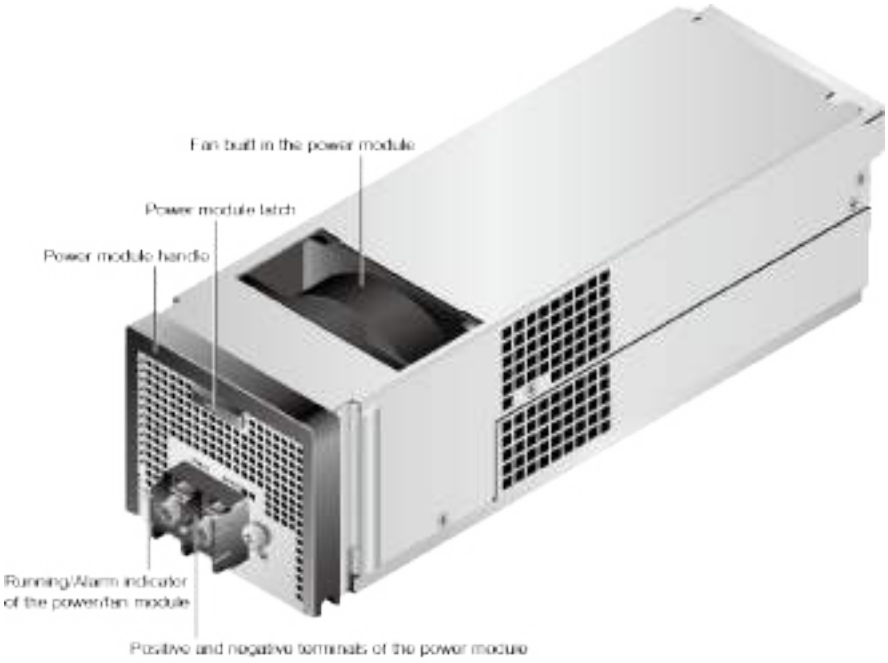


Figure 3-97 DC power module



Indicators

Table 3-42 describes indicators on a power module.

Table 3-42 Indicator on a power module

Indicator	Status and Description
Running/Alarm indicator of the power module	• Steady green: The power input is normal. • Blinking green (1 Hz): The power input is normal but the device is powered off. • Blinking green (4 Hz): The power module is being upgraded online. • Steady yellow: The power module or fan module is faulty. • Off: There is no external power input.

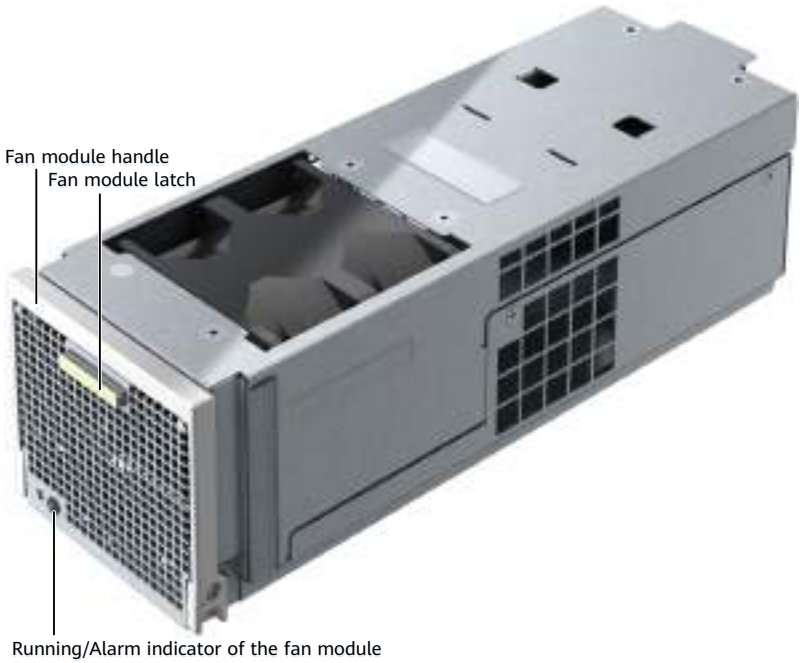
3.8.2.4 Fan Module

Fan modules dissipate heat from the system, allowing the disk enclosure to operate normally at maximum power.

Appearance

Figure 3-98 shows the appearance of a fan module.

Figure 3-98 Fan module



Indicators

Table 3-43 describes the indicators on a fan module.

Table 3-43 Indicator on the fan module

Indicator	Status and Description
Running/Alarm indicator of the fan module	• Steady green: The fan module is working properly. • Steady yellow: The fan module is faulty. • Off: The fan module is powered off.

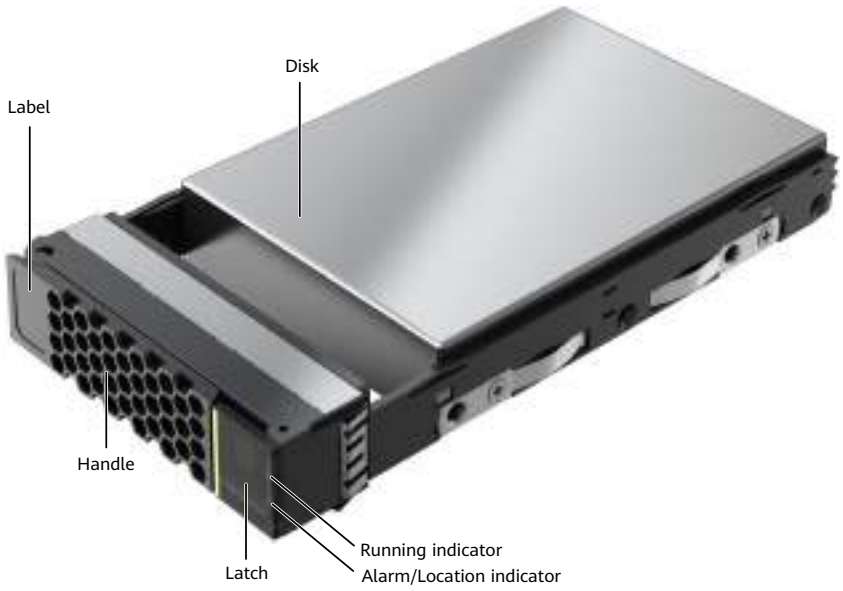
3.8.2.5 Disk Module

Disk modules provide storage capacity for a storage system to store service data.

Appearance

Figure 3-99 shows the appearance of a disk module.

Figure 3-99 Disk module



Indicators

Table 3-44 describes indicators on a disk module.

Table 3-44 Indicators on a disk module

Indicator	Status and Description
Alarm/Location indicator of the disk module	• Steady yellow: The disk module is faulty. • Blinking yellow (2 Hz): The disk module is being located. • Off: The disk module is working properly or hot swappable.
Running indicator of the disk module	• Steady green: The disk module is working properly. • Blinking green (4 Hz or higher): Data is being read and written on the disk module. • Off: The disk module is powered off or incorrectly powered on.

3.8.3 Indicator Description

After a disk enclosure is powered on, you can check the current operating status of the disk enclosure by observing its indicators.

Indicators on the Front Panel

Figure 3-100 shows the indicators on the front panel of a disk enclosure.

Figure 3-100 Indicators on the front panel of a disk enclosure

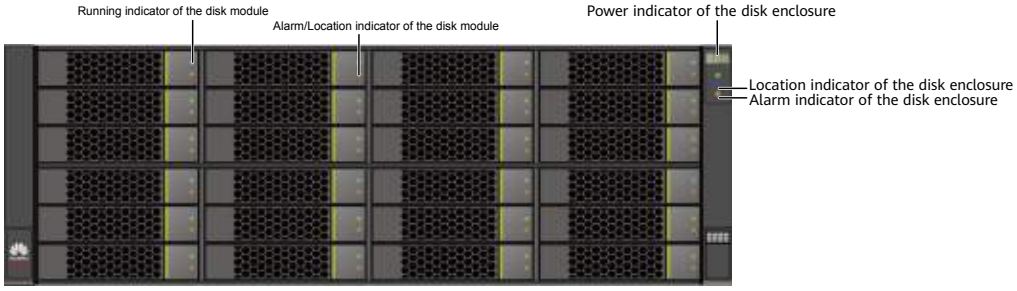


Table 3-45 describes meanings of the indicators on the front panel of a disk enclosure.

Table 3-45 Meanings of the indicators on the front panel

Module	Indicator	Status and Description
Disk module	Running indicator of the disk module	• Steady green: The disk module is working properly. • Blinking green (4 Hz or higher): Data is being read and written on the disk module. • Off: The disk module is powered off or incorrectly powered on.
	Alarm/Location indicator of the disk module	• Steady yellow: The disk module is faulty. • Blinking yellow (2 Hz): The disk module is being located. • Off: The disk module is working properly or hot swappable.
System subrack	Location indicator of the disk enclosure	• Blinking blue (2 Hz): The disk enclosure is being located. • Off: The disk enclosure is not located.
	Alarm indicator of the disk enclosure	• Steady yellow: An alarm is reported by the disk enclosure. • Off: The disk enclosure is working properly.
	Power indicator of the disk enclosure	• Steady green: The disk enclosure is powered on. • Off: The disk enclosure is powered off.

Indicators on the Rear Panel

Figure 3-101 shows the indicators on the rear panel of a disk enclosure.

Figure 3-101 Indicators on the rear panel of a disk enclosure (using the AC power module as an example)

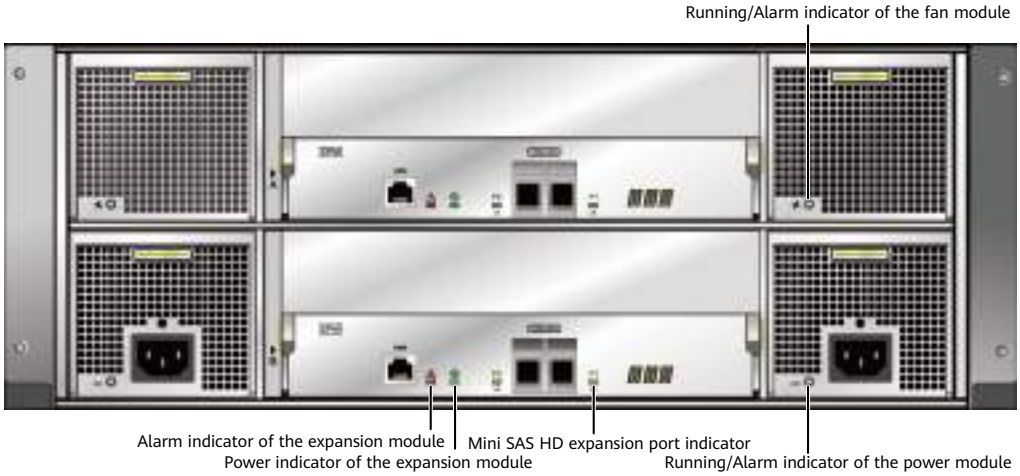


Table 3-46 describes meanings of the indicators on the rear panel of a disk enclosure.

Table 3-46 Meanings of the indicators on the rear panel

Module	Indicator	Status and Description
Fan module	Running/ Alarm indicator of the fan module	• Steady green: The fan module is working properly. • Steady yellow: The fan module is faulty. • Off: The fan module is powered off.
Power module	Running/ Alarm indicator of the power module	• Steady green: The power input is normal. • Blinking green (1 Hz): The power input is normal but the device is powered off. • Blinking green (4 Hz): The power module is being upgraded online. • Steady yellow: The power module is faulty. • Off: There is no external power input.
Expansion module	Mini SAS HD expansion port indicator	• Steady blue: The port transmission rate is 4 x 12 Gbit/s. • Steady green: The port transmission rate is 4 x 3 Gbit/s or 4 x 6 Gbit/s. • Steady yellow: The port is faulty. • Off: The port is not connected.
	Power indicator of the expansion module	• Steady green: The expansion module is powered on. • Off: The expansion module is powered off.

Module	Indicator	Status and Description
	Alarm indicator of the expansion module	• Steady yellow: An alarm is reported by the expansion module. • Off: The expansion module is working properly.

3.9 2 U Smart NVMe Disk Enclosure (with Palm-sized Disks)

This section describes a 2 U smart NVMe disk enclosure in terms of its hardware structure, component functions, front and rear views, and indicators.

3.9.1 Overview

The 2 U smart NVMe disk enclosure uses a modular design and consists of a system subrack, expansion modules, disk modules, and power modules.

Overall Structure

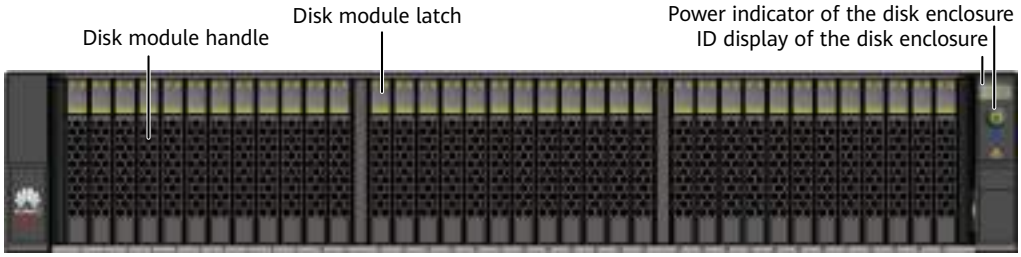
Figure 3-102 shows the overall structure of a 2 U smart NVMe disk enclosure.

Figure 3-102 Overall structure of a 2 U smart NVMe disk enclosure

Front View

Figure 3-103 shows the front view of a disk enclosure.

Figure 3-103 Front view of a disk enclosure



NOTE

- The disk slots are numbered 0 to 35 from left to right.
- The disk enclosure indicator is designed as a button, but the button function is reserved and currently unavailable.

Rear View

Figure 3-104 and Figure 3-105 show the rear view of a disk enclosure.

Figure 3-104 Rear view of a disk enclosure without USB ports (using the AC power module as an example)

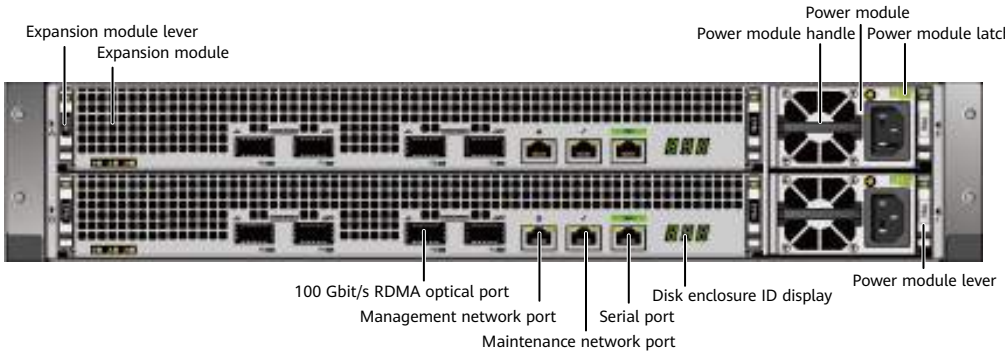
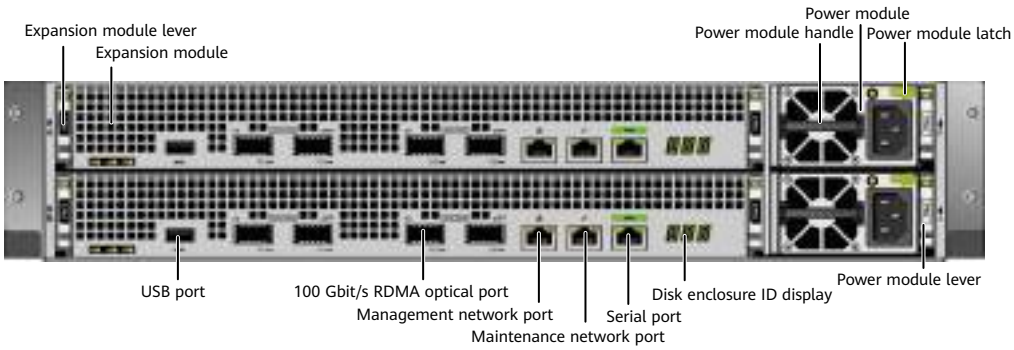


Figure 3-105 Rear view of a disk enclosure with USB ports (using the AC power module as an example)



NOTICE

Only serial cables can be inserted into serial ports. Do not insert network cables into serial ports.

NOTE

- The management, maintenance, and serial ports of a smart disk enclosure are reserved and do not need cable connections.
- The USB ports of a smart disk enclosure supply power to the status indicator on the front door of a disk bay only in the scenario where the 4 U controller enclosure is delivered as bay.

Hardware Specifications

Table 3-47 lists the dimensions, weight, and power specifications of the disk enclosure. For more specifications, refer to Specifications Query (**https://support-it.huawei.com/spec/#/home**).

Table 3-47 Hardware specifications

Item	Specifications
Dimensions (H x W x D)	86.1 mm x 447 mm x 620 mm
Weight (excluding disks and auxiliary materials such as guide rails and cables)	24.95 kg
AC power voltage and rated current	• 2000 W power supply (supporting 110 V dual-live-wire input (2W +PE)), 200 V to 240 V AC ±10%, 10 A, single-phase, 50/60 Hz • (Applicable to OceanStor 5310 and 5510) 900 W power supply (supporting 110 V dual-live-wire input (2W+PE) and 110 V single-live-wire input), 100 V to 240 V AC ±10%, 10 A, single-phase, 50/60 Hz
High-voltage DC (not supported in North America and Canada)	• 900 W power supply (240 V DC input), 192 V to 288 V DC, 5 A • (Applicable to OceanStor 5510) 2200 W power supply (336 V DC input), 260 V to 400 V, 10 A
Low-voltage DC	1200 W power supply (supporting –48 V/–60 V DC input), –38.4 V to –72 V DC, 32 A

3.9.2 Component Description

This section provides the detailed illustration and description for each component.

3.9.2.1 System Subrack

The system subrack houses a midplane that provides reliable connections for interface modules and distributes power and signals to inner modules.

Appearance

Figure 3-106 shows the appearance of a system subrack.

Figure 3-106 System subrack

3.9.2.2 Expansion Module

An expansion module provides expansion ports for communication between a disk enclosure and a controller enclosure, or between different disk enclosures. Each expansion module provides four expansion ports P0, P1, P2, and P3.

Appearance

Figure 3-107 shows the appearance of an expansion module.

Figure 3-107 Expansion module

Ports

Figure 3-108 and **Figure 3-109** show the ports on an expansion module.

Figure 3-108 Ports of an expansion module without a USB port

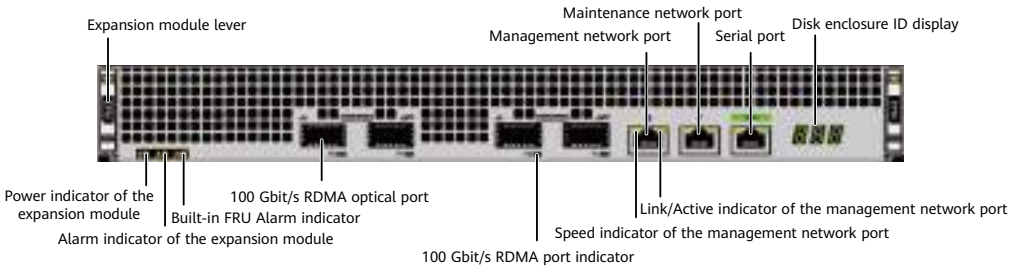
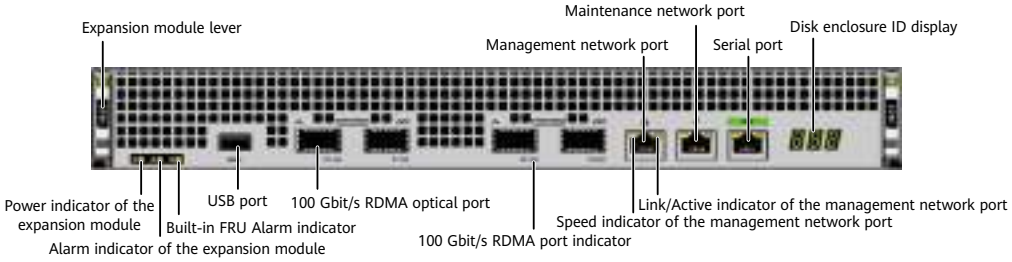


Figure 3-109 Ports of an expansion module with a USB port



NOTICE

Only serial cables can be inserted into serial ports. Do not insert network cables into serial ports.

NOTE

- The management, maintenance, and serial ports of a smart disk enclosure are reserved and do not need cable connections.
- The USB ports of a smart disk enclosure supply power to the status indicator on the front door of a disk bay only in the scenario where the 4 U controller enclosure is delivered as bay.

Indicators

For the indicators on an expansion module after the storage system is powered on, see **3.9.3 Indicator Description**.

3.9.2.3 Fan Module

Fan modules dissipate heat from the system, allowing the disk enclosure to operate normally at maximum power.

Appearance

Figure 3-110 shows the appearance of a fan module.

Figure 3-110 Fan module

Indicators

Fans are embedded inside expansion modules and do not have independent indicators. You can check the running status of fans by observing the indicators on the expansion modules.

3.9.2.4 Power Module

The disk enclosure uses AC and DC power modules to ensure proper running at maximum power.

Appearance

Figure 3-111 shows the appearance of an AC power module. **Figure 3-112** shows the appearance of a DC power module.

Figure 3-111 AC power module

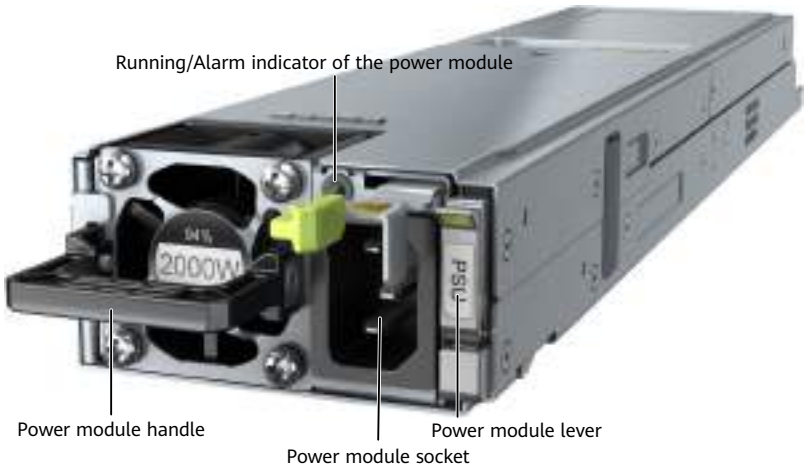


Figure 3-112 DC power module

Indicators

For the indicators on a power module after the storage system is powered on, see **3.9.3 Indicator Description**.

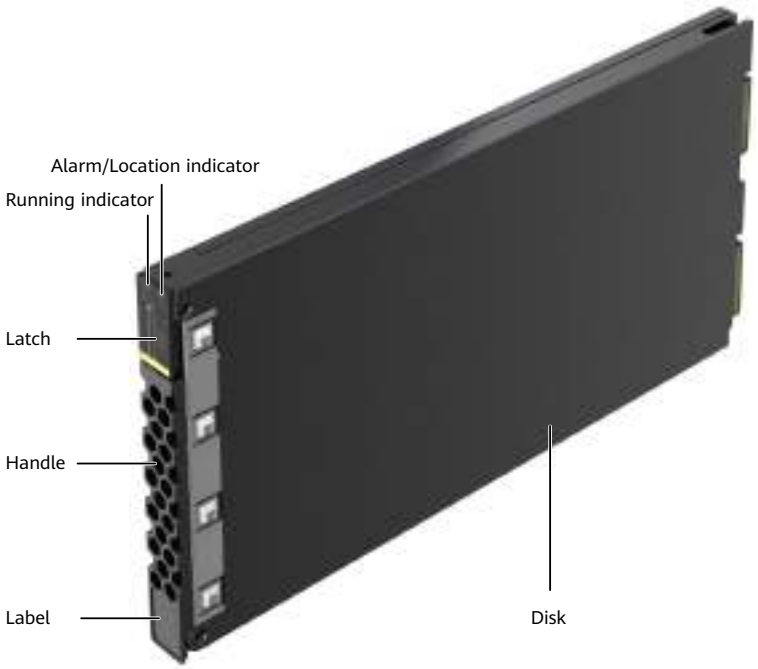
3.9.2.5 Disk Module

Disk modules provide storage capacity for a storage system. Disk modules can function as system coffer disks to save service data, system data, and cache data.

Appearance

Figure 3-113 shows the appearance of a disk module.

Figure 3-113 Disk module



Indicators

For the indicators on a disk module after the storage system is powered on, see **3.9.3 Indicator Description**.

3.9.3 Indicator Description

After a disk enclosure is powered on, you can check the current operating status of the disk enclosure by observing its indicators.

Indicators on the Front Panel

Figure 3-114 shows the indicators on the front panel of a disk enclosure.

Figure 3-114 Indicators on the front panel of a disk enclosure

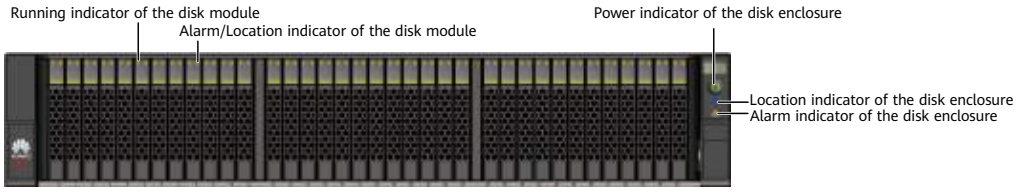


Table 3-48 describes meanings of the indicators on the front panel of a disk enclosure.

Table 3-48 Meanings of the indicators on the front panel

Module	Indicator	Status and Description
Disk module	Running indicator of the disk module	• Steady green: The disk module is working properly. • Blinking green (4 Hz): Data is being read and written on the disk module. • Off: The disk module is powered off or incorrectly powered on.
	Alarm/Location indicator of the disk module	• Steady yellow: The disk module is faulty. • Blinking yellow (2 Hz): The disk module is being located. • Off: The disk module is working properly or hot swappable.
System subrack	Location indicator of the disk enclosure	• Blinking blue (2 Hz): The disk enclosure is being located. • Off: The disk enclosure is not located.

Module	Indicator	Status and Description
	Alarm indicator of the disk enclosure	• Steady yellow: An alarm is reported by the disk enclosure. • Off: The disk enclosure is working properly.
	Power indicator of the disk enclosure	• Steady green: The disk enclosure is powered on. • Off: The disk enclosure is powered off.

Indicators on the Rear Panel

Figure 3-115 and Figure 3-116 show the indicators on the rear panel of a disk enclosure.

Figure 3-115 Indicators on the rear panel of a disk enclosure without USB ports (using the AC power module as an example)

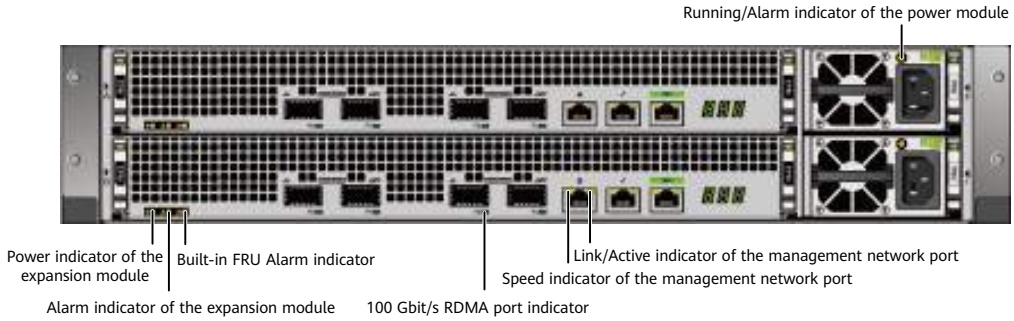


Figure 3-116 Indicators on the rear panel of a disk enclosure with USB ports (using the AC power module as an example)

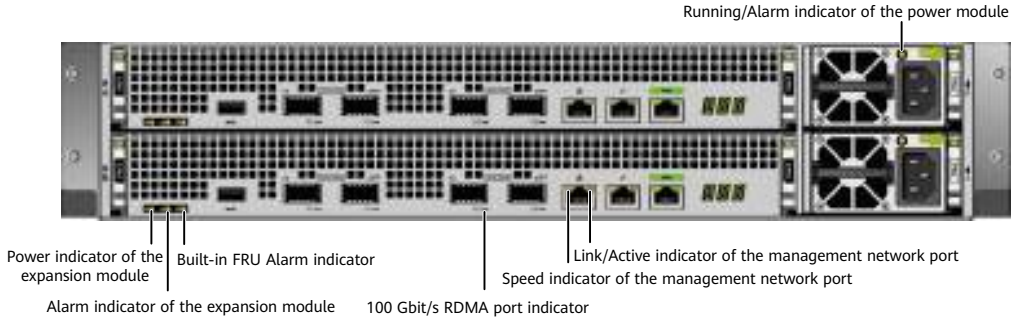


Table 3-49 describes meanings of the indicators on the rear panel of a disk enclosure.

Table 3-49 Meanings of the indicators on the rear panel

Module	Indicator	Status and Description
Expansion module	Alarm indicator of the expansion module	• Steady yellow: An alarm is reported by the expansion module. • Off: The expansion module is working properly.
	Power indicator of the expansion module	• Steady green: The expansion module is powered on. • Off: The expansion module is powered off.
	Built-in FRU Alarm indicator	• Steady yellow: A built-in FRU (fan module) of the controller is faulty. • Off: The built-in FRUs of the controller are normal.
	100 Gbit/s RDMA port indicator	• Steady blue: The speed is the highest. • Blinking blue (2 Hz): The port is transmitting data at the highest speed. • Steady green: The speed is not the highest. • Blinking green (2 Hz): The port is transmitting data, but not at the highest speed. • Steady yellow: The optical module or cable is faulty or not supported by the port. • Off: The port is not connected.
Power module	Running/Alarm indicator of the power module	• Steady green: The power input is normal. • Blinking green (1 Hz): The power input is normal but the device is powered off. • Blinking green (4 Hz): The power module is being upgraded online. • Steady yellow: The power module is faulty. • Off: There is no external power input.

3.10 High-Density Disk Enclosure

This section describes a high-density disk enclosure in terms of its hardware structure, component functions, front and rear views, and indicators.

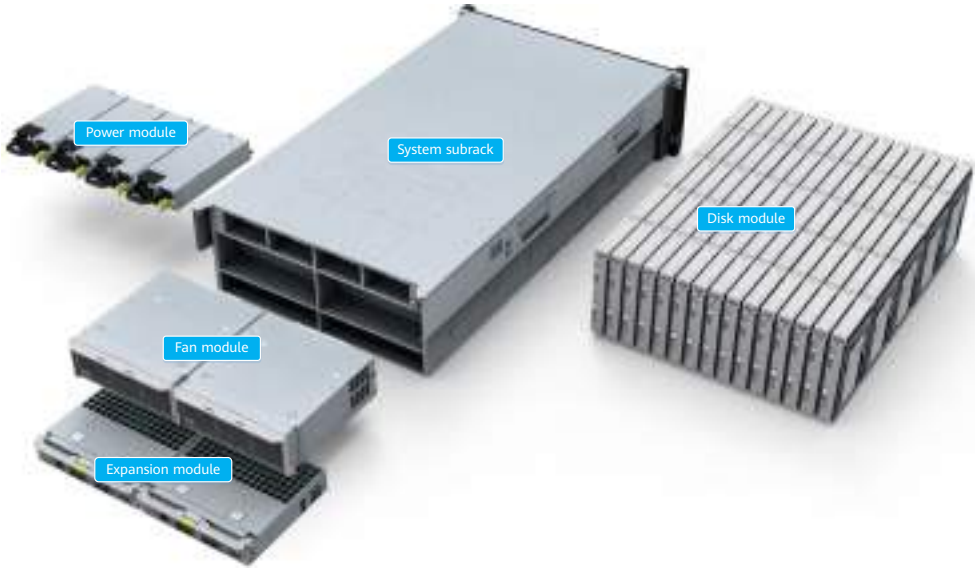
3.10.1 Overview

A high-density disk enclosure adopts a modular design and consists of a subrack, disk modules, fan modules, power modules, and expansion modules.

Overall Structure

Figure 3-117 shows the overall structure of a high-density disk enclosure.

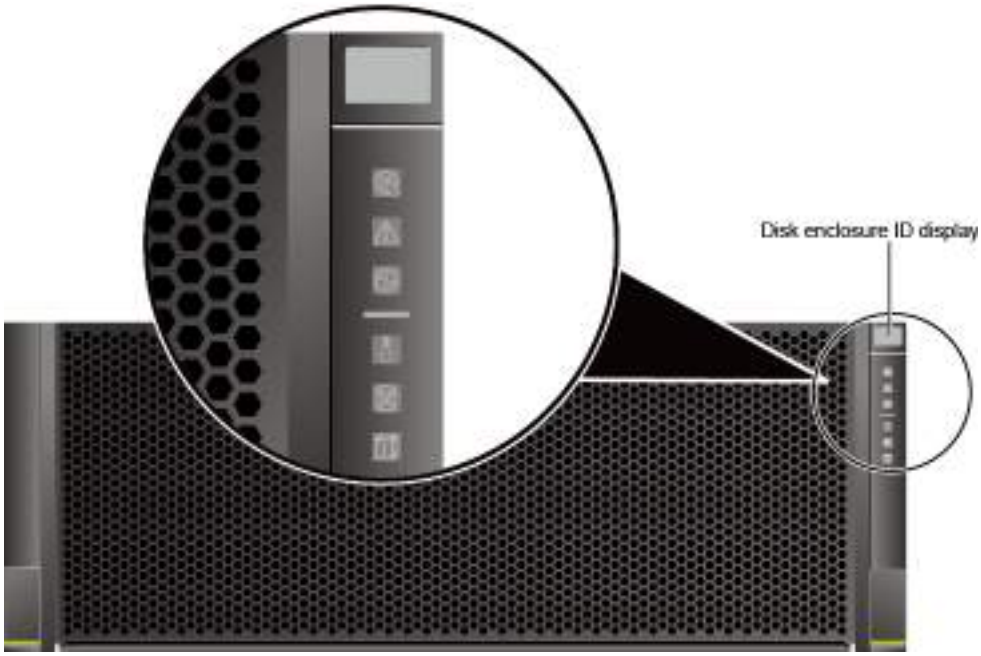
Figure 3-117 Overall structure of a high-density disk enclosure



Front View

Figure 3-118 shows the front view of a high-density disk enclosure.

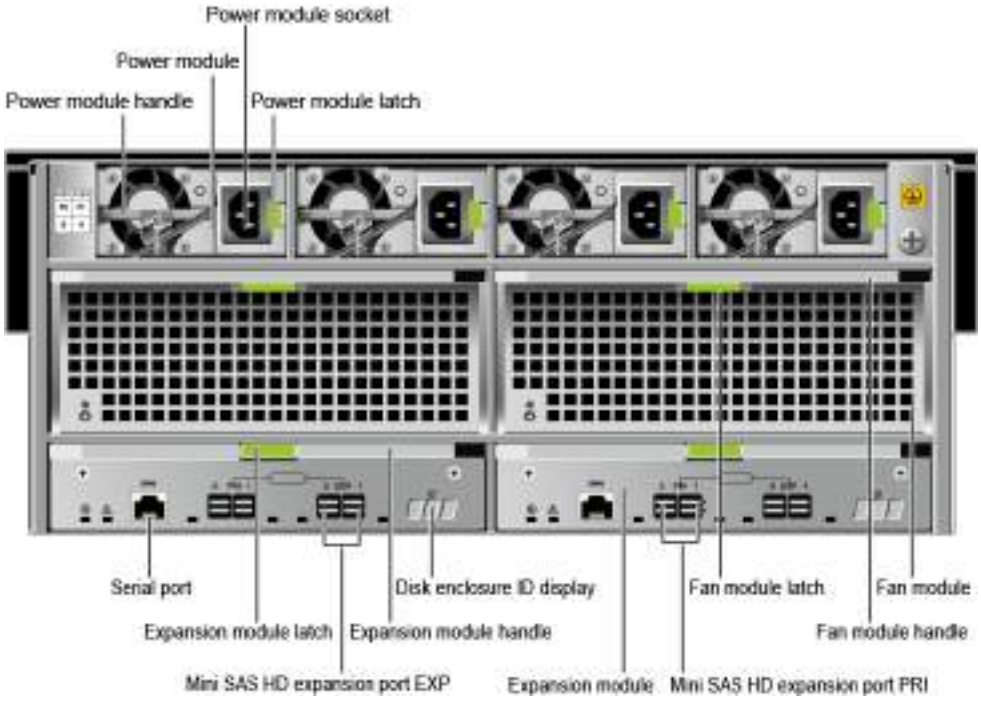
Figure 3-118 Front view of a high-density disk enclosure



Rear View

Figure 3-119 shows the rear view of a high-density disk enclosure.

Figure 3-119 Rear view of a high-density disk enclosure



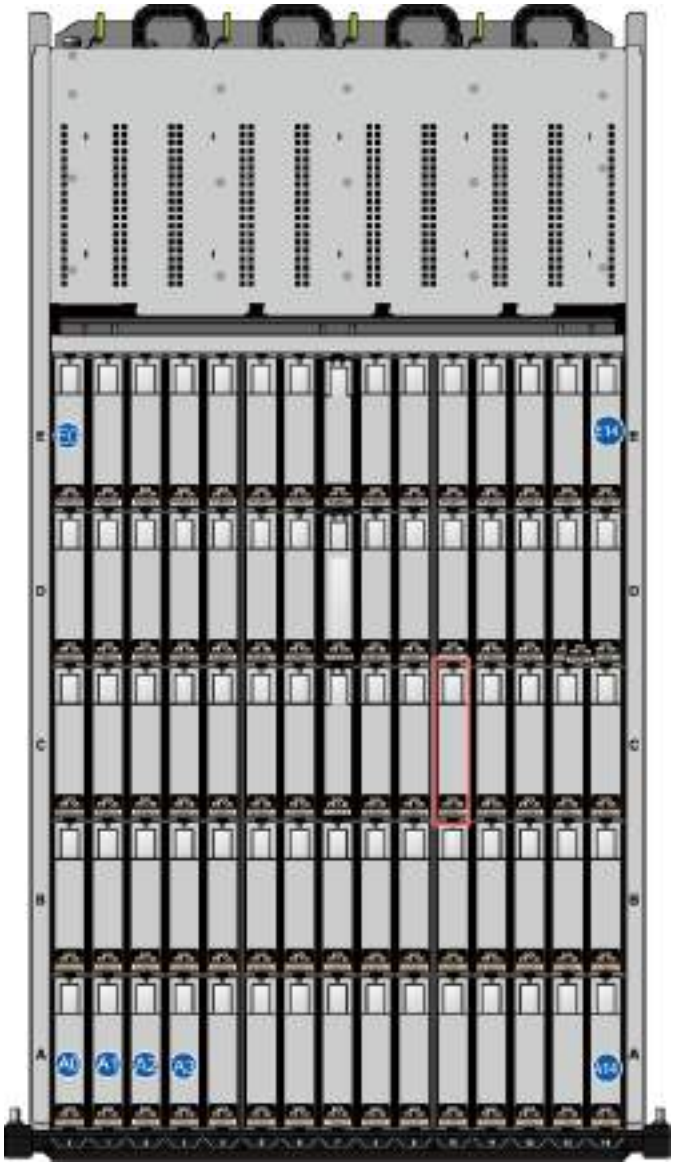
NOTICE

Only serial cables can be inserted into serial ports. Do not insert network cables into serial ports.

Top View

Figure 3-120 shows the top view of a high-density disk enclosure.

Figure 3-120 Top view of a high-density disk enclosure



The disk number of a high-density disk enclosure displayed on DeviceManager or CLI ranges from 0 to 74. These disks are numbered from left to right (15 columns) and from bottom to top (five rows). The slots of a high-density disk enclosure are numbered 0 to 14 from left to right (15 columns), and A to E from bottom to top (five rows). For example, in the preceding figure, the disk in the red box is numbered 40 in slot C10.

Table 3-50 lists the mappings between disk numbers and slot numbers of high-density disk enclosures.

Table 3-50 Mappings between disk numbers and slot numbers of high-density disk enclosures

Disk No.	Slot No.	Disk No.	Slot No.	Disk No.	Slot No.	Disk No.	Slot No.	Disk No.	Slot No.
0	A0	15	B0	30	C0	45	D0	60	E0
1	A1	16	B1	31	C1	46	D1	61	E1
2	A2	17	B2	32	C2	47	D2	62	E2
3	A3	18	B3	33	C3	48	D3	63	E3
4	A4	19	B4	34	C4	49	D4	64	E4
5	A5	20	B5	35	C5	50	D5	65	E5
6	A6	21	B6	36	C6	51	D6	66	E6
7	A7	22	B7	37	C7	52	D7	67	E7
8	A8	23	B8	38	C8	53	D8	68	E8
9	A9	24	B9	39	C9	54	D9	69	E9
10	A10	25	B10	40	C10	55	D10	70	E10
11	A11	26	B11	41	C11	56	D11	71	E11
12	A12	27	B12	42	C12	57	D12	72	E12
13	A13	28	B13	43	C13	58	D13	73	E13
14	A14	29	B14	44	C14	59	D14	74	E14

Hardware Specifications

Table 3-51 lists the dimensions and weight of the disk enclosure. For more specifications, refer to Specifications Query (**https://support-it.huawei.com/spec/#/home**).

Table 3-51 Hardware specifications

Item	Specifications
Dimensions (H x W x D)	• 176.5 mm x 446 mm x 790 mm (without a cable tray) • 176.5 mm x 446 mm x 974 mm (with a cable tray)
Weight (excluding disks and auxiliary materials such as guide rails and cables)	50.5 kg

3.10.2 Component Description

This section provides the detailed illustration and description for each component.

3.10.2.1 System Subrack

The system subrack houses a midplane that provides reliable connections for interface modules and distributes power and signals to inner modules.

Appearance

Figure 3-121 shows the appearance of a system subrack.

Figure 3-121 System subrack

3.10.2.2 Expansion Module

An expansion module provides expansion ports for communication between a high-density disk enclosure and a controller enclosure, or between different high-density disk enclosures. Each expansion module provides two PRI HD expansion ports and two EXP HD expansion ports.

Appearance

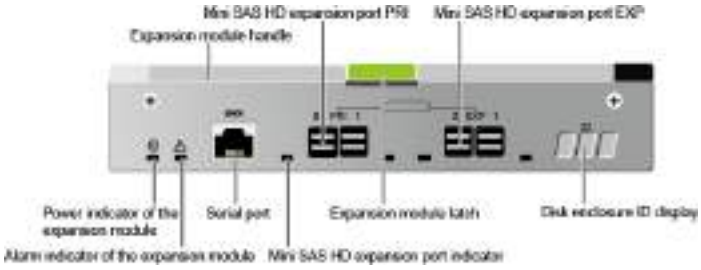
Figure 3-122 shows the appearance of an expansion module.

Figure 3-122 Expansion module

Ports

Figure 3-123 shows the ports on an expansion module.

Figure 3-123 Ports on an expansion module



NOTICE

Only serial cables can be inserted into serial ports. Do not insert network cables into serial ports.

Indicators

Table 3-52 describes the indicators on an expansion module.

Table 3-52 Indicators on an expansion module

Indicator	Status and Description
Power indicator of the expansion module	• Steady green: The expansion module is working properly. • Off: The expansion module is powered off.
Alarm indicator of the expansion module	• Steady red: An alarm is reported by the expansion module. • Off: The expansion module is powered off or working correctly.
Mini SAS HD expansion port indicator	• Steady blue: The link to the expansion port is normal, and the data transmission rate is 4 x 12 Gbit/s. • Steady green: The link to the expansion port is normal, and the data transmission rate is 4 x 6 Gbit/s. • Steady red: The port is faulty. • Off: The link to the expansion port is down.

3.10.2.3 Disk Module

Disk modules provide storage capacity for a storage system to store service data.

Appearance

Figure 3-124 shows the appearance of a disk module.

Figure 3-124 Disk module

Indicators

Table 3-53 describes indicators on a disk module.

Table 3-53 Indicators on a disk module

Indicator	Status and Description
Status indicator of the disk module	• Steady green: The disk module is working properly. • Blinking green: Data is being read and written on the disk module. • Steady red: The disk module is faulty. • Blinking red: The disk module is being located. • Off: The disk module is powered off or incorrectly powered on.

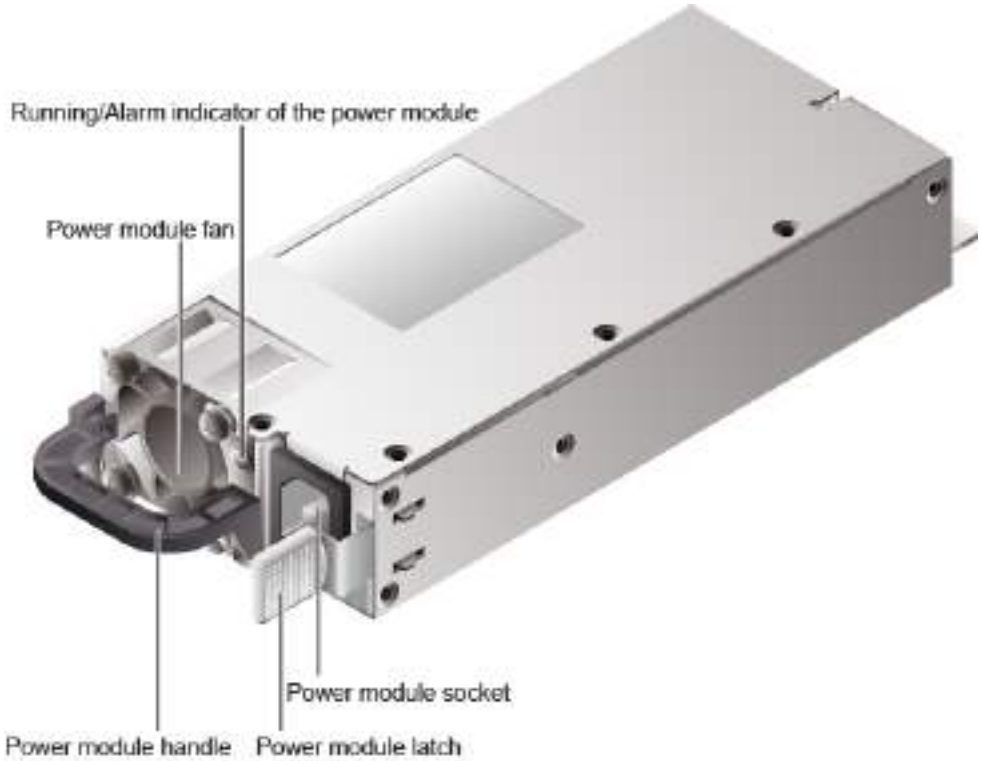
3.10.2.4 Power Module

The high-density disk enclosure uses AC power modules to ensure proper running at maximum power.

Appearance

Figure 3-125 shows the appearance of a power module.

Figure 3-125 AC power module



Indicators

Table 3-54 describes indicators on a power module.

Table 3-54 Indicator on a power module

Indicator	Status and Description
Running/Alarm indicator of the power module	• Steady green: The power module is working properly. • Off: The power module is powered off, or an undervoltage, overvoltage, overtemperature, or short-circuit occurs.

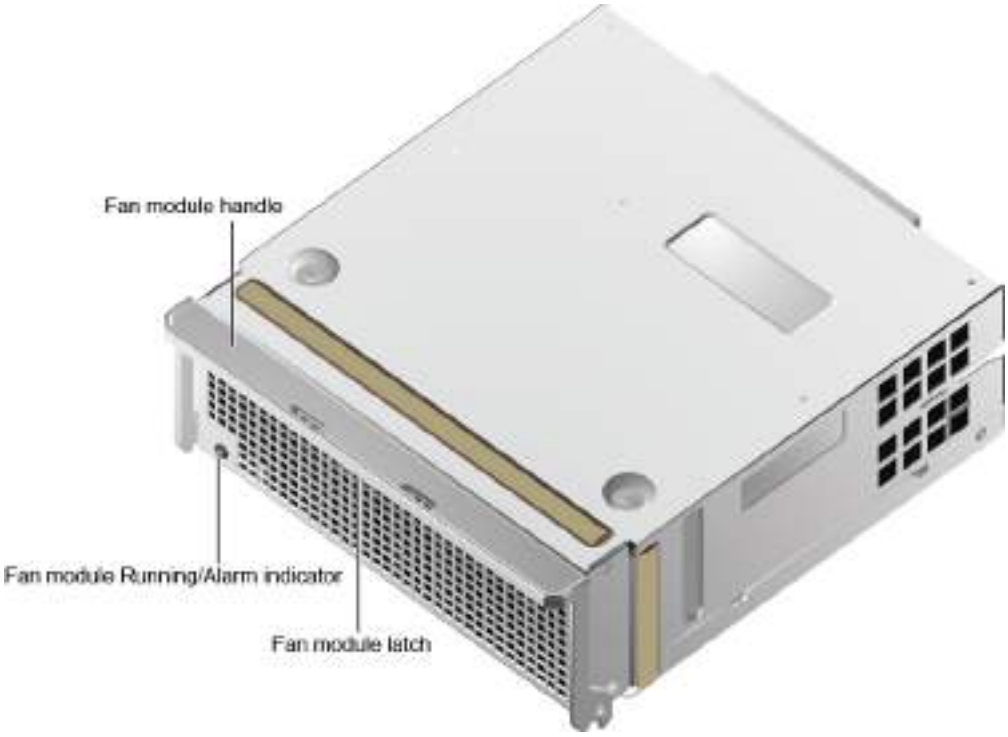
3.10.2.5 Fan Module

Fan modules dissipate heat from the system, allowing the disk enclosure to operate normally at maximum power.

Appearance

Figure 3-126 shows the appearance of a fan module.

Figure 3-126 Fan module



Indicators

Table 3-55 describes the indicators on a fan module.

Table 3-55 Indicator on the fan module

Indicator	Status and Description
Running/Alarm indicator of the fan module	• Steady green: The fan module is working properly. • Steady red: The fan module is faulty. • Off: The fan module is powered off.

3.10.3 Indicator Description

After a disk enclosure is powered on, you can check the current operating status of the disk enclosure by observing its indicators.

Indicators on the Front Panel

Figure 3-127 shows the indicators on the front panel of a high-density disk enclosure.

Figure 3-127 Indicators on the front panel of a high-density disk enclosure

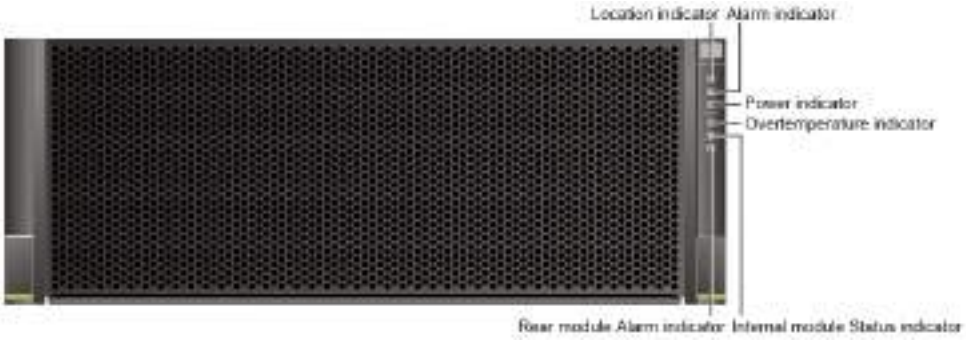


Table 3-56 describes the indicators on the front panel of a high-density disk enclosure.

Table 3-56 Meanings of the indicators on the front panel

Module	Indicator	Status and Description
System subrack	Location indicator	• Blinking blue: The high-density disk enclosure is being located. • Off: The high-density disk enclosure is not located.

Module	Indicator	Status and Description
	Alarm indicator	• Steady red: An alarm is reported by the high-density disk enclosure. • Off: The high-density disk enclosure is working properly.
	Power indicator	• Steady green: The high-density disk enclosure is powered on. • Off: The high-density disk enclosure is powered off.
	Overtemperature indicator	• Steady red: The temperature of the high-density disk enclosure is too high. • Off: The temperature of the high-density disk enclosure is within the normal range.
	Status indicator of internal modules	• Steady red: A disk module in the high-density disk enclosure is faulty. • Off: The disk modules in the high-density disk enclosure are working properly.
	Alarm indicator of rear modules	• Steady red: The number of rear field replaceable units (FRUs) is fewer than half of that in standard configuration, or rear FRUs are faulty. **NOTE** The rear FRUs of a high-density disk enclosure include power modules, fan modules, and expansion modules. • Off: The rear FRUs are working properly.

Indicators on the Rear Panel

Figure 3-128 shows the indicators on the rear panel of a high-density disk enclosure.

Figure 3-128 Indicators on the rear panel of a high-density disk enclosure

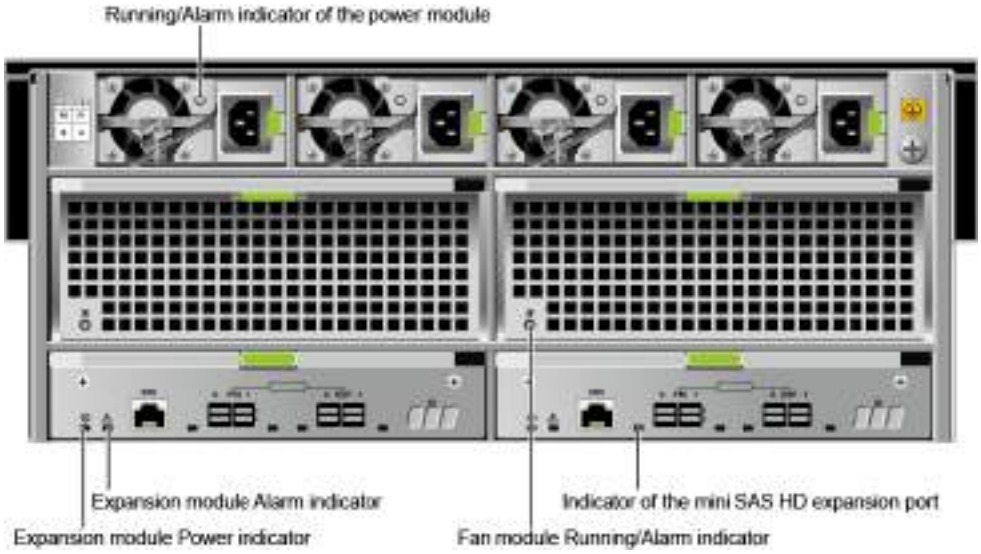


Table 3-57 describes the indicators on the rear panel of a high-density disk enclosure.

Table 3-57 Meanings of the indicators on the rear panel

Module	Indicator	Status and Description
Power module	Running/Alarm indicator of the power module	• Steady green: The power module is working properly. • Off: The power module is powered off, or an undervoltage, overvoltage, overtemperature, overcurrent, fan fault, or short-circuit occurs.
Expansion module	Mini SAS HD expansion port indicator	• Steady blue: The link to the expansion port is normal, and the data transmission rate is 4 x 12 Gbit/s. • Steady green: The link to the expansion port is normal, and the data transmission rate is 4 x 6 Gbit/s. • Steady red: The port is faulty. • Off: The link to the expansion port is down.

Module	Indicator	Status and Description
Fan module	Running/Alarm indicator of the fan module	• Steady green: The fan module is working properly. • Steady red: The fan module is faulty. • Off: The fan module is powered off.
Expansion module	Alarm indicator of the expansion module	• Steady red: An alarm is reported by the expansion module. • Off: The expansion module is working properly.
	Power indicator of the expansion module	• Steady green: The expansion module is working properly. • Off: The expansion module is powered off.

3.11 Coffer Disk

Coffer disks are used to store three types of data: storage system data, system configuration information and logs, and cache data requiring power failure protection.

Each controller has built-in disks as coffer disks. **Table 3-58** lists the partitions of the built-in coffer disks.

Table 3-58 Partitions of the built-in coffer disks

Built-in Coffer Disk	OceanStor 5310	OceanStor 5510	OceanStor 5610	Description
Size	1 x 64 GB M.2 SATA	1 x 240 GB M.2 SATA		-
Cache dirty data partition	9.5 GB	21 GB	32 GB	Stores the cache dirty data that has not been written to disks in the event of a power failure of the storage system.
OS system partition	32 GB			Stores the OceanStor OS system data.
Cluster Configuration Database (CCDB) partition	3 GB			Stores the user configuration information (such as remote replication, HyperMetro, and NAS data).

Built-in Coffer Disk	OceanStor 5310	OceanStor 5510	OceanStor 5610	Description
LogZone partition	2 GB			Stores system logs and run logs when the storage system is powered off or switches to write-through mode.
DB partition	1 GB			Stores the user configuration information (such as the LUN capacity, ID, WWN, Fibre Channel ports, and iSCSI ports).

3.12 Data Switch (CE8850-SAN)

Data switches provide a high bandwidth and low latency to connect controller enclosures for their control information exchange and service data flows.

Data switches are typically used for connections between multiple controller enclosures when:

- The storage system is installed for the first time. For detailed connection diagrams and configurations, see the *Installation Guide* specific to your product model.
- The storage system capacity is expanded. To expand the capacity of storage components, contact the technical support center.

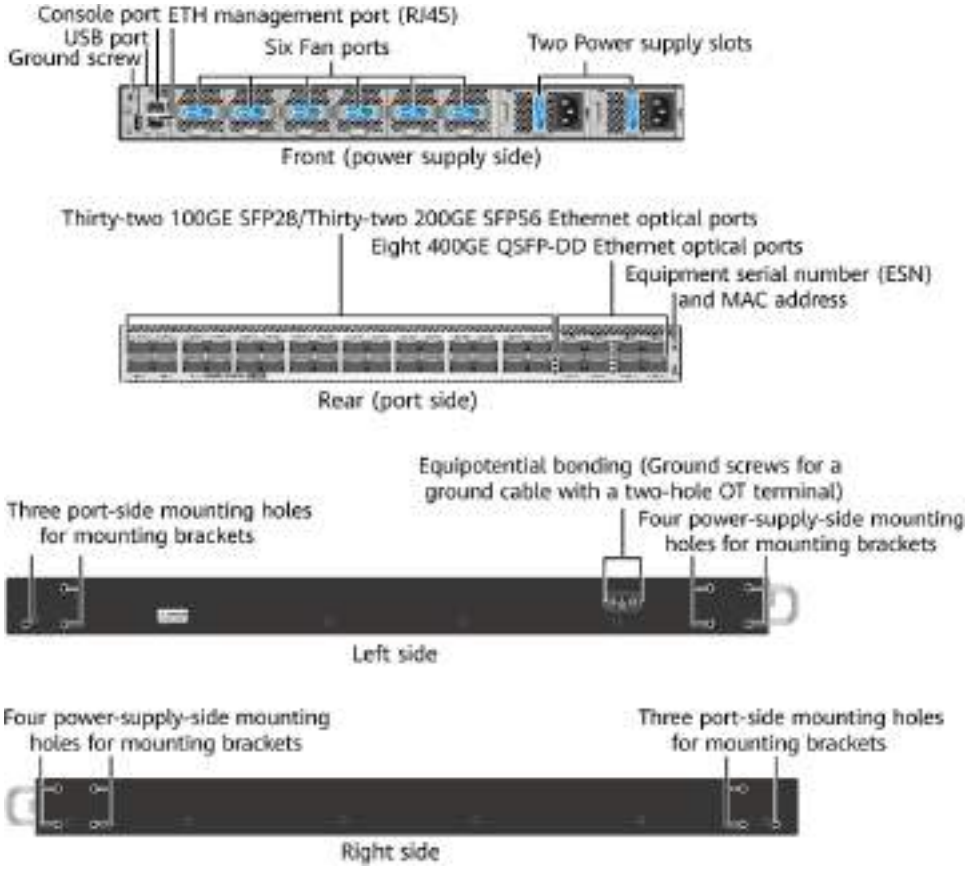
NOTE

The switches used for controller expansion can be deployed on a scale-out network only, not for front-end service networking or other purposes.

Appearance

Figure 3-129 shows the appearance of a data switch.

Figure 3-129 Data switch appearance



Indicators

The following figures and tables show and describe the indicators on a data switch.

Figure 3-130 Indicators on the data switch (rear view)

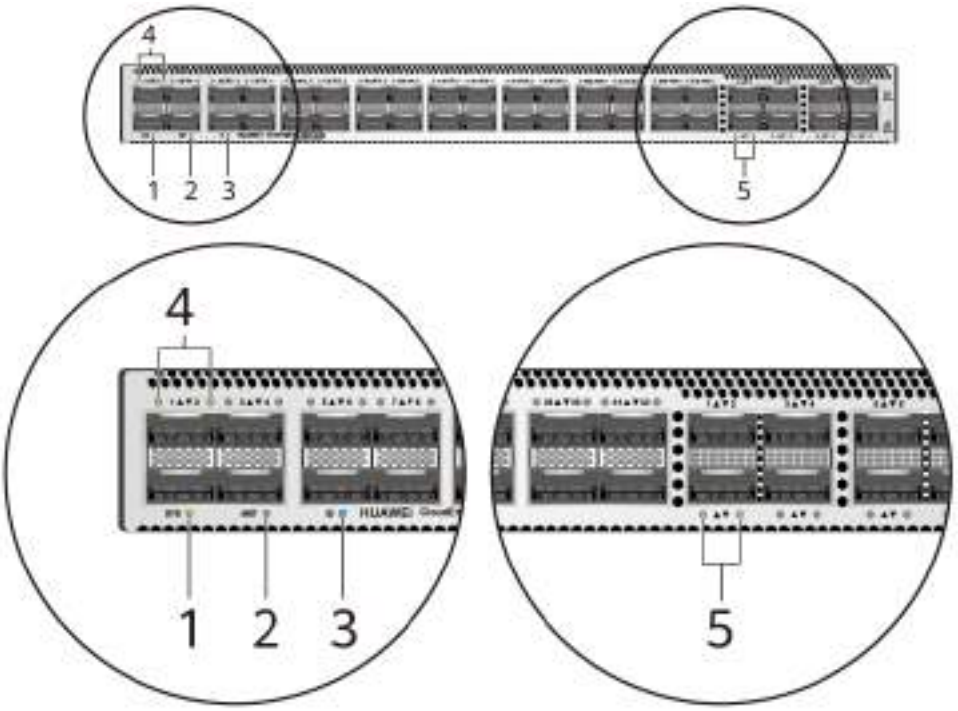


Figure 3-131 Indicators on the data switch (front view)

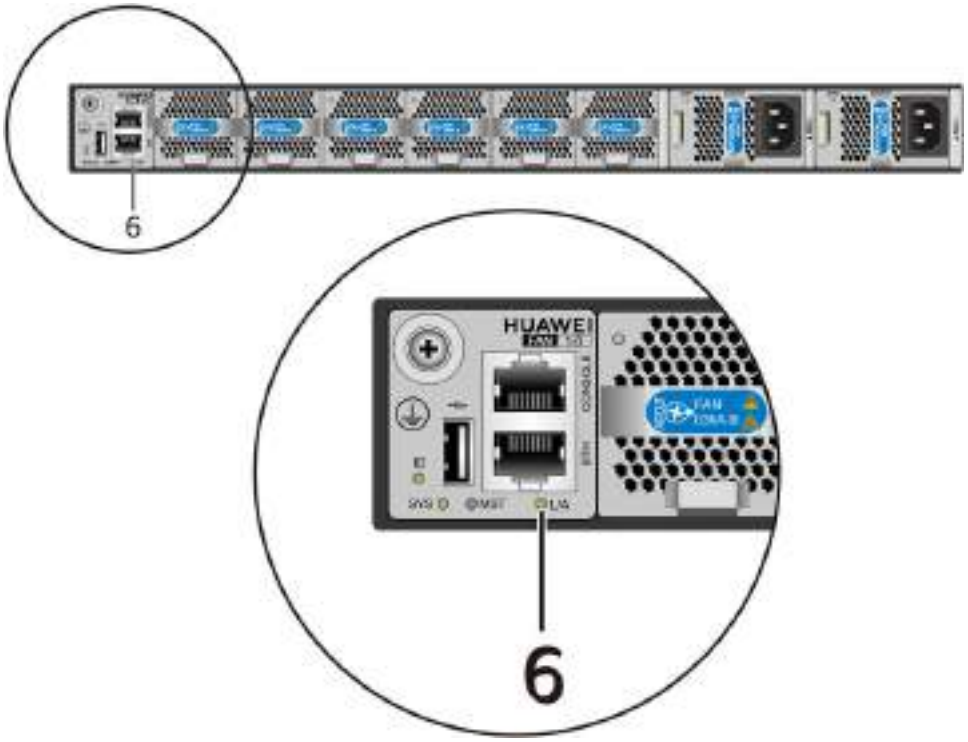


Table 3-59 Indicators

No.	Indicator	Name	Color and State	Meaning
1	SYS	System status indicator	Off	The system is not running.
			Green, blinking fast	The system is starting.
			Green, blinking slowly	The system is running normally.
			Red, steady on	• The system fails to start. • At least one power module does not work normally. • At least one fan module does not work normally.
2	MST	Stack master/ slave indicator	Off	The switch does not support stacking.
3	ID	ID indicator	Off	The ID indicator is not used (off by default).
			Blue, steady on	The ID indicator can be turned on or off remotely to help field engineers find the switch to maintain.
4	-	Service port indicator (200GE/ 100GE/40GE optical port) Arrowheads show the positions of ports. A down arrowhead indicates a port at the bottom, and an up arrowhead indicates a port at the top.	Off	No link has been established on the port or the port has been shut down.
			Green, steady on	A link is established on the port.
			Green, blinking	The port is sending or receiving data.
5	-	Service port indicator	Off	No link has been established on the port or the port has been shut down.

No.	Indicator	Name	Color and State	Meaning
		(400GE optical port) Arrowheads show the positions of ports. A down arrowhead indicates a port at the bottom, and an up arrowhead indicates a port at the top.	Green, steady on	A link is established on the port.
			Green, blinking	The port is sending or receiving data.
6	L/A	ETH management port indicator	Off	No link is established on the port.
			Green, steady on	A link is established on the port.
			Green, blinking	The port is sending or receiving data.

3.13 (Optional) Quorum Server

This section describes Huawei quorum servers: 1288H V5 and TaiShan 200 (2280 balanced model).

NOTE

When HyperMetro is used, the storage systems can also connect to third-party quorum servers. For the compatibility requirements on third-party quorum servers, see **Huawei Storage Interoperability Navigator**.

3.13.1 (Optional) Quorum Server (1288H V5)

For HyperMetro, if the heartbeats between two storage systems are interrupted, the quorum server decides which storage system continues providing services, thereby greatly improving host service continuity.

Front Panel of the Quorum Server

Figure 3-132 shows the front panel of the quorum server.

Figure 3-132 Front panel of the quorum server

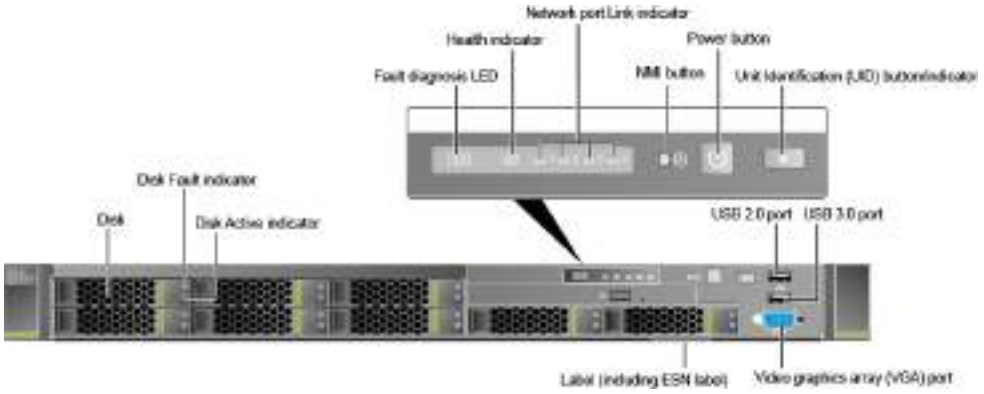


Table 3-60 describes the indicators and buttons on the quorum server front panel.

Table 3-60 Indicators and buttons on the front panel

Indicator and Button	Color	State
Fault diagnosis LED	None	• ---: The quorum server is operating properly. • **Error Code**: A fault occurs in quorum server hardware.
Power button/ indicator	Yellow and green	• Off: The device is not powered on. • Blinking yellow: The system is being started. • Steady yellow: The system is in the standby state. • Steady green: The system is properly powered on. **NOTE** You can hold down the power button for 6 seconds to power off the quorum server.
Unit Identification (UID) button/ indicator	Blue	The UID button/indicator helps identify and locate a quorum server in a rack. You can turn on or off the UID indicator by manually pressing the UID button or remotely running a command on the iBMC. • Steady on: The quorum server is located. • Off: The quorum server is not located. • You can hold down the UID button for 4 to 6 seconds to reset the system.

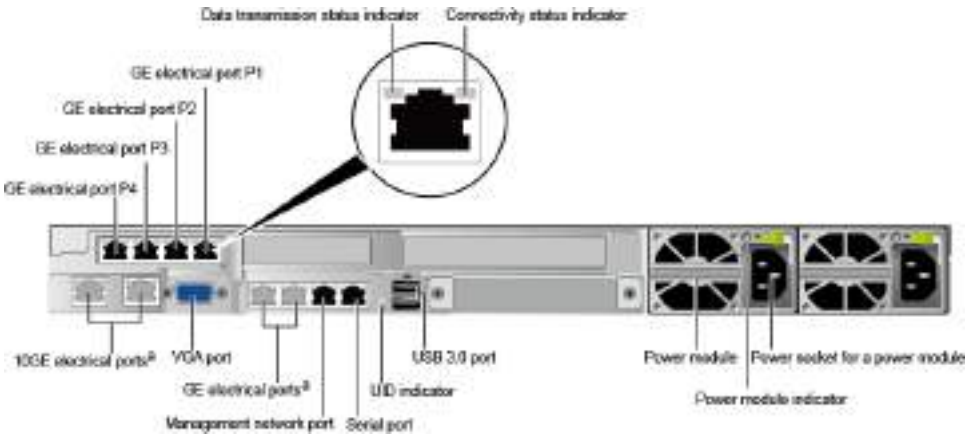
Indicator and Button	Color	State
Health indicator	Red and green	• Steady green: The device is operating properly. • Blinking red at 1 Hz: A major alarm is generated. • Blinking red at 5 Hz: A critical alarm is generated.
NMI button	None	The NMI button triggers a quorum server to generate a non-maskable interrupt. You can press this button or control it remotely through the WebUI. **NOTE** • Click the NMI button only when the OS is abnormal. Do not click this button when the quorum server is operating properly. • Click the NMI button only for internal commissioning. Before clicking this button, ensure that the OS has the handler for NMI interrupt. Otherwise, the OS may crash. Exercise caution when clicking this button.
Disk Active indicator	Green	• Off: The disk is not detected or is faulty. • Blinking green: Data is being read from, written to the disk, or synchronized between disks. • Steady green: The disk is inactive.
Disk Fault indicator	Yellow	• Off: The disk is working properly or disks cannot be detected in the RAID group. • Blinking yellow: The disk is being located, or the RAID is being reconstructed. • Steady yellow: The disk is faulty or member disks in the RAID group are abnormal.

Indicator and Button	Color	State
Network port Link indicator	Green	Each indicator shows the status of an Ethernet port on the network interface card (NIC). • Steady green: The port is properly connected. • Off: The port is not in use. **NOTE** If the NIC provides only two network ports, network port indicators 1 and 2 on the front panel are used.

Rear View of the Quorum Server

Figure 3-133 shows the rear view of the quorum server.

Figure 3-133 Rear view of the quorum server



NOTE

- The default IP address of the management network port on the quorum server is 192.168.2.100, and the default subnet mask is 255.255.255.0.
- a: This port is reserved and does not have any function. Do not connect cables here.

Table 3-61 describes the indicators on the quorum server rear panel.

Table 3-61 Indicators on the rear panel

Indicator	Color	State
Data transmission status indicator	Yellow	• Off: No data is being transmitted. • Blinking: Data is being transmitted.
Connectivity status indicator	Green	• Steady green: The port is properly connected. • Off: The port is not in use.

Indicator	Color	State
UID indicator	Blue	The UID indicator helps identify and locate a quorum server. You can turn on or off the UID indicator by manually pressing the UID button or remotely running a command. • Steady on: The quorum server is located. • Off: The quorum server is not located. • You can hold down the UID button for 4 to 6 seconds to reset the system.
Power module indicator	Green	• Steady green: The power input is normal. • Off: There is no AC power input, or the power module is in the standby state or is faulty.

3.13.2 (Optional) Quorum Server (TaiShan 200)

This section describes the 2280 balanced model (2280 for short) of the TaiShan 200 server. For HyperMetro, if the heartbeats between two storage systems are interrupted, the quorum server decides which storage system continues providing services, thereby greatly improving host service continuity.

Front Panel Components

Figure 3-134 shows the components on the front panel of a server with 12 x 3.5-inch disks.

Figure 3-134 Components on the front panel of a server with 12 x 3.5-inch disks

1	Disk	2	VGA port
3	USB 3.0 port	4	Label plate with an SN label

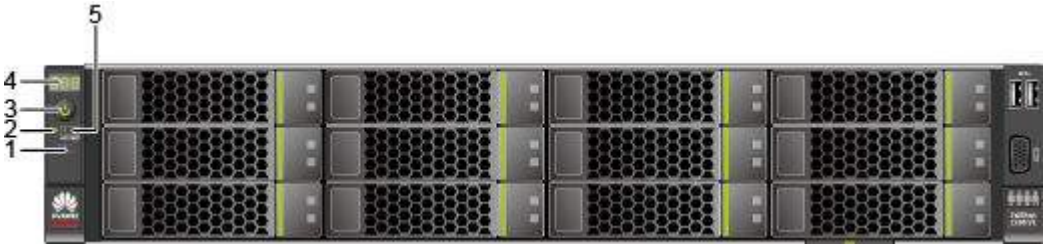
Table 3-62 Description of ports on the front panel

Port	Type	Description
USB port	USB 3.0	The USB ports allow USB devices to be connected to the server. **NOTE** Before connecting an external USB device, check that the USB device functions properly. A server may operate abnormally if an abnormal USB device is connected.
VGA port	DB15	The VGA port is connected to a terminal, such as a monitor or KVM.

Front Panel Indicators and Buttons

Figure 3-135 shows the indicators and buttons on the front panel of a server with 12 x 3.5-inch disks.

Figure 3-135 Indicators and buttons on the front panel of a server with 12 x 3.5-inch disks



1	UID button/indicator	2	Health indicator
3	Power button/indicator	4	Fault diagnosis LED
5	FlexIO presence indicators (1 and 2)	-	-

Table 3-63 Indicators and buttons on the front panel

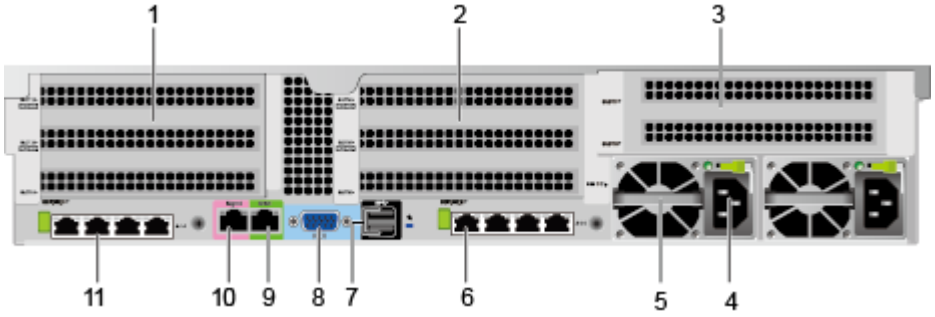
No.	Type	Description
1	UID button/indicator	The UID button/indicator helps identify and locate a device. UID indicator: • Off: The device is not being located. • Blinking blue: The device has been located and is differentiated from other devices that have also been located. • Steady blue: The device is being located. UID button: • You can turn on or off the UID indicator by pressing the UID button on the panel or by using the iBMC CLI or WebUI. • You can press this button to turn on or off the UID indicator. • You can press and hold down this button for 4 to 6 seconds to reset the iBMC.
2	Health indicator	• Steady green: The server is operating properly. • Blinking red at 1 Hz: A major alarm is generated. • Blinking red at 5 Hz: A critical alarm is generated.
3	Power button/ indicator	Power indicator: • Steady yellow: The server is in the standby state. • Steady green: The server is properly powered on. • Blinking yellow: The iBMC is starting. • Off: The server is not connected to a power source. Power button: • When the server is powered on, you can press this button to shut down the OS. • When the server is powered on, you can hold down this button for 6 seconds to forcibly power off the server. • When the server is ready to power on, you can press this button to start the server.
4	Fault diagnosis LED	• ---: The server is operating normally. • Error code: A server component is faulty.

No.	Type	Description
5	FlexIO presence indicators (1 and 2)	• 1 and 2: The numbers 1 and 2 respectively represent the FlexIOs 1 and 2. • Steady green: The FlexIO is properly connected. • Off: The FlexIO is faulty or not in use.

Rear Panel Components

Figure 3-136 shows the components on the rear panel of the 2280.

Figure 3-136 Rear panel components



1	I/O module 1	2	I/O module 2
3	I/O module 3	4	PSU socket
5	Power supply unit (PSU)	6	FlexIO 2
7	USB 3.0 port	8	VGA port
9	Serial port	10	Management network port
11	FlexIO 1	-	-

NOTE

- I/O modules 1, 2 and 3 can be disk modules or riser modules. The preceding figure is for reference only.
- FlexIO 1 or 2 can be a NIC with four GE electrical ports.
- FlexIO 1 or 2 is not hot-swappable. If you need to replace it, power off the server.

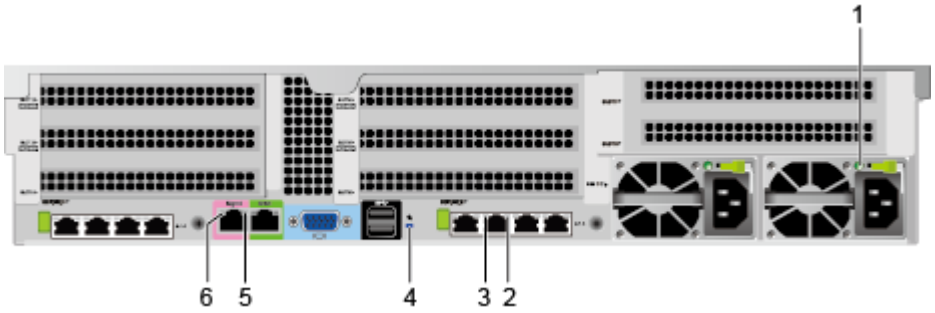
Table 3-64 Ports on the rear panel

Port	Type	Quantity	Description
VGA port	DB15	1	The VGA port is connected to a terminal, such as a monitor or KVM.
USB port	USB 3.0	2	The USB ports allow USB devices to be connected to the server. **NOTE** Before connecting an external USB device, check that the USB device functions properly. A server may operate abnormally if an abnormal USB device is connected.
Management network port	RJ45	1	This 1000 Mbit/s Ethernet port is used for server management.
Serial port	RJ45	1	The serial port is used as the system serial port by default. You can set it as the iBMC serial port by using the iBMC CLI. This port is used for debugging.
GE electrical port	RJ45	4/8	The mainboard CPU can provide GE electrical ports. A maximum of eight GE electrical ports can be provided through the two FlexIOs.
PSU socket	-	2	Determine the number of PSUs based on actual requirements, but ensure that the rated power of the PSUs is greater than that of the server. When one PSU is used, **Predicted PSU Status** cannot be set to **Active/Standby** on the iBMC WebUI.

Rear Panel Indicators

Figure 3-137 shows the indicators on the rear panel of the 2280.

Figure 3-137 Rear panel indicators



1	PSU indicator	2	GE electrical port link status indicator
3	GE electrical port data transmission status indicator	4	UID indicator
5	Management network port link status indicator	6	Management network port data transmission status indicator

Table 3-65 Indicators on the rear panel

No.	Indicator	Status
1	PSU indicator	• Steady green: The power input and output are normal. • Steady orange: The input is normal, but no power output is supplied due to overheat protection, overcurrent protection, short circuit protection, output overvoltage protection, or some component failures. • Blinking green at 1 Hz: – The input is normal, the server is standby. – The input is overvoltage or undervoltage. • Blinking green at 4 Hz: under online PSU firmware upgrade. • Off: No AC power is supplied.
2	GE electrical port link status indicator	• Steady green: The network is properly connected. • Off: The network is not connected.
3	GE electrical port data transmission status indicator	• Blinking yellow: Data is being transmitted. • Off: No data is being transmitted.
4	UID indicator	The UID indicator helps identify and locate a device. • Off: The device is not being located. • Blinking blue: The device has been located and is differentiated from other devices that have also been located. • Steady blue: The device is being located. **NOTE** You can turn on or off the UID indicator by pressing the UID button or remotely running a command on the iBMC CLI.

No.	Indicator	Status
5	Management network port link status indicator	• Steady green: The network is properly connected. • Off: The network is not connected.
6	Management network port data transmission status indicator	• Blinking yellow: Data is being transmitted. • Off: No data is being transmitted.

NOTE

For details about the components of the 2280 balanced model of the TaiShan 200 server, see the *TaiShan 200 Server User Guide (Model 2280)*.

3.14 Device Cables

Device cables used in the storage system include power cables, ground cables, and signal cables. This section shows their appearances and describes the functions and specifications of various cables.

3.14.1 Power Cables

Power cables are classified into DC power cables, AC power cables, and PDU power cables. Power cables supply power to devices in a cabinet. One end of a power cable is connected to the power socket of the storage system, and the other end to an external power supply.

DC Power Cable

Each DC power module is equipped with two DC power cables. **Figure 3-138** shows the appearance of DC power cables.

Figure 3-138 DC power cable

NOTE

Connect the black cable to the positive pole (+) of the power supply and the blue cable to the negative pole (-).

AC Power Cable

- Each AC power module is equipped with one AC power cable. **Figure 3-139** shows the appearance of an AC power cable.

  Figure 3-139 AC power cable

- If a cabinet is equipped with power distribution units (PDUs), use PDU power cables to supply power to devices in the cabinet. **Figure 3-140** shows the appearance of a PDU power cable.

  Figure 3-140 PDU power cable

3.14.2 Ground Cables

Ground cables are used for device grounding to improve the security when you perform operations on a storage device.

Appearance

Figure 3-141 shows the appearance of a ground cable.

Figure 3-141 Ground cable

3.14.3 Network Cables

The storage system uses network cables for its management network ports, service network ports, and other ports to connect to other devices or servers for communication.

Appearance

The storage system communicates with the external network using network cables. One end of the network cable connects to the management network port, service network port, or other network port of the storage system, and the other end connects to the network switch, application server, or other devices.

Figure 3-142 shows the appearance of a network cable.

NOTE

- GE electrical ports use CAT5 network cables or CAT6A shielded network cables.
- For details about the standard cable types and length requirements for 10GE electrical ports, see **Specifications Query**.

Figure 3-142 Network cable

3.14.4 Serial Cables

A serial cable connects the serial port on a storage system to a maintenance terminal.

Appearance

One end of a serial cable is an RJ-45 connector connecting to the serial port on a storage system. The other end is a DB-9 connector connecting to the port on a maintenance terminal.

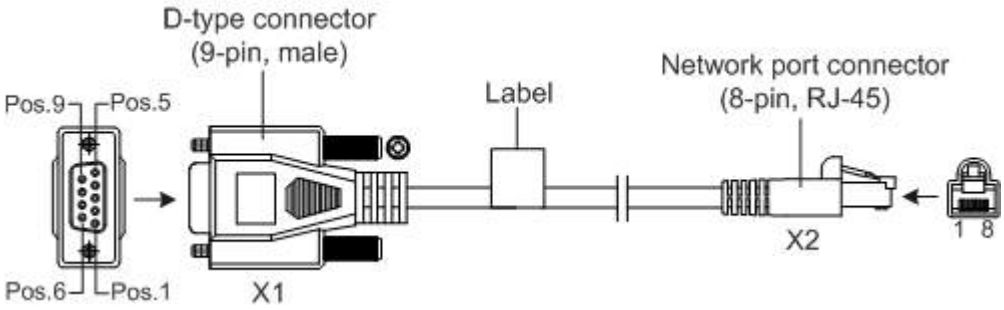
Figure 3-143 shows the appearance of a serial cable.

Figure 3-143 Serial cable

Structure

Figure 3-144 shows the structure of a serial cable.

Figure 3-144 Structure of a serial cable



Pin Assignments

Table 3-66 describes the pin assignments of a serial cable.

Table 3-66 Pin assignments of a serial cable

X1 (DB9)	X2 (RJ45)	Signal
8	1	CTS (Clear to Send)
6	2	DSR (Data Set Ready)
2	3	RXD (Receive Data)
5	4	GND
5	5	GND
3	6	TXD (Transmit Data)
4	7	DTR (Data Terminal Ready)
7	8	RTS (Request to Send)

3.14.5 Mini SAS HD Cables

Mini SAS HD cables are used to connect expansion ports. They can be either electrical or optical cables.

NOTE

- For the lengths of the mini SAS HD electrical and optical cables, refer to Specifications Query (**https://support-it.huawei.com/spec/#/home**).
- The mini SAS HD optical cables can be used to connect devices over distance, for example, for connections between cabinets.
- The optical connector of a mini SAS HD optical cable has a built-in O/E conversion module and provides electrical ports.

3.14.5.1 Mini SAS HD Electrical Cables

Mini SAS HD electrical cables are used to connect a controller enclosure to a SAS disk enclosure or connect two SAS disk enclosures.

NOTE

For the lengths of the mini SAS HD electrical cables, see **Specifications Query**.

Figure 3-145 shows the appearance of a mini SAS HD electrical cable.

Figure 3-145 Mini SAS HD electrical cable

3.14.5.2 Mini SAS HD Optical Cables

Mini SAS HD optical cables are used to connect a controller enclosure to a SAS disk enclosure or connect two SAS disk enclosures.

NOTE

- For the lengths of the mini SAS HD optical cables, see **Specifications Query**.
- For OceanStor 5310, mini SAS HD optical cables cannot be used to connect the onboard SAS ports on a controller enclosure to a disk enclosure.

Figure 3-146 shows the appearance of a mini SAS HD optical cable.

Figure 3-146 Mini SAS HD optical cable

NOTE

The only difference between a mini SAS HD optical cable and an optical fiber is the connector. You can bind mini SAS HD optical cables in the same way as binding optical fibers. For details, see section "Cable Routing and Bundling Basics" in the *General Cable Operation Guide*.

3.14.6 Optical Fibers

The storage system communicates with Fibre Channel switches through optical fibers. One end of the optical fiber connects to an interface module on the storage system, and the other end connects to the Fibre Channel switch or the application server. An optical fiber uses LC connectors at both ends.

Figure 3-147 shows the appearances of optical fibers.

NOTE

- When connecting cables, select proper cables according to site requirements and label information.
- For details on how to bind the cables, see section "Cable Routing and Bundling Basics" in the *General Cable Operation Guide*.

Figure 3-147 Optical fibers

3.14.7 100G QSFP28 Cables

The 100G QSFP28 cable is used to connect a smart disk enclosure.

NOTE

For the types and lengths of the cables, see "Type and length of back-end cables" in the **Specifications Query**.

Figure 3-148 shows the appearance of a 100G QSFP28 cable.

Figure 3-148 QSFP28 cable

3.14.8 25G SFP28 Cables

The 25G SFP28 cable is used for connections between two controller enclosures.

NOTE

For the types and lengths of the cables, see "Type and length of back-end cables" in the **Specifications Query**.

Figure 3-149 shows the appearance of a 25G SFP28 cable.

Figure 3-149 SFP28 cable

4 Software Architecture

Storage system software manages storage devices and stored data, and assists application servers in data operations.

The software suite provided by OceanStor storage systems consists of software running on the storage system, maintenance terminal, and application server. These three types of software work jointly to deliver storage, backup, and disaster recovery services in a smart, efficient, and cost-effective manner.

Figure 4-1 shows the storage system software architecture.

Figure 4-1 Storage system software architecture

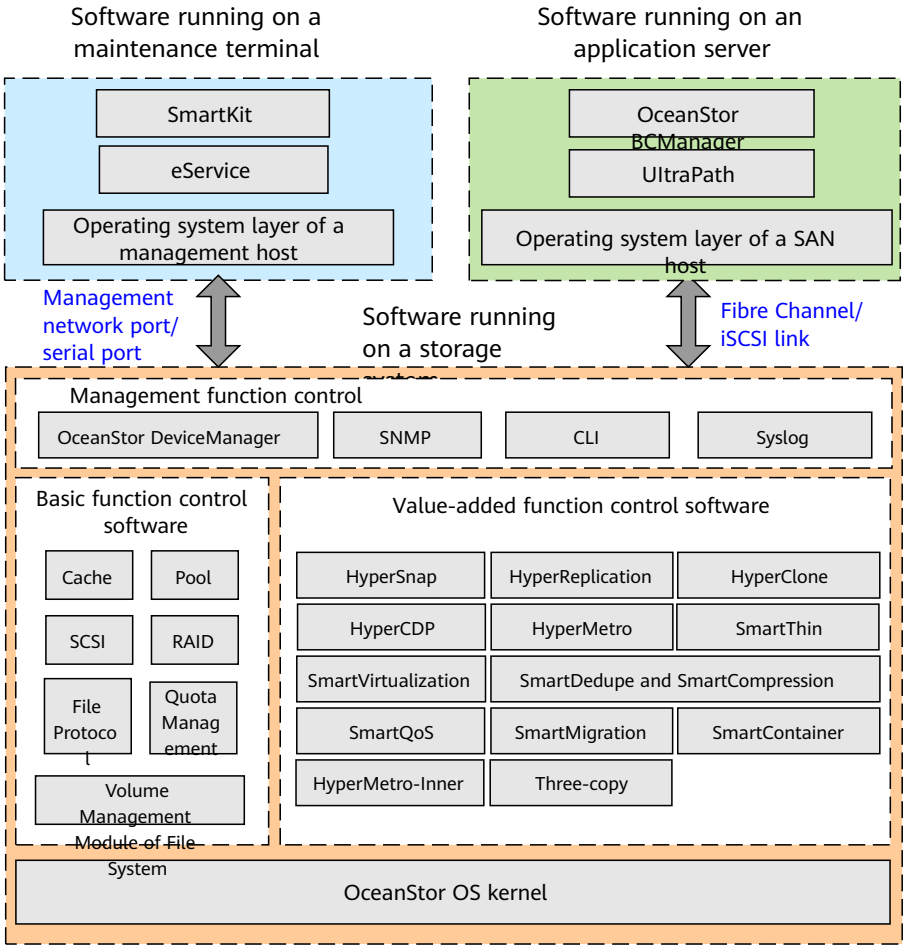


Table 4-1 describes the storage system software architecture.

Table 4-1 Storage system software architecture

Software	Function
Software running on a storage system	The storage system uses Huawei-developed storage operating system (OceanStor OS), which consists of the following: • The basic function software provides basic data storage and access functions. • The value-added software provides advanced functions such as backup, disaster recovery, and performance tuning. • The management software provides the management utilities to the storage system. • The OceanStor OS kernel manages hardware and runs storage service software.

Software	Function
Software running on a maintenance terminal	Configures and maintains the storage system. The software includes SmartKit and eService.
Software running on an application server	Enables the application server to communicate and cooperate with the storage system over a SAN. The software includes OceanStor BCManager and UltraPath.

Table 4-2 describes the software running on a storage system.

Table 4-2 Software running on a storage system

Software Set	Software	Function
OceanStor OS kernel	-	It is customized based on the EulerOS to manage hardware and run storage service software.
Management software	OceanStor DeviceManager	OceanStor DeviceManager is an integrated storage management platform developed by Huawei. It provides easy configuration, management, and maintenance of storage devices.
	SNMP[a, b]	The storage system can interwork with third-party management software using the SNMP protocol, and provide the functions of the third-party management software using the MIB interface. A variety of network management software supports SNMP. Users can choose desired software based on their requirements.
	CLI[c]	The storage system supports CLI-based management and configuration. Users can use a third-party terminal software to log in to the storage system through its serial port or management network port (over SSH), and manage the storage system on the CLI.
	Syslog	The storage system can send alarm information to a third party. Syslog software is used to receive and save the information. Users can choose desired Syslog software based on site requirements.

Software Set	Software	Function
Basic function software	SCSI software module	Manages the status of SCSI commands, and dispatches, resolves, and processes SCSI commands.
	RAID software module	Uses data stripping and redundancy to provide high performance, large capacity, and high reliability for data storage. A wide range of RAID levels are provided for diversified data reliability and access performance.
	Pool software module	Logically combines disks from different disk enclosures into storage pools to provide storage resources for services.
	Cache software module	Uses high-speed and small-capacity memory as a buffer to improve system performance. It is mainly used for data caching.
	File protocol module	Provides file system sharing and backup functions.
	Quota management module	Provides quota management for file system sharing. A shared file system allows you to specify the maximum storage capacity available to a specific directory.
	Volume management module of file system	Implements virtualized management based on volumes.
Value-added software	HyperSnap software module	Provides the snapshot function. Snapshot does not provide a complete physical duplicate but only an image of the source data, and locates the image through a mapping table.

Software Set	Software	Function
	HyperReplication software module	Provides the remote replication function. Remote replication creates an available data duplicate almost in real time on a storage system that resides in a different region from the local storage system. The duplicate can be used immediately without data recovery, protecting service continuity and data availability to the maximum. A consistency group manages remote replication tasks in batches. Any operation to the consistency group is also applied to the remote replication tasks in the group, ensuring data consistency throughout those remote replication tasks.
	HyperClone software module	Provides the clone function. A clone generates a full data copy of the source data in the local storage system.
	HyperMetro software module	Provides the HyperMetro function. HyperMetro enables real-time data synchronization and access between two storage systems, improving resource utilization. If data access fails, HyperMetro implements seamless service switchover, ensuring data security and service continuity.
	HyperCDP software module	HyperCDP achieves continuous data protection at an interval of several seconds, generating more intensive recovery points on storage devices.
	SmartQoS software module	Provides the SmartQoS function. SmartQoS controls the storage performance of LUNs, and prioritizes the quality of service (QoS) of critical applications.
	SmartThin software module	Provides the SmartThin function. SmartThin achieves the on-demand space allocation. It allocates free storage space in quota to application servers only as needed, increasing the storage space usage.
	SmartMigration software module	Provides the SmartMigration function. SmartMigration migrates services on a source LUN transparently to a target LUN without interrupting host services. After the migration, the target LUN can replace the source LUN to carry the services.

Software Set	Software	Function
	SmartVirtualiza-tion software module	Provides the SmartVirtualization function. SmartVirtualization enables a local storage system to centrally manage storage resources of third-party storage systems, simplifying storage system management and reducing maintenance costs.
	SmartDedupe and SmartCompression software module	Provides deduplication and compression. The deduplication function is used to analyze and delete duplicate data in a storage system. The compression function is used to minimize space occupied by data.
	SmartContainer software module	Provides the container function. Container services are established on storage nodes and applications are deployed on containers to integrate storage, computing, and networking.
a: Simple Network Management Protocol b: The supported character encoding is UTF-8. c: Command Line Interface		

Table 4-3 describes the software running on a maintenance terminal.

Table 4-3 Software running on a maintenance terminal

Software	Function
SmartKit	SmartKit helps service engineers and O&M engineers deploy, maintain, and upgrade devices.
eService	eService is remote maintenance and management software used for device monitoring, alarm reporting, and device inspection.

Table 4-4 describes the software running on an application server.

Table 4-4 Software running on an application server

Software	Function
OceanStor BCManager	Provides data protection and disaster recovery for application servers by using value-added features (asynchronous remote replication and snapshot) on the storage system. It centrally manages the requirements for data protection and disaster recovery between storage systems and application servers.
UltraPath	A storage system driver program installed on application servers. When multiple data channels are set up between an application server and a storage system, UltraPath selects an optimal channel for the application server to access the storage system. UltraPath provides an easy and efficient path management solution for proven data transmission reliability and high path security.

5 Product Specifications

Refer to the Specifications Query (**https://support-it.huawei.com/spec/#/home**) for the hardware and software specifications of the product.

6 Environmental Requirements

Environmental requirements cover the following aspects: temperature, humidity, particle contaminants, corrosive airborne contaminants, heat dissipation, and noise.

6.1 Environmental Parameters

Refer to the Specifications Query (**https://support-it.huawei.com/spec/#/home**) for the environmental conditions required by the storage system for proper running or safe storage.

Heat Dissipation

Heat dissipation of storage systems is implemented as follows:

- Controller enclosure

  Cooling air enters from the front fan holes and gaps of the controller enclosure. After dissipating the heat of interface modules, controllers, power modules, disks, and BBUs, the air is discharged out of rear fan holes and gaps. The controller enclosure dynamically adjusts rotational speed of the fans based on the operational temperature of the storage system.
- Disk enclosure
  - For a SAS disk enclosure: Cooling air enters from the front fan holes and gaps of disk enclosures. After dissipating the heat of power modules, disks, and expansion modules, the air is discharged out of power modules' fan holes in the rear side. The disk enclosure dynamically adjusts rotational speed of the fans based on the operational temperature of the storage system.
  - For a smart disk enclosure: Cooling air enters from the front fan holes and gaps of the disk enclosure. After dissipating the heat of power modules, disks, and expansion modules, the air is discharged out of rear fan holes and gaps. The disk enclosure dynamically adjusts rotational speed of the fans based on the operational temperature of the storage system.

For better maintenance, ventilation, and heat dissipation, pay attention to the following when installing the storage system in the cabinet:

- To ensure smooth ventilation, the cabinet should be at least 100 cm away from the equipment room walls and at least 120 cm away from other cabinets (that are in front of or behind).
- To keep air convection between the cabinet and the equipment room, no enclosed space is allowed in the cabinet. 1 U (44.45 mm) space should be left above and below each device.

Noise

Disks and fans, especially fans, emit noise when they are working. If the temperature rises, the fans rotate faster and emit more noise. Therefore, the noise of the storage system is related to the ambient temperature.

Disk Storage

SSDs cannot be preserved for a long term when they are powered off. When SSDs are powered off and the ambient temperature is lower than 40ºC, the maximum preservation time for SSDs that carry no data is 12 months, and that for SSDs carrying data is 3 months. Exceeding the maximum preservation time may cause data loss or SSD failure.

Cabinet Requirements

Devices that comply with the FCC/ICES standard must be used in shielded cabinets, such as Huawei FR42612L.

Equipment Room Management

- After the equipment room has been constructed, check whether the static air quality meets the requirements of ISO 14644-1 Class 8. Devices can be installed in the equipment room only after the requirements are met. During device running, check whether the dynamic air quality meets the requirements of ISO 14644-1 Class 8.
- Wear shoe covers and ESD clothes before entering the equipment room. After devices have been installed in the equipment room, do not decorate, polish, or drill holes in the equipment room to prevent dust. If necessary, take dust-proof measures.
- If more devices are added when the existing devices are running in the equipment room, the operations (such as unpacking, cable making, and hole drilling) must be performed in an isolated area to prevent dust and pollution.
- The humidifiers must use purified water without any salt.

Equipment Room Cleaning

Contaminants in an equipment room may be from various sources and in various forms. Mechanical processes in the equipment room may generate dangerous contaminants or stir the contaminants on the ground. Opening or closing hardware panels or any movement between metal components may generate metal scraps. Measures must be taken to clean contaminants (such as metal

particles, dust, solvent vapor, corrosive gases, soot, useless optical fibers, and salt) in the environment to prevent short circuits, corrosion, and electrical impacts on devices. Therefore, it is important to keep a highly clean data center environment.

Table 6-1 Equipment room cleaning requirements

Frequency	Task
Daily	Clear visible garbage, metal scraps, and dust in time.
Weekly	Clean and maintain the raised floor.
Quarterly	Clean the surfaces in the equipment room (such as equipment tops and racks), and clean the air filters of the air conditioners.
Every two years	Clean the air conditioning system, ventilation pipes, and floor gaps. If dust around the equipment room is heavy, increase the cleaning frequency.

CAUTION

- You are advised to have qualified professionals to clean the equipment room during device running.
- You are advised to use vacuum cleaners and dedicated dust-free clothes to clean the equipment room. If detergents are required, use professional detergents for the equipment room. Ensure that the detergents do not contain ammonia, chlorine, phosphate, decolorizer, sulfur, nitrogen oxide, hydrofluoric acid, volatile ingredients, or flammable ingredients. During routine cleaning, you are not advised to use water to clean large areas of the equipment room, avoiding impact on the equipment room humidity.

6.2 Contaminants

6.2.1 Particle Contaminants

Particle contaminants and other negative environmental factors (such as abnormal temperature and humidity) may expose IT equipment to a higher risk of corrosive failure. This section specifies the limitation on particle contaminants with the aim at avoiding such risks.

The concentration level of particle contaminants in a data center should meet the requirements listed in the white paper entitled *2011 Gaseous and Particulate Contamination Guidelines for Data Centers* by American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) Technical Committee (TC) 9.9.

ASHRAE, affiliated to International Organization for Standardization (ISO), is an international organization operated for the exclusive purpose of advancing the arts and sciences of heating, ventilation, air-conditioning, and refrigeration (HVAC & R). The *2011 Gaseous and Particulate Contamination Guidelines for Data Centers* is widely accepted, which is prepared by the members of ASHRAE TC 9.9, AMD, Cisco, Cray, Dell, EMC, Hitachi, HP, IBM, Intel, Seagate, SGI, and Sun.

According to the Guidelines, particle contaminants in a data center shall reach the cleanliness of ISO 14644-1 Class 8:

- Each cubic meter contains not more than 3,520,000 particles that are greater than or equal to 0.5 μm.
- Each cubic meter contains not more than 832,000 particles that are greater than or equal to 1 μm.
- Each cubic meter contains not more than 29,300 particles that are greater than or equal to 5 μm.

It is recommended that you use an effective filter to process air flowing into the data center as well as a filtering system to periodically clean the air already in the data center.

ISO 14644-1, Cleanrooms and Associated Controlled Environments - Part 1: Classification of Air Cleanliness, is the primary global standard on air cleanliness classification. **Table 6-2** gives the air cleanliness classification by particle concentration.

Table 6-2 Air cleanliness classification by particle concentration of ISO 14644-1

ISO Class	Maximum Allowable Concentrations (Particles/m^3) for Particles Equal To and Greater Than the Following Sizes					
-	≥ 0.1 μm	≥ 0.2 μm	≥ 0.3 μm	≥ 0.5 μm	≥ 1 μm	≥ 5 μm
Class 1	10	2	-	-	-	-
Class 2	100	24	10	4	-	-
Class 3	1000	237	102	35	8	-
Class 4	10,000	2,370	1,020	352	83	-
Class 5	100,000	23,700	10,200	3,520	832	29
Class 6	1,000,000	237,000	102,000	35,200	8,320	293
Class 7	-	-	-	352,000	83,200	2,930
Class 8	-	-	-	3,520,000	832,000	29,300
Class 9	-	-	-	-	8,320,000	293,000

6.2.2 Corrosive Airborne Contaminants

Corrosive airborne contaminants and other negative environmental factors (such as abnormal temperature and humidity) may expose IT equipment to higher risks of corrosive failure. This section specifies the limitation on corrosive airborne contaminants with an aim at avoiding such risks.

Table 6-3 lists common corrosive airborne contaminants and their sources.

Table 6-3 Common corrosive airborne contaminants and their sources

Category	Source
H_2S	Geothermal emissions, microbiological activities, fossil fuel processing, wood rot, sewage treatment
SO_2 and SO_3	Coal combustion, petroleum products, automobile emissions, ore smelting, sulfuric acid manufacture
S	Foundries, sulfur manufacture, volcanoes
HF	Fertilizer manufacture, aluminum manufacture, ceramics manufacture, steel manufacture, electronics device manufacture
NO_x	Automobile emissions, fossil fuel combustion, chemical industry
NH_3	Microbiological activities, sewage, fertilizer manufacture, geothermal emissions, refrigeration equipment
C	Incomplete combustion (aerosol constituent), foundry
CO	Combustion, automobile emissions, microbiological activities, tree rot
Cl_2 and ClO_2	Chlorine manufacture, aluminum manufacture, zinc manufacture, refuse decomposition
HCl	Automobile emissions, combustion, forest fire, oceanic processes, polymer combustion
HBr and HI	Automobile emissions
O_3	Atmospheric photochemical processes mainly involving nitrogen oxides and oxygenated hydrocarbons
C_NH_N	Automobile emissions, animal waste, sewage, tree rot
Organosilicon and organotin	Chemical plant, rubber plant, paint or ink containing organosilicon

The concentration level of corrosive airborne contaminants in a data center should meet the requirements listed in the white paper entitled *2011 Gaseous and Particulate Contamination Guidelines for Data Centers* by the American Society of

Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) Technical Committee (TC) 9.9.

According to the Guidelines, corrosive airborne contaminants in a data center should meet the following requirements:

- Copper corrosion rate

  Less than 300 Å/month as per ANSI/ISA-71.04-1985 severity level G1.
- Silver corrosion rate

  Less than 200 Å/month.

NOTE

Å, or angstrom, is a unit of length. One Å is equal to 1/10,000,000,000 meter.

According to ANSI/ISA-71.04-1985 Environmental Conditions for Process Measurement and Control Systems: Airborne Contaminants, the gaseous corrosivity levels are G1 (mild), G2 (moderate), G3 (harsh), and GX (severe), as described in **Table 6-4**.

Table 6-4 Gaseous corrosivity levels as per ANSI/ISA-71.04-1985

Severity Level	Copper Reactivity Level	Description
G1 (mild)	300 Å/month	An environment sufficiently well-controlled such that corrosion is not a factor in determining equipment reliability.
G2 (moderate)	300 Å/month to 1000 Å/month	An environment in which the effects of corrosion are measurable and may be a factor in determining equipment reliability.
G3 (harsh)	1000 Å/month to 2000 Å/month	An environment in which there is high probability that corrosion will occur.
GX (severe)	> 2000 Å/month	An environment in which only specially designed and packaged equipment would be expected to survive.

See **Table 6-5** for the copper and silver corrosion rate requirements.

Table 6-5 Concentration limitation of corrosive airborne contaminants in a data center

Group	Gas	Unit	Concentration
Group A	H_2S	ppb[a]	< 3
	SO_2	ppb	< 10
	Cl_2	ppb	< 1

Group	Gas	Unit	Concentration
	NO_2	ppb	< 50
Group B	HF	ppb	< 1
	NH_3	ppb	< 500
	O_3	ppb	< 2
a: Part per billion (ppb) is the number of units of mass of a contaminant per billion units of total mass.			

Group A and group B are common gas groups in a data center. The concentration limits of group A or group B that correspond to copper reactivity level G1 are calculated based on the premise that relative humidity in the data center is lower than 50% and that the gases in the group interact with each other. A 10% increase in the relative humidity will heighten the gaseous corrosivity level by 1.

Corrosion is not determined by a single factor, but by comprehensive environmental factors such as temperature, relative humidity, corrosive airborne contaminants, and ventilation. Any of the environmental factors may affect the gaseous corrosivity level. Therefore, the concentration limitation values specified in the previous table are for reference only.

6.2.3 Organisms

Plants and animals are not allowed in the equipment room.

To meet these requirements, take the following measures in the equipment room:

- Keep the atmosphere dry.
- Prevent molds on everything.
- Block cable holes and antenna holes.
- Clean and sterilize the equipment room periodically (do not use volatile or corrosive substances for sterilization).

6.2.4 Mechanically Active Substance

The equipment room should be free from explosive, conductive, magnetism-permeable, and corrosive dust. **Table 6-6** lists the requirements for concentration of the mechanically active materials in the equipment room.

Table 6-6 Requirements for concentration of mechanically active materials

Mechanically Active Material	Unit	Concentration
Sand	mg/m^3	≤ 30
Suspending dust	mg/m^3	≤ 0.2

Mechanically Active Material	Unit	Concentration
Dust deposit	mg/(m^2h)	≤ 1.5

To meet these requirements, take the following measures in the equipment room:

- Use dustproof materials on the ground, wall, and ceiling of the equipment room.
- Install screens for outdoor doors and windows, and use dustproof materials for outer windows.
- Clean the equipment room, especially the air filters once every three months.
- In areas with heavy dust, you are advised to clean the equipment once a year. (Invite professional companies to do so.)
- Wear shoe covers and ESD clothes before entering the equipment room.

7 Standards Compliance and Certifications

For details about the standards and certifications of the product, see the **Standards Compliance and Certifications for Enterprise Storage Products**.

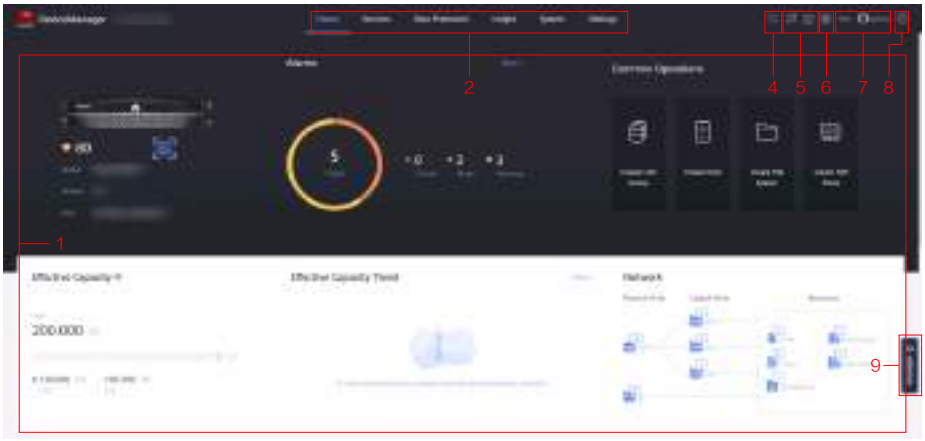
8 Operation and Maintenance

The storage systems can be operated and maintained by using DeviceManager and the command-line interface (CLI), adapting to different environments and user habits.

Introduction to DeviceManager

DeviceManager is a piece of software for managing Huawei storage devices. It helps you configure, manage, and maintain storage devices with ease. The following shows the DeviceManager main window.

Figure 8-1 DeviceManager main window



The following table describes the components of the DeviceManager main window.

Table 8-1 Components of the DeviceManager main window

No.	Name	Description
1	Function pane	The function pane shows a page associated with the current operation.

No.	Name	Description
2	Navigation bar	The navigation bar shows the functional modules of a storage system that are divided logically.
3	SmartGUI	SmartGUI mines users' historical operation data and builds a configuration parameter recommendation model based on user profiles to recommend configuration parameters for the block service and file service.
4	Global search	You can search for an object, page, or operation by entering the name of a LUN, LUN group, host, host group, port group, logical port, LUN snapshot, clone, and tenant.
5	Alarm and task statistics area	The alarm statistics area displays the number of alarms of each severity, helping you learn about the running status of the system. All tasks executed by users are displayed in the task statistics area, helping you know whether the tasks are successfully executed.
6	Device management area	The device management area allows you to view and modify device information as well as power off and restart devices.
7	Logout and language switchover area	The logout and language switchover area provides a logout button and a language switchover button. DeviceManager supports simplified Chinese and English.
8	Help and technical support	This area provides links to the online help and technical support websites.
9	eService	Scan the QR code to query device information and eService settings.

Introduction to the CLI

The CLI enables users to manage and maintain the storage systems using command lines.

Users need to log in to the CLI by using terminal software, such as the HyperTerminal provided by Windows, or PuTTY.

There are two ways to log in to the CLI.

- Log in through a serial port of a storage system. To connect to a serial port, the maintenance terminal must be located next to the storage system. Therefore, this login mode is applicable to users who do not know the management IP address of a storage system or a storage system is faulty.
- Log in through a management network port of a storage system. When there are reachable routes, a user can log in to the CLI by entering the IP address of

the management network port of a storage system in the terminal software. IP networks are easily accessible. Therefore, a user can log in to a storage system remotely, and this login mode is more popular.

A How to Obtain Help

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

A.1 Preparations for Contacting Huawei

To better resolve the fault, you are advised to collect troubleshooting information and make debugging preparations before contacting Huawei.

A.1.1 Collecting Troubleshooting Information

You need to collect troubleshooting information before troubleshooting.

You need to collect the following information:

- Name and address of the customer
- Contact person and telephone number
- Time when the fault occurred
- Description of the fault phenomena
- Device type and software version
- Measures taken after the fault occurs and the related results
- Troubleshooting level and required solution deadline

A.1.2 Making Debugging Preparations

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

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

A.2 How to Use the Document

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

To better solve the problems, use the documents before you contact Huawei for technical support.

A.3 How to Obtain Help from Website

Huawei provides users with timely and efficient technical support through the regional offices, secondary technical support system, telephone technical support, remote technical support, and onsite technical support.

Contents of the Huawei technical support system are as follows:

- Huawei headquarters technical support department
- Regional office technical support center
- Customer service center
- Technical support website: **https://support.huawei.com/enterprise/**

You can query how to contact the regional offices at **https://support.huawei.com/enterprise/**.

A.4 Ways to Contact Huawei

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

Huawei Technologies Co., Ltd.

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

Website: **https://e.huawei.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) on the network. Application programs of data services run on the application server.
Asynchronous remote replication	A kind of remote replication. When the data at the primary site is updated, the data does not need to be updated synchronously at the mirroring site to finish the update. In this way, performance is not reduced due to data mirroring.
Air baffle	It optimizes the ventilation channels and improves the heat dissipation capability of the system.
Audit log guarantee mode	A mode for recording audit logs. This mode preferentially ensures that the audit log function is normal and no audit log is missing.
Audit log non-guarantee mode	A mode for recording audit logs. In this mode, services are running properly. Audit logs may be missing.

B

Backup	A collection of data stored on (usually removable) non-volatile storage media for purposes of recovery in case the original copy of data is lost or becomes inaccessible; also called a backup copy. To be useful for recovery, a backup must be made by copying the source data image when it is in a consistent state. The act of creating a backup.

Backup window	An interval of time during which a set of data can be backed up without seriously affecting applications that use the data.
Bandwidth	The numerical difference between the upper and lower frequencies of a band of electromagnetic radiation. A deprecated synonym for data transfer capacity that is often incorrectly used to refer to throughput.
Baud rate	The maximum rate of signal state changes per second on a communications circuit. If each signal state change corresponds to a code bit, then the baud rate and the bit rate are the same. It is also possible for signal state changes to correspond to more than one code bit, so the baud rate may be lower than the code 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	The probability that a transmitted bit will be erroneously received. The bit error rate (BER) is measured by counting the number of bits in error at the output of a receiver and dividing by the total number of bits in the transmission. BER is typically expressed as a negative power of 10.
Bonding	Bonding of multiple independent physical network ports into a logical port, which ensures the high availability of server network connections and improves network performance.
Boundary scan	A test methodology that uses shift registers in the output connections of integrated circuits (ICs). One IC is often connected to the next IC. 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 known as Joint Test Action Group (JTAG).
Browser/Server	Architecture that defines the roles of the browser and server. The browser is the service request party and the server is the service provider.
Built-in FRU Alarm indicator	It indicates errors on the built-in FRUs of a controller, such as errors on fans or memory modules.

C

Cache hit ratio	The ratio of the number of cache hits to the number of all I/Os during a read task, usually expressed as a percentage.
Captive screw	Specially designed to lock into place on a parent board or motherboard, allowing for easy installation and removal of attached pieces without release of the screw.
Challenge Handshake Authentication Protocol	A password-based authentication protocol that uses a challenge to verify that a user has access rights to a system. A hash of the supplied password with the challenge is sent for comparison so the cleartext password is never sent over the connection.
Compliance mode	A protection mode of WORM. In compliance mode, files within their protection period cannot be changed or deleted by either the file user or by the system administrator. Files with expired protection periods can be deleted but not changed by the file user or the system administrator.
Controller	The control logic in a disk or tape that performs command decoding and execution, host data transfer, serialization and deserialization of data, error detection and correction, and overall management of device operations. The control logic in a storage subsystem that performs command transformation and routing, aggregation (RAID, mirroring, striping, or other), high-level error recovery, and performance optimization for multiple storage devices.
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.
Copying	A pair state. The state indicates that the source LUN data is being synchronized to the target LUN.
Container root directory	Space used to store the metadata for running container images and container instances.
Container image	An image is a special file system, which provides the programs, libraries, resources, and configuration files required for running containers. It also contains configuration parameters, for example, for anonymous disks, environment variables, and users. The image does not contain dynamic data, and its content will not be modified after construction.
Containerized application	An image can start multiple containers, and an application can contain one or a group of containers.

Container node	Controller that runs the container service.
Configuration item list	A series of modifiable configuration items defined in the Helm chart of the container.
Container service	Containerized application management service, which manages the lifecycle of containerized applications.

D

Data compression	The process of encoding data to reduce its size. Lossy compression (i.e., compression using a technique in which a portion of the original information is lost) is acceptable for some forms of data (e.g., digital images) in some applications, but for most IT applications, lossless compression (i.e., compression using a technique that preserves the entire content of the original data, and from which the original data can be reconstructed exactly) is required.
Data flow	A process that involves processing data extracted from the source system. These processes include: 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	A movement of data or information between information systems, formats, or media. Migration is performed for reasons such as possible decay of storage media, obsolete hardware or software (including obsolete data formats), changing performance requirements, the need for cost efficiencies etc.
Data source	A system, database (database user; database instance), or file that can make BOs persistent.
Dirty data	Data that is stored temporarily on the cache and has not been written onto disks.
Disaster recovery	The recovery of data, access to data and associated processing through a comprehensive process of setting up a redundant site (equipment and work space) with recovery of operational data to continue business operations after a loss of use of all or part of a data center. This involves not only an essential set of data but also an essential set of all the hardware and software to continue processing of that data and business. Any disaster recovery may involve some amount of down time.

Disk array	A set of disks from one or more commonly accessible disk subsystems, combined with a body of control software. The control software presents the disks' storage capacity to hosts as one or more virtual disks. Control software is often called firmware or microcode when it runs in a disk controller. Control software that runs in a host computer is usually called a volume manager.
Disk domain	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 enclosure	Consists of the following parts in redundancy: expansion module, disk, power module, and fan module. System capacity can be expanded by cascading multiple disk enclosures.
Disk location	The process of locating a disk in the storage system by determining the enclosure ID and slot ID of the disk.
Disk utilization	The percentage of used capacity in the total available capacity.

E

eDevLUN	Logical storage array space created by a third-party storage array.
Expansion module	A component used for expansion.
Expansion	Connects a storage system to more disk enclosures through connection cables, expanding the capacity of the storage system.

F

Field replaceable unit	A unit or component of a system that is designed to be replaced in the field, i.e., without returning the system to a factory or repair depot. Field replaceable units may either be customer-replaceable or their replacement may require trained service personnel.
Firmware	Low-level software for booting and operating an intelligent device. Firmware generally resides in read-only memory (ROM) on the device.

Flash Translation Layer	Flash Translation Layer (FTL) organizes and manages host data, enables host data to be allocated to NAND flash chips of SSDs in an orderly manner, maintains the mapping relationship between logical block addresses (LBAs) and physical block addresses (PBAs), and implements garbage collection, wear leveling, and bad block management.
Front-end port	The port that connects the controller enclosure to the service side and transfers service data. Front-end port types are Fibre Channel and iSCSI.
Front-end interconnect I/O module (FIM)	On a storage device, all controllers share the front-end interface modules.

G

Garbage collection	The process of reclaiming resources that are no longer in use. Garbage collection has uses in many aspects of computing and storage. For example, in flash storage, background garbage collection can improve write performance by reducing the need to perform whole block erasures prior to a write.
Gateway	A device that receives data via one protocol and transmits it via another.
Global garbage collection	With a view to defragmentation of storage arrays and garbage collection of disks, global garbage collection reduces garbage of disks by enabling storage arrays to inform disks of not implementing invalid data relocation and of controlling space release so that disks and controllers consume less space, reducing costs and prolonging the useful life of storage arrays.
Global system for mobile communications	The second-generation mobile networking standard defined by the European Telecommunications Standards Institute (ETSI). It is aimed at designing a standard for global mobile phone networks. GSM consists of three main parts: mobile switching subsystem (MSS), base station subsystem (BSS), and mobile station (MS).
Global wear leveling	With a view to individual characteristics of a single disk, global wear leveling uses space allocation and write algorithms to achieve wear leveling among disks, preventing a disk from losing efficacy due to excessive writes and prolonging the useful life of the disk.

H

Hard disk tray	The tray that bears the hard disk.
Heartbeat	Heartbeat supports node communication, fault diagnosis, and event triggering. Heartbeats are protocols that require no acknowledgement. They are transmitted between two devices. The device can judge the validity status of the peer device.
Hit ratio	The ratio of directly accessed I/Os from the cache to all I/Os.
Hot swap	The substitution of a replacement unit (RU) in a system for a defective unit, where the substitution can be performed while the system is performing its normal functioning normally. Hot swaps are physical operations typically performed by humans.
HyperMetro	A value-added service of storage systems. HyperMetro means 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 generally; made up of two storage arrays and one quorum server. HyperMetro services can be created on a HyperMetro domain.
HyperMetro vStore pair	A HyperMetro vStore pair consists of two vStores, that is, two tenants. After a HyperMetro relationship is set up for a pair of vStores, the datasets in the two vStores work in redundancy mode and provide storage services in one dataset view, achieving hitless service failover.
HyperMetro-Inner	On an eight-controller network, with HyperMetro-Inner, continuous mirroring, back-end global sharing, and three-copy technologies, a storage system can tolerate one-by-one failures of seven controllers among eight controllers, concurrent failures of two controllers, and failure of a controller enclosure.
HyperDetect	HyperDetect is a feature that provides ransomware detection.
Handle	A handle resides on the structural part of a module. It is used to insert or remove a module into or from a chassis, not helpful in saving efforts.
Helm chart	A Helm chart is in TAR format. It is similar to the deb package of APT or the rpm package of Yum. It contains a group of yaml files that define Kubernetes resources.

I

In-band management	The management control information of the network and the carrier service information of the user network are transferred through the same logical channel. In-band management enables users to manage storage arrays through commands. Management commands are sent through service channels, such as I/O write and read channels. The advantages of in-band management include high speed, stable transfer, and no additional management network ports required.
Initiator	The system component that originates an I/O command over an I/O interconnect. The endpoint that originates a SCSI I/O command sequence. I/O adapters, network interface cards, and intelligent I/O interconnect control ASICs are typical initiators.
I/O	Shorthand for input/output. I/O is the process of moving data between a computer system's main memory and an external device or interface such as a storage device, display, printer, or network connected to other computer systems. This encompasses reading, or moving data into a computer system's memory, and writing, or moving data from a computer system's memory to another location.
Intelligent ransomware detection	The system detects known ransomware features to identify whether the file systems are attacked by ransomware. If no ransomware attack is identified, the system analyzes and compares the changes in file system snapshots, and uses machine learning algorithms to further check whether the file systems are infected by ransomware.
Interface module	A replaceable field 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/Os or computing requests to physical resources of the system.
Logical unit	The addressable entity within a SCSI target that executes I/O commands.
Logical unit number	The SCSI identifier of a logical unit within a target. Industry shorthand, when phrased as "LUN", for the logical unit indicated by the logical unit number.

LUN formatting	The process of writing 0 bits in the data area of the logical drive and generating related parity bits so that the logical drive can be in the ready state.
LUN mapping	A storage system maps LUNs to application servers so that application servers can access storage resources.
LUN migration	A method for the LUN data to migrate between different physical storage spaces while ensuring data integrity and uninterrupted operation of host services.
LUN snapshot	A type of snapshot created for a LUN. This snapshot is both readable and writable and is mainly used to provide a snapshot LUN from point-in-time LUN data.
Lever	A lever resides on the structural part of a module. It is used to insert or remove a module into or from a chassis, saving efforts.
Local image repository	A private repository used to store the container images and Helm charts imported by users. It is different from the standard image repository. The imported images and Helm charts must meet the compatibility requirements of the system.

M

Maintenance terminal	A computer connected through a serial port or management network port. It maintains the storage system.
Management interface module	The module that integrates one or more management network ports.
Management network	An entity that provides means to transmit and process network management information.
Management network port	The network port on the controller enclosure connected to the maintenance terminal. It is provided for the remote maintenance terminal. Its IP address can be modified with the change of the customer's environment.

N

NVM Express	A host controller interface with a register interface and command set designed for PCI Express-based SSDs.

NVMe SSD	A solid state disk (SSD) with a non-volatile memory express (NVMe) interface. Compared with other SSDs, such SSDs can deliver higher performance and shorter latency.

O

Out-of-band management	A management mode used during out-of-band networking. The management and control information of the network and the bearer service information of the user network are transmitted through different logical channels.

P

Power failure protection	When an external power failure occurs, the AC PEM depends on the battery for power supply. This ensures the integrity of the dirty data in the cache.
Pre-copy	When the system monitors a failing member disk in a RAID group, the system copies the data from the disk to a hot spare disk in advance.
Palm-sized NVMe SSD	A palm-sized NVMe SSD is a type of NVMe SSD of which the dimensions (H x W x D) are 160 mm x 79.8 mm x 9.5 mm (neither 3.5-inch nor 2.5-inch).

Q

Quorum server	A server that can provide arbitration services for clusters or HyperMetro to prevent the resource access conflicts of 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 redundancy 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.

Ransomware file interception	When launching attacks, ransomware usually generates encrypted files with special file name extensions. In light of this, the system intercepts the write to files with specific file name extensions to block the extortion from known ransomware and protect file systems in the storage system.
Real-time ransomware detection	Ransomware has similar I/O behavior characteristics. By analyzing file I/O behavior characteristics, the system quickly filters out abnormal files and performs deep content analysis on the abnormal files to detect files attacked by ransomware. Then, secure snapshots are created for file systems where files have been attacked, and alarms are reported to notify the data protection administrator, limiting the impact of ransomware and reducing losses.
Reconstruction	The regeneration and writing onto one or more replacement disks of all of the user data and check data from a failed disk in a mirrored or RAID array. In most arrays, a rebuild can occur while applications are accessing data on the array's virtual disks.
Redundancy	The inclusion of extra components of a given type in a system (beyond those required by the system to carry out its function) for the purpose of enabling continued operation in the event of a component failure.
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 mirrors 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.
Reverse synchronization	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. On a TCP/IP network, each IP packet is routed independently. Routes can change dynamically.

S

Script	A parameterized list of primitive I/O interconnect operations intended to be executed in sequence. Often used with respect to ports, most of which are able to execute scripts of I/O commands autonomously (without policy processor assistance). A sequence of instructions intended to be parsed and carried out by a command line interpreter or other scripting language. Perl, VBScript, JavaScript and Tcl are all scripting languages.
Serial port	An input/output location (channel) that sends and receives data (one bit at a time) to and from the CPU of a computer or a communications device. Serial ports are used for serial data communication and as interfaces for some peripheral devices, such as mouse devices 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.
Simple network management protocol	An IETF protocol for monitoring and managing systems and devices in a network. The data being monitored and managed is defined by an MIB. The functions supported by the protocol are the request and retrieval of data, the setting or writing of data, and traps that signal the occurrence of events.
Single point of failure	One component or path in a system, the failure of which would make the system inoperable.
Slot	A position defined by an upper guide rail and the corresponding lower guide rail in a frame. A slot houses a board.
Small computer system interface	A collection of ANSI standards and proposed standards that define I/O interconnects primarily intended for connecting storage subsystems or devices to hosts through host bus adapters. Originally intended primarily for use with small (desktop and desk-side workstation) computers, SCSI has been extended to serve most computing needs, and is arguably the most widely implemented I/O interconnect in use today.
Snapshot	A point in time copy of a defined collection of data. Clones and snapshots are full copies. Depending on the system, snapshots may be of files, LUNs, file systems, or any other type of container supported by the system.
Snapshot copy	A copy of a snapshot LUN.

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 system	An integrated system that 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 to the actual storage media used to back up data.
Streaming media	Streaming media is media continuously streamed over the network. Combining technologies concerning streaming media data collection, compression, encoding, storage, transmission, playback, and network communications, streaming media can provide high-quality playback effects in real time at low bandwidth.
Subnet	A type of smaller network that forms a larger network according to a rule, such as, forming a network according to different districts. This facilitates the management of a large network.
Smart disk enclosure	Being compared with traditional disk enclosures, the smart disk enclosures are equipped with Arm chips and DDR memories or other computing modules to achieve powerful computing capabilities. With such capabilities, the smart disk enclosures can help controllers to share some computing loads, accelerating data processing.
Share authentication	During vStore configuration synchronization, the share authentication information (including the share information and domain controller configuration) is synchronized to the secondary end.

T

Target	The endpoint that receives a SCSI I/O command sequence.
Target LUN	The LUN on which target data resides.
Thin LUN	A logic disk that can be accessed by hosts. It dynamically allocates storage resources from the thin pool according to the actual capacity requirements of users.

Topology	The logical layout of the components of a computer system or network and their interconnections. Topology deals with questions of what components are directly connected to other components from the standpoint of being able to communicate. It does not deal with questions of physical location of components or interconnecting cables. The communication infrastructure that provides Fibre Channel communication among a set of PN_Ports (e.g., a Fabric, an Arbitrated Loop, or a combination of the two).
Trim	A method by which the host operating system may inform a storage device of data blocks that are no longer in use and can be reclaimed. Many storage protocols support this functionality via various names, e.g., ATA TRIM and SCSI UNMAP.

U

User interface	The space where users interact with a machine.
U-shaped bracket	It is an optional structural part like letter "U". It is located between the mounting ear of a chassis and the mounting bar of a cabinet or bay and is used to adjust the locations of the chassis and mounting bar of the cabinet or bay.

W

Wear leveling	A set of algorithms utilized by a flash controller to distribute writes and erases across the cells in a flash device. Cells in flash devices have a limited ability to survive write cycles. The purpose of wear leveling is to delay cell wear out and prolong the useful life of the overall flash device.
Write amplification	Increase in the number of write operations by the device beyond the number of write operations requested by hosts.
Write amplification factor	The ratio of the number of write operations on the device to the number of write operations requested by the host.

Write back	A caching technology in which the completion of a write request is signaled as soon as the data is in the cache. Actual writing to non-volatile media occurs at a later time. Write back includes inherent risks: an application will take 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 these reasons, sufficient write back implementations include mechanisms to preserve cache contents across system failures (including power failures) and a flushed cache at system restart time.
Write Once Read Many	A type of storage, designed for fixed content, that preserves what is written to it in an immutable fashion. Optical disks are an example of WORM storage.
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 equipped with the write through technology is approximately that of a non-cached system. However, if the written data is also held in a cache, subsequent read performance may be dramatically improved.

Z

Zone	A collection of Fibre Channel N_Ports and/or NL_Ports (i.e., device ports) that are permitted to communicate with each other via the fabric. Any two N_Ports and/or NL_Ports that are not members of at least one common zone are not permitted to communicate via the fabric. Zone membership may be specified by: 1) port location on a switch, (i.e., Domain_ID and port number); or, 2) the device's N_Port_Name; or, 3) the device's address identifier; or, 4) the device's Node_Name. Well-known addresses are implicitly included in every zone.

C Acronyms and Abbreviations

B	
BBU	Backup Battery Unit
C	
CLI	Command Line Interface
F	
FC	Fibre Channel
H	
HBA	Host Bus Adapter
HPC	High-performance Computing
I	
IOPS	Input/Output Operations Per Second
iSCSI	Internet Small Computer Systems Interface
L	
LUN	Logical Unit Number
N	
NVMe	Non-volatile Memory Express
O	
ODT	Offloaded Data Transfer
OLTP	Online Transaction Processing

OLAP	Online Analytical Processing
R	
RAID	Redundant Array of Independent Disks
ROW	Redirect-On-Write
S	
SAS	Serial Attached SCSI
SNMP	Simple Network Management Protocol
SRM	Site Recovery Manager
SSD	Solid-State Drive
T	
TCO	Total Cost of Ownership
V	
VAAI	vSphere Storage APIs for Array Integration
VDI	Virtual Desktop Infrastructure
VSS	Volume Shadow Copy Service

OceanStor
6.1.x
Administrator Guide

Issue 03
Date 2022-08-25

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: https://e.huawei.com

About This Document

Purpose

This document describes how to perform daily management, monitoring, and troubleshooting on the storage systems.

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

Product Model	Product Version
OceanStor 5310	6.1.3 6.1.5
OceanStor 5510	
OceanStor 5610	
OceanStor 6810	
OceanStor 18510	
OceanStor 18810	

NOTICE

This document is updated periodically with the software version. The operations described in this document use the latest version as an example. Note that the supported functions and features vary according to the software version. The content in this document is for reference only.

Intended Audience

This document is intended for:

- Technical support engineers
- Maintenance engineers

Symbol Conventions

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

Symbol	Description
DANGER	Indicates a hazard with a high level of risk which, if not avoided, will result in death or serious injury.
WARNING	Indicates a hazard with a medium level of risk which, if not avoided, could result in death or serious injury.
CAUTION	Indicates a hazard with a low level of risk which, if not avoided, could result in minor or moderate injury.
NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
NOTE	Supplements the important information in the main text. 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 03 (2022-08-25)

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

Optimized some descriptions.

Issue 02 (2022-04-15)

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

Optimized some descriptions.

Issue 01 (2022-01-25)

This issue is the first official release.

Contents

1 Administrator Roles and Permissions

To prevent misoperations from compromising the storage system stability and service data security, the storage system defines user roles to control user permissions. Before using this document, check the operation permissions of your current account.

1.1 Administrator Roles and Permissions (Applicable to 6.1.3)

Definition of User Roles

Role: defines the scope of objects that can be operated or accessed by a user.

The storage system provides both built-in and user-defined roles.

- Built-in roles are preset in the storage system with certain permission. For details about the permissions owned by the built-in roles, see **Table 1-1**.

  You can run the **show role system id=***?* or **show role vstore id=***?* command on the CLI to query the detailed permissions of a specific system or vStore role. For details about the command, see the command reference specific to your product version.
- User-defined roles allow users to configure the scope of permission as required. For details about the permissions of user-defined roles, see **A.1 Permission Matrix for User-defined Roles (Applicable to 6.1.3)**.

Table 1-1 Built-in roles

Built-in Role	Permission	Owning Group
Super administrator	All permissions	System group
Administrator	All permissions except user management, batch configuration and high-risk maintenance operations	System group
Security administrator	System security configuration permissions, including management of security rules, certificates, KMC, and data destruction	System group
SAN resource administrator	SAN resource management permissions, including management of storage pools, LUNs, mapping views, hosts, ports, and background configuration tasks	System group
Data protection administrator	Data protection management permissions, including management of LUNs, local data protection, remote data protection, HyperMetro, and background configuration tasks	System group
Remote device administrator	Cross-device data protection management permissions, including management of remote replication, HyperMetro, 3DC, LUNs, and mapping views. This role is used for remote authentication in cross-device data protection scenarios.	System group
Monitor	Routine O&M permissions, such as information collection, performance collection, and inspection. This role does not have the permission to manage SAN resources, data protection, and security configuration.	System group
NDMP backup administrator	NDMP backup management permissions, including management of local data protection, remote data protection, HyperMetro, and resource tuning	System group
Non-privileged administrator	Basic system permissions, including querying information about the system, users, and roles. This role can be used to query information only on the CLI management page. It is displayed as **Empty role** on the CLI management page.	System group

Built-in Role	Permission	Owning Group
vStore administrator	All permissions for managing vStores	vStore group
vStore protocol administrator	vStore protocol management permissions, including authenticated user and share management for vStores	vStore group
vStore data protection administrator	vStore data protection management permissions, including management of LUNs, local data protection, remote data protection, HyperMetro, and background configuration tasks of vStores	vStore group
vStore WORM administrator	vStore WORM management permissions, including management of global security regulation clock, WORM file systems, vStore litigation hold, and file fingerprints	vStore group
vStore NDMP backup administrator	NDMP backup management permissions of a vStore, including management of local data protection, remote data protection, HyperMetro, and resource tuning	vStore group

Querying the Current User's Permission

You can perform the following operations to query the operation permission and scope of your current account.

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **User and Security** > **Users and Roles** > **Roles**.

Step 3 Query the current user's role information in the middle pane and determine the operation permission and scope according to **Table 1-1** and **A.1 Permission Matrix for User-defined Roles (Applicable to 6.1.3)**.

----End

NOTE

Super administrators can view the information about all users on the device.

1.2 Administrator Roles and Permissions (Applicable to 6.1.5)

Definition of User Roles

Role: defines the scope of objects that can be operated or accessed by a user.

The storage system provides both built-in and user-defined roles.

- Built-in roles are preset in the storage system with certain permission. For details about the permissions owned by the built-in roles, see **Table 1-2**.

  You can run the **show role system id=***?* or **show role vstore id=***?* command on the CLI to query the detailed permissions of a specific system or vStore role. For details about the command, see the command reference specific to your product version.
- User-defined roles allow users to configure the scope of permission as required. For details about the permissions of user-defined roles, see **A.2 Permission Matrix for User-defined Roles (Applicable to 6.1.5)**.

Table 1-2 Built-in roles

Built-in Role	Permission	Owning Group
Super administrator	All permissions	System group
Administrator	All permissions except user management, role management, global security regulation clock management, litigation hold file management, S3 key management, storage system power-off and restart, and running of major management O&M commands in the developer view, engineer view, and diagnostic view	System group
Security administrator	System security configuration permissions, including management of security policies, security rules, HyperCDP objects, disks, certificates, disk data destruction policies, key services, antivirus functions, and file service snapshots	System group

Built-in Role	Permission	Owning Group
SAN resource administrator	Management permissions on SAN resources, including management of disk domains, storage pools, disks, controller enclosures or disk enclosures, recycle bin policies, internal objects, LUNs and clone LUNs, application type objects, initiators, targets, iSNS servers, mapping views, host groups, hosts, port groups, LUN groups, ports, controllers, interface modules, DNS load balancing services, BGP configurations, BGP peers, block service snapshots, HyperCDP objects, HyperClone, omtask, and storage connectivity	System group
NAS resource administrator	Management permissions on NAS resources, including management of disk domains, storage pools, ports, DNS load balancing services, BGP configurations, BGP peers, NFS services, share services, file systems and clone file systems, domain authentication information, dtree services, quota services, CIFS services, Kerberos realm configurations, file signatures, application type objects, audit logs, file service snapshots, omtask, storage connectivity, and HyperCDP objects	System group
Data protection administrator	Data protection management permissions, including management of recycle bin policies, internal objects, LUNs, application type objects, initiators, mapping views, host groups, hosts, ports, remote devices, block service snapshots, HyperCDP objects, snapshot consistency groups (CGs), HyperClone, clone CGs, LUN CGs, LUN groups, remote replication, CGs, DR Star, HyperMetro CGs, HyperMetro domains, HyperMetro pairs, quorum servers, omtask, storage connectivity, protection groups, file systems, dtree services, file service snapshots, quota services, NDMP services, and vStore services	System group
Remote device administrator	Cross-device data protection management permissions, including management of recycle bin policies, internal objects, LUNs, initiators, mapping views, host groups, hosts, port groups, LUN groups, ports, HyperCDP objects, HyperClone, clone CGs, block service snapshots, snapshot CGs, CGs, remote devices, remote replication, HyperMetro CGs, HyperMetro domains, HyperMetro pairs, quorum servers, SmartQoS, LUN migration, system information, mirroring policies, omtask, storage connectivity, protection groups, file systems, dtree services, file service snapshots, quota services, and NDMP services. This role is used for remote authentication in cross-device data protection scenarios.	System group

Built-in Role	Permission	Owning Group
Monitor	Routine O&M permissions, such as information collection, performance collection, and inspection, including alarm policy management, log information export (such as system logs, configuration information, and diagnosis files), system log management, configuration file management, running data (configuration information) management, Call Home (eService) service management, and management of the CLI views that can be switched over	System group
NDMP backup administrator	NDMP backup service management permissions, including management of initiators, mapping views, host groups, hosts, port groups, LUN groups, ports, HyperCDP objects, HyperClone, clone CGs, block service snapshots, snapshot CGs, CGs, remote devices, remote replication, HyperMetro CGs, HyperMetro domains, HyperMetro pairs, quorum servers, SmartQoS, LUN migration, system information, mirroring policies, omtask, storage connectivity, protection groups, file systems, dtree services, file service snapshots, quota services, and NDMP services	System group
Non-privileged administrator	Basic system permissions, including querying information about the role and users of this role, changing the password of users of this role, querying and modifying CLI configurations, and querying license information, security policies and system information. A user of this role can log in to the system only using the CLI.	System group
vStore administrator	Management of vStore LUNs, LUN groups, initiators, mapping views, hosts, host groups, port groups, HyperCDP objects, HyperClone, clone CGs, LUN CGs, block service snapshots, snapshot CGs, CGs, DR Star, remote replication, HyperMetro CGs, HyperMetro pairs, SmartQoS, LUN migration, omtask, storage connectivity, certificates, antivirus services, protection groups, NFS services, service plane domain servers, file systems, share and share permissions, file signatures, CIFS services, dtree services, file service snapshots, quota services, NDMP services, audit logs, Kerberos realm and services, and encryption types	vStore group
vStore protocol administrator	vStore protocol management permissions, including management of vStore omtask, service plane domain servers, share and share permissions, Kerberos realm and services, and encryption types	vStore group

Built-in Role	Permission	Owning Group
vStore data protection administrator	vStore data protection management permissions, including management of vStore LUNs, initiators, mapping views, hosts, host groups, HyperCDP objects, HyperClone, clone CGs, LUN CGs, block service snapshots, snapshot CGs, LUN groups, remote replications, CGs, DR Star, HyperMetro CGs, HyperMetro pairs, omtask, storage connectivity, protection groups, file systems, file service snapshots, and NDMP services	vStore group
vStore WORM administrator	vStore WORM management permissions, including management of vStore omtask, file system WORM, file systems, share and share permissions, file signatures, and litigation hold files	vStore group
vStore NDMP backup administrator	vStore NDMP backup service management permissions, including management of vStore recycle bin policies, internal objects, LUNs, initiators, mapping views, host groups, hosts, port groups, LUN groups, ports, HyperCDP objects, HyperClone, clone CGs, block service snapshots, snapshot CGs, CGs, remote devices, remote replication, HyperMetro CGs, HyperMetro domains, HyperMetro pairs, quorum servers, SmartQoS, LUN migration, system information, mirroring policies, omtask, storage connectivity, protection groups, file systems, dtree services, file service snapshots, quota services, and NDMP services	vStore group

Querying the Current User's Permission

You can perform the following operations to query the operation permission and scope of your current account.

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **User and Security** > **Users and Roles** > **Roles**.

Step 3 Query the current user's role information in the middle pane and determine the operation permission and scope according to **Table 1-2** and **A.2 Permission Matrix for User-defined Roles (Applicable to 6.1.5)**.

----End

NOTE

Super administrators can view the information about all users on the device.

2 Common Management Software and Access Method

This chapter describes common management software and the access methods to help administrators with their operations.

2.1 Overview of Common Management Software

You can use DeviceManager and command-line interface (CLI) to query, configure, manage, and maintain storage systems. You can use serviceability tools, such as SmartKit and eService, to improve the maintenance efficiency.

The O&M management software helps administrators manage and monitor the storage system. **Table 2-1** describes software commonly used to manage storage systems.

Table 2-1 Common management software

Management Software	Function
DeviceManager	Helps you to allocate storage resources, manage users, data protection features, and alarms, and monitor device performance.
CLI	Helps you to allocate storage resources, manage users, data protection features, and alarms, and monitor device performance.
SmartKit	Helps you with routine maintenance, upgrade, patch installation, troubleshooting, expansion, and parts replacement.

Management Software	Function
eService	Supports alarm reporting, file uploading, and remote access.

Introduction to DeviceManager

DeviceManager is a piece of software for managing Huawei storage devices. It helps you configure, manage, and maintain storage devices with ease. **Figure 2-1** and **Figure 2-2** show the DeviceManager main window.

NOTE

GUIs may vary with product versions and models. The information displayed on the interface is only for reference and is subject to the actual situation.

Figure 2-1 DeviceManager main window (OceanStor 5310, OceanStor 5510, OceanStor 5610)

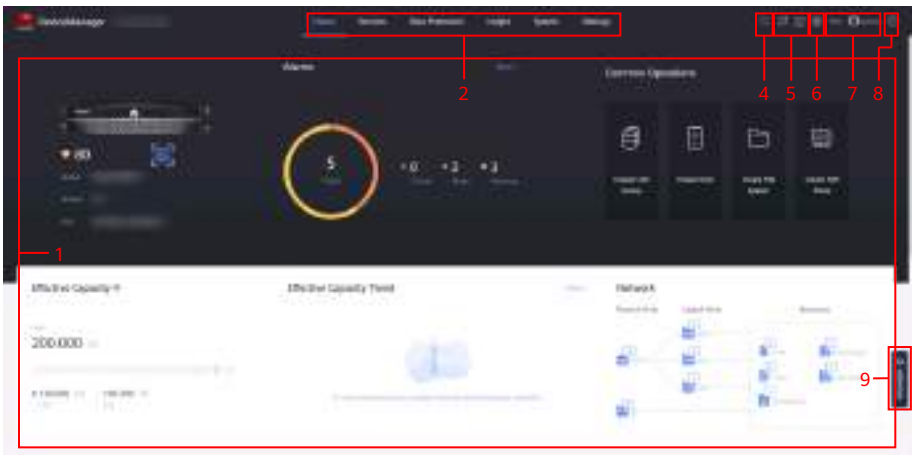


Figure 2-2 DeviceManager main window (OceanStor 6810, OceanStor 18510, and OceanStor 18810)

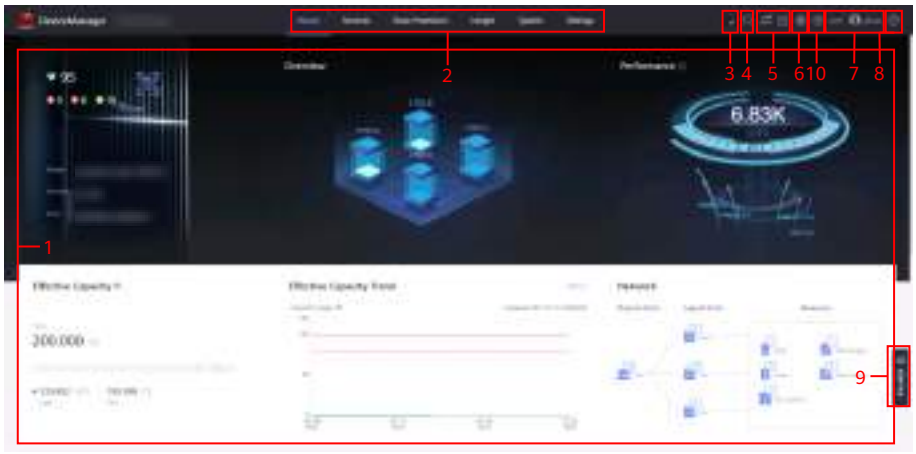


Table 2-2 describes the components of the DeviceManager main window.

Table 2-2 Components of the DeviceManager main window

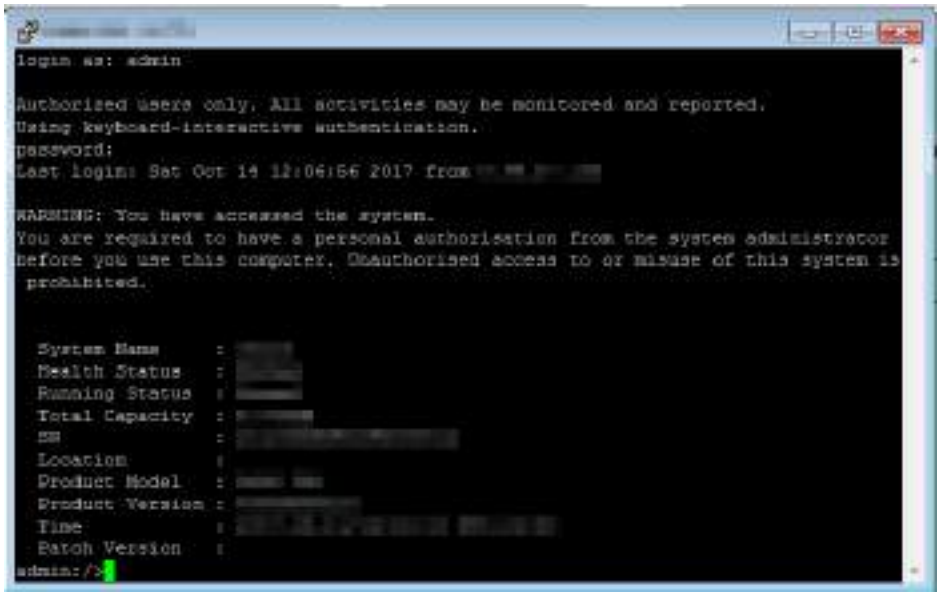
No.	Name	Description
1	Function pane	The function pane shows a page associated with the current operation.
2	Navigation bar	The navigation bar shows the functional modules of a storage system that are divided logically.
3	SmartGUI	SmartGUI mines users' historical operation data and builds a configuration parameter recommendation model based on user profiles to recommend configuration parameters for the block service and file service.
4	Global search	You can search for an object, page, or operation by entering the name of a LUN, LUN group, host, host group, port group, logical port, LUN snapshot, clone, and tenant.

No.	Name	Description
5	Alarm and task statistics area	The alarm statistics area displays the number of alarms of each severity, helping you learn about the running status of the system. All tasks executed by users are displayed in the task statistics area, helping you know whether the tasks are successfully executed.
6	Device management area	The device management area allows you to view and modify device information as well as power off and restart devices.
7	Logout and language switchover area	The logout and language switchover area provides a logout button and a language switchover button. DeviceManager supports simplified Chinese and English.
8	Help and technical support	This area provides links to the online help and technical support websites.
9	eService	Scan the QR code to query device information and eService settings.
10	Shortcut area	This area is for resource allocation and data protection.

Introduction to CLI

CLI enables you to use command lines to manage and maintain storage systems. After you input commands with the help of a keyboard, commands are interpreted and executed by the program, and execution results are displayed as text or graphics on CLI. **Figure 2-3** shows the CLI main window.

Figure 2-3 CLI main window



After logging in to CLI, you can view information about a storage system, including the system name, health status, running status, and total capacity.

Introduction to SmartKit

SmartKit is a desktop management platform on which all IT tools can be managed in a unified manner. It provides various tools for deployment, maintenance, and upgrade of IT devices. **Figure 2-4** shows the SmartKit main window.

Figure 2-4 SmartKit main window

Table 2-3 describes the components of the SmartKit main window.

Table 2-3 Description of functional areas in SmartKit

No.	Description
1	Navigation tree for functions: enables you to select functions.
2	Scheduled task and system setting buttons.
3	Buttons for obtaining online help and more information as well as selecting a language
4	SmartKit login account area: displays the account having the maximum permission.
5	**Authentication Now** button: enables you to authenticate your identity to obtain more functions and supports. **Exit** button: exits the current login account. You can check whether the enterprise network or carrier network service is obtained.
6	Field switching bar: enables you to switch between **Storage**, **Server**, **Cloud Compute**, and **Machine Vision**.
7	**Function Management** button: displays all the functions integrated in SmartKit. You can install, upgrade, or uninstall one or more functions on this page.
8	: enables you to upgrade the upgradable functions in the current scenario-based task. : enables you to install the functions that have not been installed in the current scenario-based task.
9	**More**: enables you to view all the functions of a product field to which the current scenario-based task belongs.
10	Scenario-based task entrance: enables you to use the corresponding function.
11	**Links** (for enterprise users): provides links to websites such as Bulletins, iKnow, Support-E, and InfoKit for Storage, InfoKit for Server, or InfoKit for Cloud Computing. **Links** (for carriers): provides links to the support website, EOX bulletins, recommended software versions, as well as InfoKit for Storage, InfoKit for Server, or InfoKit for Cloud Computing. NOTE: These links are not displayed on the **Home** page if the role of the login user is **Customer** or **Visitor**.

Introduction to eService

As a large number of Huawei IT products such as storage devices, servers, and cloud computing products are put into use, users have increasingly high requirements on the troubleshooting efficiency. In traditional service support

mode, technical support personnel provide local services manually. Faults may not be detected in a timely manner and information may not be delivered correctly.

The eService intelligent cloud O&M platform (eService for short) integrates cloud management, remote maintenance, automatic service request (SR) creation, and proactive prediction and prevention functions to improve customer O&M capabilities and takes planned maintenance actions to prevent potential risks.

Being authorized by customers, eService monitors device alarms in 24/7 mode. Whenever an alarm is detected, it automatically notifies the eService cloud system and creates SRs. Huawei service engineers will help customers solve problems in a timely manner.

eService enables the client to work with the cloud system.

- Client system: deployed on the customer side.

  It collects customer device alarms and sends them to the eService cloud system in a timely manner to implement remote maintenance functions, such as remote inspection and remote log collection.
- Cloud system: deployed on the eService cloud system.

  The eService cloud system receives device alarms from the client system in 24/7 mode, automatically notifies Huawei technical support personnel to handle the alarms in a timely manner, and supports remote inspection and log collection for devices on the customer side.

Intelligent O&M provided by eService has the following advantages:

- eService provides a self-service O&M system for customers, aiming for precise customized information services.
- Based on HUAWEI CLOUD, the eService cloud system drives IT O&M activities through big data analytics and artificial intelligence (AI) technologies to identify faults in advance, reduce O&M difficulties, and improve O&M efficiency.
- Data is encrypted during the data transmission, ensuring secure data transmission. eService can access the customer's system only after being authorized by the customer.
- eService provides 24/7 secure, reliable, and proactive O&M services. SRs can be automatically created.
- Customers can use any PC to access eService at any time and place to view device information.

For details, see the *eService Intelligent Cloud O&M Platform User Guide* or log in to **http://support.eservice.huawei.com** to access and use eService.

2.2 Logging In to the Storage System

You can log in to the storage system using either DeviceManager or the CLI to configure, manage, and maintain the system.

For details about how to log in to DeviceManager and the CLI, see "Logging In to DeviceManager" in the *Initialization Guide* and "Logging In to the CLI of the Storage System" in the *Command Reference* specific to your product model.

2.3 Logging In to the Storage System O&M Software

You can use the SmartKit software to deploy, maintain, and upgrade storage systems, and use eService Client to report the alarm notification and configuration data of storage systems.

2.3.1 Logging In to the eService Client

This section explains how to log in to eService.

Prerequisites

eService Client has been installed.

Procedure

Step 1 Start eService.

You can start eService using either of the following methods:

- After eService is installed, start eService immediately and click **Finish**.
- On the desktop, double-click the **eService** icon  to start eService.

Step 2 In the login dialog box that is displayed, select an interface language, fill in **Administrator Password**, and click **Log In**.

Step 3 Optional: Set the login password.

1. When you log in to the system for the first time, the system displays the message **Please set the password upon the first login**. Click **OK**.

   The **Set Password and Security Email Address** page is displayed

2. Enter the password and confirm the password and security email address, and click **OK**.

   The system displays a message indicating that the password and security email address are successfully set.

   NOTE

   - The new password must contain uppercase letters, lowercase letters, and special characters. The new password must contain 8 to 32 characters.
   - The password validity period is six months. Change the password within the specified period.

----End

Follow-up Procedure

For system security, eService will log out automatically if a user that has logged in does not perform any operations for 10 minutes. A window that asks you to log in again is displayed.

You can enter **Administrator Password** to log in to eService again.

2.3.2 Logging In to the SmartKit

After logging in to SmartKit, you can deploy, maintain, and upgrade storage devices through configuration. This section describes how to log in to SmartKit.

Context

- After SmartKit is installed, the background programs in ToolStore keep running and access the technical support website, obtaining upgrading information about SmartKit and tools in it and providing pop-up messages.
- You must have administrator rights to run some tools. Therefore, you are advised to run SmartKit as an operating system administrator.

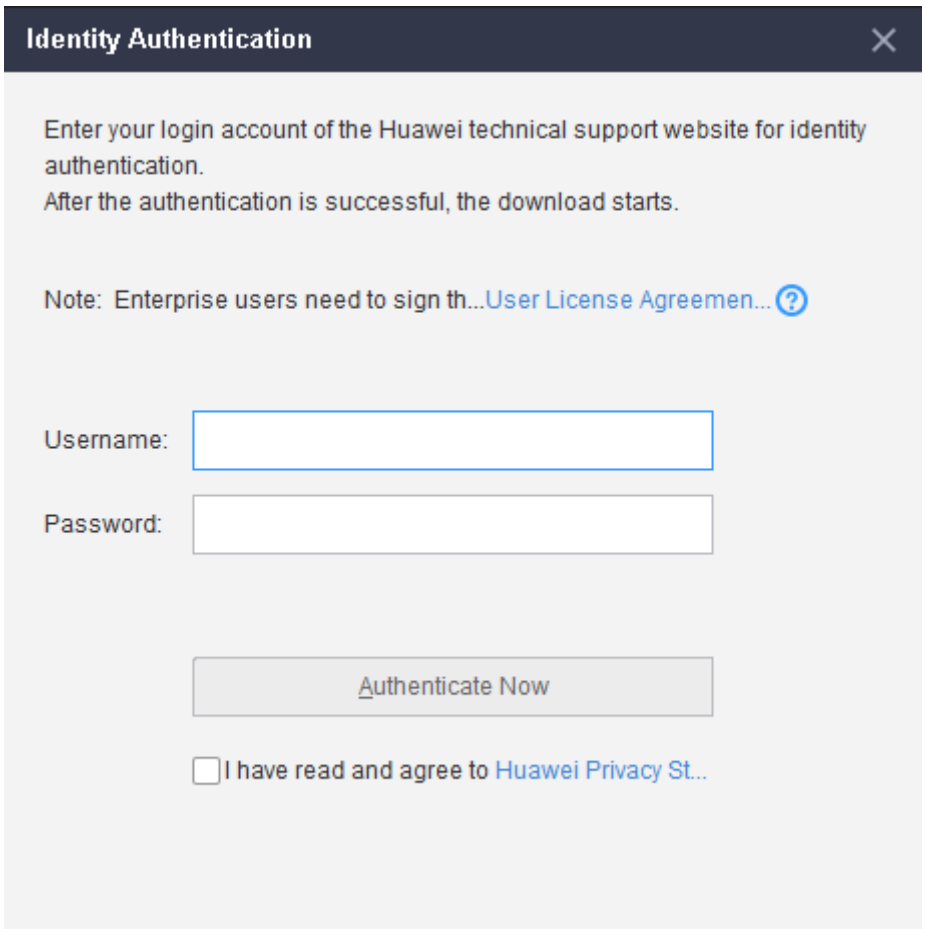
Procedure

Step 1 Run **SmartKit** on the maintenance terminal.

Step 2 (Optional) If you use SmartKit for the first time, a usage guide page is displayed introducing major functions of SmartKit.

Step 3 Perform identity authentication.

1. In the upper right corner, choose **Unauthenticated** > **Authenticate**. The **Identity Authentication** page is displayed.



2. Enter the username and password for the Huawei enterprise support website.

3. Read carefully **Huawei Privacy Statement**, and then select **I have read and agree to Huawei Privacy Statement**.

   NOTE

   You can click **Huawei Privacy Statement** to read the statement.

4. Click **Authenticate Now**. The **Identity Authentication** page is displayed.
5. Select the right service, which can be **Enterprise** or **Carrier**.
6. Click **OK** to complete the identity authentication for SmartKit.

----End

3 Maintenance Item Overview

This list of maintenance items and frequencies helps system administrators check the device environment and device status. If a fault occurs, it will be detected and rectified in a timely manner, ensuring that the storage systems continue running normally.

Table 3-1, **Table 3-2**, and **Table 3-3** describe the first, daily, and weekly maintenance items, respectively.

Table 3-1 First maintenance items

Maintenance Item	Operation
Checking the installation of SmartKit tools	On the maintenance terminal, check whether SmartKit tools have been installed. • Device Archive Collection • Storage Information Collection • Disk Health Analysis • Inspection • Hot Patch Installation **NOTE** If SmartKit has not been installed, log in to **https://support.huawei.com/enterprise/en**, search **SmartKit**, and download the installation package and operation guide of the corresponding version. Follow instructions in the operation guide to install tools.
Checking the installation and configuration of eService	On the maintenance terminal, check whether eService has been installed and an appropriate alarm policy has been configured. **NOTE** If eService has not been installed, log in to **https://support.huawei.com/enterprise/en**, search **eService**, and download the installation package and operation guide of the corresponding version. Follow instructions in the operation guide to install tools.

Maintenance Item	Operation
Checking the alarm policy configuration	On DeviceManager, check whether the alarm policy has been configured. The alarm policy is for sending alarms to client servers or mobile phones, to allow customers to promptly check and handle alarms, including: • Email notification • SMS notification • System notification • Alarm dump • Trap IP address management • USM user management • Alarm masking • Syslog notification **NOTE** If it has not been configured, see section **Configuring Alarm Handling Policies** of the *Initialization Guide* of the corresponding product model.

Table 3-2 Daily maintenance items

Maintenance Item	Operation
Checking and handling alarms	Log in to DeviceManager or use the alarm reporting mode that has been configured to view and handle the alarms in a timely manner based on the suggestions. **NOTE** If an alarm still exists, use SmartKit tools to collect relevant information and contact Huawei technical support.

Table 3-3 Weekly maintenance items

Maintenance Item	Operation
Checking storage devices	On a maintenance terminal, use the tool **Inspection** of SmartKit to perform checks. • Hardware status • Software status • Value-added services • Alarm check **NOTE** If a fault occurs and the rectification method recommended by the tool does not work, use SmartKit to collect fault information and contact Huawei technical support.
Checking the equipment room environment	Check the equipment room environment according to **4.2.2.1 Check Method**. **NOTE** If the equipment room environment does not meet the requirements, adjust the environment in a timely manner based on the related specifications.
Checking the rack environment	Check whether the rack environment meets requirements in section **4.2.2.2.2 Checking Racks**. **NOTE** If the rack environment cannot meet the requirements, adjust the environment accordingly in a timely manner.

4 Routine Maintenance

Routine maintenance allows you to check the operating environment and device status and handle exceptions in time, ensuring normal device running.

4.1 Inspection Using SmartKit

You can use the SmartKit inspection tool to inspect the storage system based on the inspection policy you have set. Device inspection enables you to know the real-time status of the device.

Prerequisites

The SmartKit inspection tool has been installed on the maintenance terminal.

Context

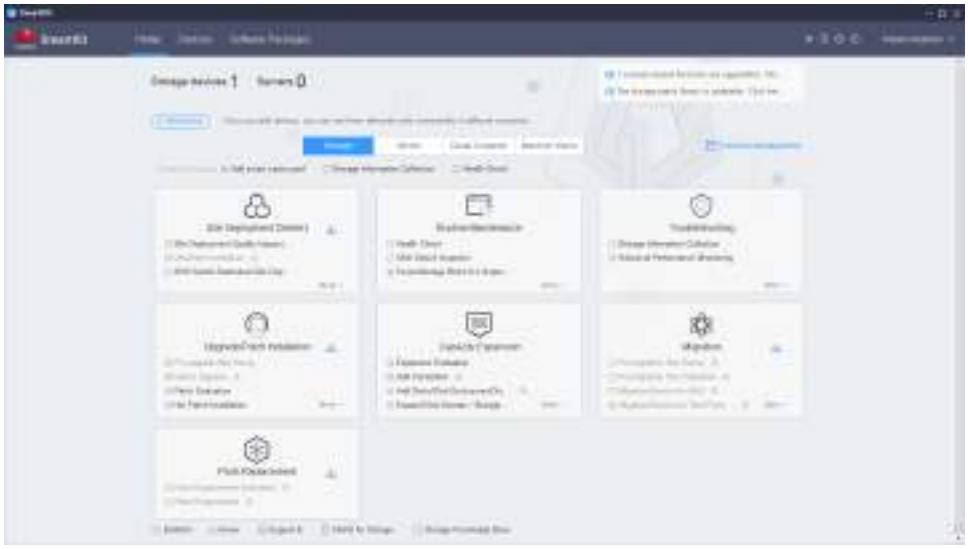
After starting SmartKit, you can obtain tool use instructions by clicking  in the upper right corner of the interface.

Procedure

Step 1 Start SmartKit.

The **SmartKit** page is displayed, as shown in **Figure 4-1**.

Figure 4-1 SmartKit homepage



Step 2 Add a device.

1. Click **Devices** and then **Add**.

   The **Add device step 2-1: Basic Information** dialog box is displayed.

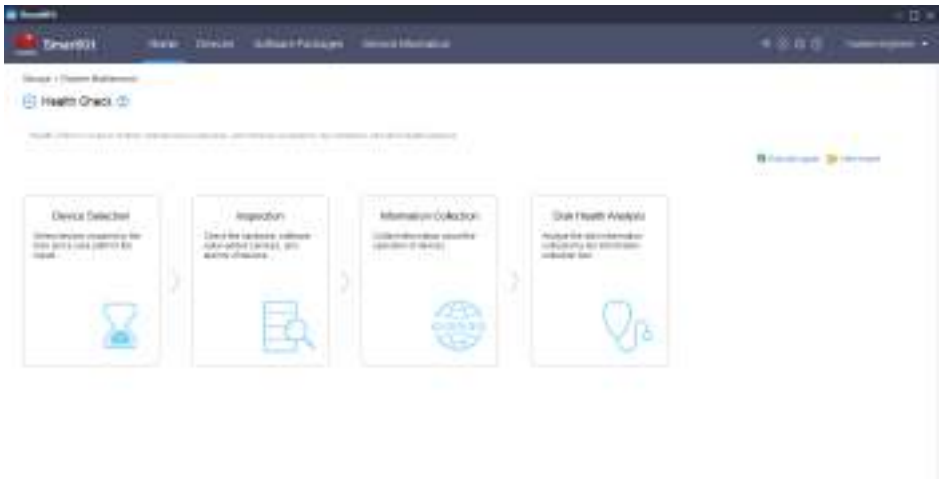
2. Enter basic information, including the IP address and proxy. In the **Add Policy** and **Select Proxy** areas, select **Specify IP Address (add a device by the IP address)** and **No Proxy**, respectively.
3. Enter configurations, including the user name, password, and port of the device. Click **Next**. In the **Login Information** area, enter **Username**, **Password**, and **Port** of the device to be added. The default value of **Port** is **22**.
4. Click **Finish**.

   The newly added device is displayed in the device list.

Step 3 Inspect a device.

1. On the main page, choose **Routine Maintenance** > **Health Check**.

   The **Health Check** page is displayed.



2. Click in the upper left part, and perform related operations by following instructions.

----End

4.2 Manual Inspection

This section describes the manual inspection items, including routine inspections on the equipment room condition, cabinet condition, and device running indicators. The inspection results help maintenance engineers understand the device running status and detect exceptions.

4.2.1 Viewing and Handling Alarms

Detailed descriptions and troubleshooting suggestions are provided to each alarm in the list for convenient fault rectification.

Precautions

Exported alarms and events are saved in ***.tgz** (Save All) or ***.xls** (Save Selected) file. Do not change the content of the file.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Insight** > **Alarm and Events** > **Current Alarms**.

Step 3 **Optional**: Click next to **Severity**, **Object**, or **Occurred** to filter alarms. Click next to **ID** to search for alarms.

Step 4 Click **Description** of an alarm and handle the alarm by referring to **Suggestion** on the right.

NOTE

After SmartGUI is enabled (by clicking the button on the top of the DeviceManager home page), the intelligent alarm analysis function is supported for some capacity and fault alarms. For an alarm that supports the intelligent analysis function, on the **Alarm Details** page, choose **Suggestion** > **intelligent alarm analysis** to view the intelligent analysis result. The intelligent alarm analysis function will display all the alarms related to the alarm and provides handling suggestions. You can quickly locate the root causes of alarms and rectify faults according to handling suggestions. To view traditional handling suggestions, choose **Suggestion** > **Switch Back to Traditional Suggestion**.

Step 5 **Optional:** Clear alarms.

1. In the alarm list, select the alarms that you want to clear and click **Clear**.
2. In the information dialog box that is displayed, click **OK**.

Step 6 **Optional:** Export alarms.

Select the alarms to be exported, click , and perform operations as prompted.

Step 7 **Optional:** Click **Send Simulated Alarm** to simulate the reporting of a fault alarm.

Send this simulated alarm to test the alarm function of the device. If this simulated alarm already exists, this alarm will be considered invalid after being resent. Before the test, confirm that this simulated alarm has been manually cleared. After the test, manually clear the alarm.

----End

4.2.2 Checking the Operating Environment of the Storage Device

Check that the operating environment in which the storage device works meets associated requirements to ensure stable running of the device.

4.2.2.1 Check Method

This section describes how to check the equipment room environment. Checking the equipment room helps the maintenance personnel know the environment conditions and detect potential environment risks to prevent device faults due to environment issues.

Storage devices require a reliable operating environment. Usually, they are installed in a dedicated equipment room with a dedicated air-conditioning system and a redundant power system. **Table 4-1** lists the environment check items. For the check criteria, see **4.2.2.2 Check Criteria**.

Table 4-1 Environment check items

Item	Check Method
Temperature, humidity, and altitude	Read the thermometer, and hygrometer, and barometer in the equipment room.
Vibration and shock	Hire a professional organization to measure the vibration and shock on the storage system when it is working or stored.
Particle contaminants	Hire a professional organization to monitor the particle contaminants in the equipment room.
Corrosive gas contaminants	Hire a professional organization to monitor the corrosive gas contaminants in the equipment room.

Item	Check Method
Internal rack environment	• Verify that power cables (with strong electrical current) and service cables (with weak electrical current) lay on different sides of a rack. • Verify that power cables and service cables are laid out orderly and arranged in a similar manner to cables on other racks. • Verify that labels are clearly marked and securely attached. • Verify that vacant slots are covered with filler panels. • Verify that one end of each power cable is fully plugged into an external power socket and the other end into a storage device socket. • Verify that signal cables are fully plugged into appropriate device ports. • Verify that one end of each ground cable is secured by a ground clip and the other end is fastened to a rack ground terminal. • Verify that two groups of power cables are available for redundancy. • Verify that each network cable or optical fiber is correctly connected to the front-end port of the storage device and the application server port or switch. Verify that the management network port is connected to the network of the maintenance terminal.

Troubleshooting

- If the measured temperature or humidity falls outside the normal range, tune the air conditioners in the equipment room until the temperature or humidity falls within the normal range.
- If the power supply system fails to meet the standard, append dedicated power lines and a power transformer with sufficient capacity.

4.2.2.2 Check Criteria

This section describes the criteria for checking the storage system's operating environment.

4.2.2.2.1 Equipment Operating Environment

Environment requirements cover temperature, humidity, particle contaminants, corrosive airborne contaminants, heat dissipation, and noise.

For details, see section **Environmental Requirements** in the *Product Description* of the corresponding product model.

4.2.2.2.2 Checking Racks

Properly installed racks of the storage device help ensure the stable and long-term running of the storage device. Check rack conditions periodically to reduce device failure possibilities.

Impact on the System

The storage device imposes demanding requirements on rack conditions. An improperly installed rack impairs the proper running of the storage device.

Tools and Materials

Ensure that the tools and materials for checking rack conditions are available. The required tools include binding straps, an electroprobe, and a multimeter.

Reference Standard

Table 4-2 lists the items and standards for checking rack conditions.

Table 4-2 Rack condition check items and standards

Check Item	Standard
In-rack environment	There is no sundries, dust, or metal scraps in the rack. After installing or removing devices in the rack, clean the metal scraps in time.
General layout of cables	Power cables (with strong electrical current) and service cables (with weak electrical current) lay on different sides of a rack.
Layout of power cables	Power cables are laid out orderly and arranged in a similar manner to power cables on other racks.
Layout of service cables	Service cables are laid out orderly and arranged in a similar manner to service cables on other racks.
Cable labeling	Labels are clearly marked and securely attached.
Empty slot	Empty slots are covered with filler panels for proper heat dissipation and a neat appearance.
Power cable plug	One end of each power cable is fully plugged into an external power socket and the other end into a storage device socket.
Signal cable plug	Signal cables are fully plugged into appropriate device ports.
Ground cable	One end of each ground cable is secured by a ground clip and the other end is fastened to a rack ground terminal.
Power cable	Two groups of power cables are available for redundancy.

Check Item	Standard
Front-end port connection	• For Ethernet front-end ports, each network cable is properly connected to the front-end port and the application server port or switch. • For Fibre Channel front-end ports, each optical fiber is properly connected to the front-end port and the application server port or switch.
Management network port connection	The management network cable is properly connected to the management network port and the network of the maintenance terminal.

Procedure

- Verify that power cables (with strong electrical current) and service cables (with weak electrical current) lay on different sides of a rack.
- Verify that power cables and service cables are laid out orderly and arranged in a similar manner to cables on other racks.
- Verify that labels are clearly marked and securely attached.
- Verify that vacant slots are covered with filler panels.
- Verify that one end of each power cable is fully plugged into an external power socket and the other end into a storage device socket.
- Verify that signal cables are fully plugged into appropriate device ports.
- Verify that one end of each ground cable is secured by a ground clip and the other end is fastened to a rack ground terminal.
- Verify that two groups of power cables are available for redundancy.
- Verify that each network cable or optical fiber is correctly connected to the front-end port of the storage device and the application server port or switch.
- Verify that the management network port is connected to the network of the maintenance terminal.

Troubleshooting

If any check item fails to meet its standard, rectify the issue by referring to **Table 4-2**.

4.2.3 Checking Indicators

Indicators reflect the working status of hardware in real time. By observing these indicators, you can quickly assess whether the hardware is working properly.

4.2.3.1 Check Method

By observing the indicators, maintenance personnel can understand the system health status and locate faulty modules.

Check the front-panel and rear-panel indicators on the controller enclosure on site according to the check criteria to determine whether all components on the controller enclosure are working properly.

If a module of the storage system is abnormal, refer to the *Product Description* of the corresponding product model to learn about detailed indicator meanings. Then, troubleshoot faults based on the detailed fault information you have obtained.

4.2.3.2 Check Criteria

For details about the meaning of each indicator status, see the *Product Description* of the corresponding product model.

4.2.4 Checking the Running Status of the Storage Device

This section describes how to check the running status of a storage device by examining its indicators and checking the functional status on DeviceManager. This allows you to detect device faults in time.

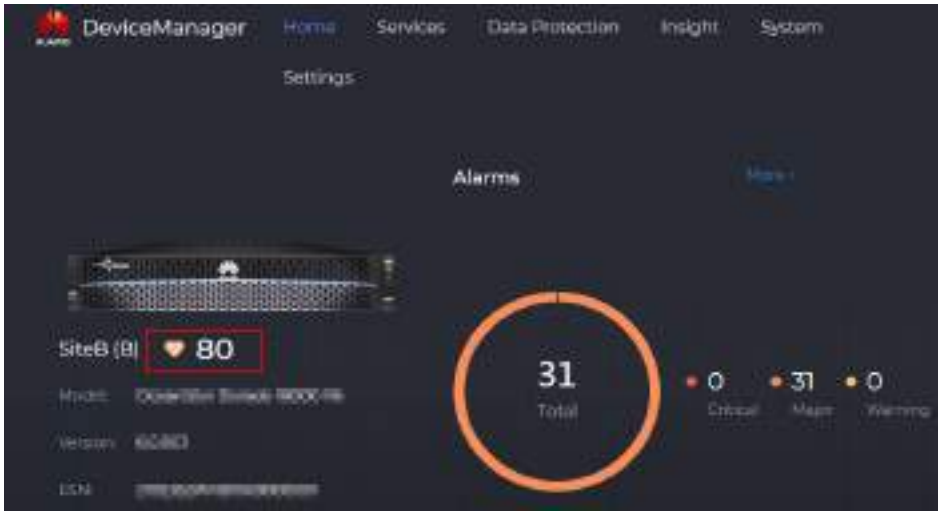
4.2.4.1 Checking the Storage System Status

Check the storage system status on the DeviceManager home page.

Check Criteria

You can view the storage system status on the DeviceManager home page, as shown in **Figure 4-2**.

Figure 4-2 Storage system status



- When no alarm is generated in the storage system, the system status is **100**.
- When the highest severity among the alarms generated in the storage system is **Warning**, the system status is **95**.

- When the highest severity among the alarms generated in the storage system is **Major**, the system status is **80**.
- When the highest severity among the alarms generated in the storage system is **Critical**, the system status is **60**.
- If the running status of the storage system is abnormal, the system status is **0**.

4.2.4.2 Checking the Storage System Inventory

You can query the number and health status of storage devices in the inventory on DeviceManager.

Procedure

Step 1 Choose **System** > **Hardware** > **Inventory**.

Step 2 Query the number and health status of enclosures, controllers, disks, and ports in the inventory.

Step 3 Select **Enclosures**, **Controllers**, **Disks**, or **Ports** to query more details in the lower pane. **Table 4-3**, **Table 4-4**, **Table 4-5**, and **Table 4-6** describe the information of each component.

Table 4-3 Enclosure (controller enclosure/disk enclosure) information

Parameter	Description
Name	Name of the enclosure.
Health Status	Health status of the enclosure. Possible values are: • **Normal**: The functionality and operating performance of the enclosure are normal. • **Faulty**: The enclosure is working improperly. • **Unknown**: Whether the enclosure functions properly cannot be determined. For example, if a disk enclosure is faulty, the storage system cannot query the health status of the disk enclosure.
Running Status	Running status of the enclosure. Possible values are **Online** and **Offline**.
Model	Model of the enclosure.

Parameter	Description
Temperature (°C)	Temperature of the enclosure.
ESN	Equipment serial number of the enclosure.
MAC Address	MAC address of the enclosure.
Locate Enclosure	When the enclosure is being located, its location indicator is blinking.
Cancel Locating	When you cancel locating the enclosure, its location indicator is off.

Table 4-4 Controller information

Parameter	Description
Location	Location of the controller.
Health Status	Health status of the controller. Possible values are: • **Normal**: The functionality and operating performance of the controller are normal. • **Faulty**: The controller is working improperly. • **Unknown**: Whether the controller functions properly cannot be determined. For example, if a controller is faulty, the storage system cannot query the health status of the controller.
Running Status	Running status of the controller. Possible values are **Unknown**, **Normal**, **Running**, **Sleep in high temperature**, **Online** and **Offline**.
CPU	CPU model.
Cache	Cache size of the controller.
Temperature (°C)	Temperature of the controller.
Role	Possible values are **Primary** and **Secondary**.
Electronic Label	Electronic label of the controller.

Table 4-5 Disk information

Parameter	Description
Location	Location of the disk.
Capacity	Usable capacity of the disk.

Parameter	Description
Manufacturing Capacity	Nominal capacity defined by the manufacturer.
ID	Disk ID.
Disk Domain	Disk domain to which the disk belongs.
Type	Possible values are **SSD**, **SSD SED**, **NVMe SSD**, and **NVMe SSD SED**.
Role	Possible values are **Free disk**, **Member disk**, **Hot spare disk**, and **Cache disk**.
Health Status	Health status of the disk. Possible values are: • **Normal**: The functionality and operating performance of the disk are normal. • **Faulty**: The disk is working improperly. • **Failing**. The disk is failing and must be replaced soon.
Running Status	Running status of the disk. Possible values are **Online** and **Offline**.
Degree of Wear	Wear degree of the disk. The disk service life is determined by erasure times. The system computes the remaining service life and total service life under the current workload based on disk wear status in the last one or multiple statistical periods and uses the percentage of used service life (the total service life minus the remaining service life) to the total service life as the degree of wear.
Estimated Lifespan (Months)	Estimated service life of the disk.
BOM	BOM of the disk.
Barcode	Barcode of the disk, which helps asset management.
Data Erasure Progress	Data erasure progress of the disk.
Encryption Type	Encryption type of the disk.
AK Expiration Date	This parameter is valid only for self-encrypting drives (SEDs).
Model	Model of the disk.
Locate Disk	When the disk is being located, its location indicator is blinking.
Cancel Locating	When you cancel locating the disk, its location indicator is off.
Erase Data	Erases data on non-member disks. For details, see **5.16 Erasing Data from Disks (SmartErase)**.

Table 4-6 Port (Ethernet port/FC port) information

Parameter	Description
Name	Name of the port.
Location	Location of the port.
ID	ID of the port.
Health Status	Health status of the port. Possible values are: • **Normal**: The functionality and operating performance of the port are normal. • **Faulty**: The port is working improperly. • **Unknown**: Whether the port functions properly cannot be determined. For example, if a port is faulty, the storage system cannot query the health status of the port. • **Bit errors found**: The application server or other storage devices cannot communicate with the storage system through the port, which may deteriorate the service performance of the device.
Running Status	Running status of the port. Possible values are **Link up** and **Link down**.
MAC Address[a]	MAC address of the Ethernet port.
IPv4 Address/ Subnet Mask[a]	IPv4 address and subnet mask of the Ethernet port.
IPv6 Address/ Prefix[a]	IPv6 address and prefix of the Ethernet port.
WWPN[b]	WWPN of the Fibre Channel port.
Working Rate (Gbit/s)	Working rate of the port.
Max. Working Rate (Gbit/s)	Maximum working rate of the port.
MTU (Bytes)[a]	Maximum size of a data packet that can be transferred between the Ethernet port and the application server.
Operation Mode[b]	Possible values are: • **FC-AL**: indicates the arbitrated loop mode. • **P2P**: indicates the point-to-point mode. • **auto_adapt**: indicates the autonegotiation mode.
Bond Name[a]	Bond name of the Ethernet port.

Parameter	Description
Logical Type[a]	Possible values are **Management port**, **Maintenance port**, or **Front-end port**.
Port State	Isolation status of the port. Possible values are **Enabled** and **Disabled**. When **Port State** is **Disabled**, the port cannot be used.
Initiators	Number of initiators for the port.
a: Applies only to Ethernet ports. b: Applies only to Fibre Channel ports.	

----End

4.2.4.3 Checking Controller Enclosures or Disk Enclosures

You can learn about the health and running status of a controller enclosure or disk enclosure by checking its status information on DeviceManager.

Impact on the System

A fault in a controller enclosure or disk enclosure may impair read/write performance, reduce reliability, even interrupt system services, and cause data loss.

Reference Standard

If a controller enclosure or disk enclosure is working properly, the following items are true on DeviceManager:

- **Health Status** of the enclosure is **Normal**, and **Running Status** is **Online**.
- No enclosure alarm appears on the **Current Alarms** tab page.

Procedure

Step 1 Choose **System** > **Hardware** > **Devices**.

Step 2 Click the desired controller enclosure or disk enclosure.

The detailed information about the enclosure is displayed.

Step 3 View the enclosure information in the dialog box that is displayed.

Table 4-7 describes the parameters.

Table 4-7 Enclosure parameters

Parameter	Description
Health Status	Health status of the enclosure. Possible values are: • **Normal**: The enclosure is functioning properly. • **Faulty**: The enclosure is functioning improperly.

Parameter	Description
Running Status	Running status of the enclosure. Possible values are **Online** and **Offline**.
Model	Model of the enclosure.
Temperature (°C)	Temperature of the enclosure.
ESN	Serial number of the enclosure.
MAC Address	MAC address of the enclosure.
Electronic Label	Electronic label of the enclosure. **NOTE** The electronic label shows only the factory defaults of the device and is used to trace production information. This information does not change after capacity expansion.

----End

Follow-up Procedure

If an enclosure alarm appears on the **Current Alarms** tab page, select and handle the alarm according to its details and repair suggestions.

4.2.4.4 Checking Controllers

Controllers in a storage system process storage applications, implement storage mechanisms (storage pool, LUN mapping, and stripe setting), and manage alarms. You can learn about the health and running status of a controller by checking its status information on the DeviceManager.

Impact on the System

A fault on a controller may impair read/write performance, deteriorate reliability, interrupt services, or cause data loss.

Reference Standard

If controllers are working properly, the following items are true on the DeviceManager:

- All of the controllers are in the **Normal** health status and **Online** running status.
- No controller alarm appears on the **Current Alarms** tab page.

Procedure

Step 1 Choose **System > Hardware > Devices**.

Step 2 In the navigation tree on the left, select the controller enclosure where the controller to be checked resides.

Step 3 Click the controller to be checked in the device view on the right.

The detailed information about the controller is displayed.

NOTE

You can click  to adjust the device view.

Step 4 View the controller information in the dialog box that is displayed.

Table 4-8 describes associated status parameters.

Table 4-8 Controller status parameters and their meanings

Parameter	Description
Health Status	Health status of the controller. Possible values are: • **Normal**: The functionality and operating performance of the controller are normal. • **Faulty**: The controller is working improperly.
Running Status	Running status of the controller. Possible values are **Online** and **Offline**.

----End

Follow-up Procedure

If a controller alarm appears on the **Current Alarms** tab page, select the alarm and diagnose the problem according to its details and repair suggestions.

4.2.4.5 Checking Power Modules

Power modules provide power for controller enclosures and disk enclosures, ensuring reliable running of storage systems. You can learn about the health and running status of a power module by checking its status information on the DeviceManager.

Impact on the System

- If a power module is faulty, data reliability deteriorates.
- If all of the power modules are faulty, services are interrupted and the storage device is powered off.

Reference Standard

If power modules are working properly, the following items are true on the DeviceManager:

- All of the power modules are in the **Normal** health status and **Online** running status.

- No power module alarm appears on the **Current Alarms** tab page.

Procedure

Step 1 Choose **System > Hardware > Devices**.

Step 2 In the navigation tree on the left, select the controller enclosure or disk enclosure where the power module to be checked is located.

Step 3 Click the power module to be checked in the device view.

The detailed information about the power module is displayed.

NOTE

You can click  to adjust the device view.

Step 4 View the power module information in the group box that is displayed.

Table 4-9 describes associated status parameters.

Table 4-9 Power module status parameters and their meanings

Parameter	Description
Health Status	Health status of a power module. The value can be: • **Normal**: The functionality and operating performance of the power module are normal. • **Faulty**: The power module is working improperly. • **No input**: The power module has been installed but does not supply power.
Running Status	Running status of a power module. The value can be **Online** or **Offline**.

----End

Follow-up Procedure

If a power module alarm appears on the **Current Alarms** tab page, select the alarm and diagnose the problem according to its details and repair suggestions.

4.2.4.6 Checking Controller Enclosure BBUs

Controller enclosure backup battery units (BBUs) provide power failure protection for controller enclosures, allowing data to be stored in the event of a power failure. You can learn about the health and running status of a BBU by checking its status information on DeviceManager.

Impact on the System

BBUs of controller enclosures provide power supply to controller enclosures upon power failure. In this way, data can be saved even if controller enclosures

encounter power failure. If the BBUs also become faulty, cache data cannot be saved to disks upon power failure, resulting in data loss.

Reference Standard

If controller enclosure BBUs are working properly, the following items are true on the DeviceManager:

- All of the BBUs are in the **Normal** health status and **Online** running status.
- No BBU alarm appears on the **Current Alarms** tab page.

Procedure

Step 1 Choose **System > Hardware > Devices**.

Step 2 In the navigation tree on the left, select the controller enclosure where the BBU module to be checked is located.

Step 3 Click the BBU module to be checked in the device view.

The detailed information about the BBU module is displayed.

NOTE

You can click  to adjust the device view.

Step 4 View the BBU information in the group box that is displayed.

Table 4-10 describes associated status parameters.

Table 4-10 BBU status parameters and their meanings

Parameter	Description
Health Status	Health status of a BBU. The value can be: • **Normal**: The functionality and operating performance of the BBU are normal. • **Faulty**: The BBU is working improperly. • **Insufficient power**: The power level of the BBU is low though its operating performance is normal.
Running Status	Running status of a BBU. The value can be **Online**, **Charging**, or **Discharging**.

----End

Follow-up Procedure

If a BBU alarm appears on the **Current Alarms** tab page, select the alarm and diagnose the problem according to its details and repair suggestions.

4.2.4.7 Checking Fan Modules

Fan modules provide a cyclic aeration system to a controller enclosure or disk enclosure, ensuring the stable running of a storage system. You can learn about the health and running status of a fan module by checking its status information on the DeviceManager.

Impact on the System

If a fan module malfunctions, the temperature of the controller enclosure or disk enclosure may rise, causing system exceptions.

Reference Standard

If fan modules are working properly, the following items are true on the DeviceManager:

- All of the fan modules are in the **Normal** health status and **Running** running status.
- No fan module alarm appears on the **Current Alarms** tab page.

Procedure

Step 1 Choose **System > Hardware > Devices**.

Step 2 In the navigation tree on the left, select the disk enclosure or controller enclosure where the fan module to be checked is located.

Step 3 Click the fan module to be checked in the device view.

The detailed information about the fan module is displayed.

NOTE

You can click  to adjust the device view.

Step 4 View the fan module information in the group box that is displayed.

Table 4-11 describes associated status parameters.

Table 4-11 Fan module status parameters and their meanings

Parameter	Description
Health Status	Health status of a fan module. The value can be: • **Normal**: The functionality and operating performance of the fan module are normal. • **Fault**: The fan module is working improperly.
Running Status	Running status of a fan module. The value can be **Running** or **Not running**.

----End

Follow-up Procedure

If a fan module alarm appears on the **Current Alarms** tab page, select the alarm and diagnose the problem according to its details and repair suggestions.

4.2.4.8 Checking Disks

Disks are used to store data as a basic component of the storage device. You can learn about the health and running status of a disk by checking its status information on DeviceManager.

Impact on the System

Faulty disks may impair read/write performance and cause data loss on the storage device.

Reference Standard

If disks are working properly, the following items are true on DeviceManager:

- All of the disks are in the **Normal** health status and **Online** running status.
- No disk alarm appears on the **Current Alarms** tab page.

Procedure

Step 1 Choose **System > Hardware > Devices**.

Step 2 In the navigation tree on the left, select the disk enclosure or controller enclosure where the disk to be checked is located.

Step 3 Click the disk to be checked in the device view.

The detailed information about the disk is displayed.

Step 4 View the disk information in the group box that is displayed.

Table 4-12 describes associated status parameters.

Table 4-12 Disk status parameters and their meanings

Parameter	Description
Health Status	Health status of a disk. The value can be: • **Normal**: The functionality and operating performance of the disk are normal. • **Faulty**: The disk is working improperly. • **Failing**: The disk is about to fail.
Running Status	Running status of a disk. The value can be **Online** or **Offline**.

----End

Follow-up Procedure

If a disk alarm appears on the **Current Alarms** tab page, select the alarm and diagnose the problem according to its details and repair suggestions.

4.2.4.9 Checking Front-End Ports

Front-end ports enable service communication between the storage device and application servers. You can learn about the health and running status of a front-end port by checking its status information on the DeviceManager.

Impact on the System

Faulty front-end port may disable service communication between the storage device and application servers.

Reference Standard

If front-end ports are working properly, the following items are true on the DeviceManager:

- All of the front-end ports are in the **Normal** health status and **Link Up** running status.
- No front-end port alarm appears on the **Current Alarms** tab page.

Procedure

Step 1 Choose **System > Hardware > Devices**.

Step 2 In the navigation tree on the left, select the controller enclosure where the front-end port to be checked is located.

Step 3 Click the front-end port to be checked in the device view.

The detailed information about the front-end port is displayed.

NOTE

You can click  to adjust the device view.

Step 4 View the front-end port information in the group box that is displayed.

Table 4-13 describes associated status parameters.

Table 4-13 Front-end port status parameters and their meanings

Parameter	Description
Health Status	Health status of a front-end port. The value can be: • **Normal**: The functionality and operating performance of the front-end port are normal. • **Faulty**: The front-end port is working improperly.

Parameter	Description
Running Status	Running status of a front-end port. The value can be **Link up** or **Link down**.

----End

Follow-up Procedure

If a front-end port alarm appears on the **Current Alarms** tab page, select the alarm and diagnose the problem according to its details and repair suggestions.

4.2.4.10 Checking Interface Modules

Interface modules are used to house front-end port and expansion ports. You can learn about the health and running status of an interface module by checking its status information.

Impact on the System

Faulty interface modules may disable the communication between the storage device and application servers, controller enclosure and disk enclosures, or storage device and storage devices.

Reference Standard

If interface modules are working properly, the following items are true on the DeviceManager:

- All of the interface modules are in the **Normal** health status and **Running** running status.
- No interface module alarm appears on the **Current Alarms** tab page.

Procedure

Step 1 Choose **System** > **Hardware** > **Devices**.

Step 2 In the navigation tree on the left, select the controller enclosure where the interface module to be checked is located.

Step 3 Click the interface module to be checked in the device view.

The detailed information about the interface module is displayed.

NOTE

You can click  to adjust the device view.

Step 4 View the interface module information in the group box that is displayed.

Table 4-14 describes associated status parameters.

Table 4-14 Interface module status parameters and their meanings

Parameter	Description
Health Status	Health status of an interface module. The value can be: • **Normal**: The functionality and operating performance of the interface module are normal. • **Faulty**: The interface module is working improperly.
Running Status	Running status of an interface module. The value can be **Link up** or **Link down**.

----End

Follow-up Procedure

If an interface module alarm appears on the **Current Alarms** tab page, select the alarm and diagnose the problem according to its details and repair suggestions.

4.2.4.11 Checking Remote Devices

You can learn about the health and running status of a remote device connecting to the storage device by using the DeviceManager.

Impact on the System

Faulty remote devices may cause data backup interruption or data loss.

Reference Standard

If remote devices are working properly, their **Health Status** is **Normal** and **Running Status** is **Link Up** on the DeviceManager.

Procedure

Step 1 Choose **Data Protection** > **Configuration** > **Remote Devices**.

Step 2 On the **Remote Devices** page, view the detailed information about the desired remote device.

Table 4-15 describes associated status parameters.

Table 4-15 Remote device status parameters and their meanings

Parameter	Description
Health Status	Health status of a remote device. The value can be: • **Normal**: The remote device is working properly. • **Faulty**: The remote device is working improperly.
Running Status	Running status of a remote device. The value can be **Link up** or **Link down**.

----End

Follow-up Procedure

For a remote device, if its **Health Status** is **Faulty** or **Running Status** is **Link down**, contact our technical support engineers for troubleshooting.

4.2.5 Checking the Running Status of Services

You need to check the running status of various services running on the storage device by using DeviceManager. This allows you to discover service faults in a timely manner, preventing data loss caused by service interruptions.

4.2.5.1 Checking Storage Pools

A storage pool is a logical disk group consisting of independent physical disks. It provides higher storage performance and redundancy than a single disk. You can learn about the health and running status of a storage pool by checking its status information on DeviceManager.

Impact on the System

A faulty or degraded storage pool may impair read/write performance, interrupt services, and cause data loss on the storage device.

Reference Standard

If storage pools are working properly, the following items are true on DeviceManager:

- All of the storage pools are in the **Normal** health status and **Online** running status.
- No storage pool alarm appears on the **Current Alarms** tab page.

Precautions

None

Procedure

Step 1 On the navigation bar of DeviceManager, select **System > Storage Pools**.

The **Storage Pools** page is displayed.

Step 2 On the **Storage Pools** page, view the information about the desired storage pool.

Table 4-16 describes associated status parameters.

Table 4-16 Storage pool status parameters and their meanings

Parameter	Description
Health Status	Health status of a storage pool. The value can be: • **Normal**: The functionality and operating performance of the storage pool are normal. • **Degrade**: The storage pool is working in a poor performance. • **Faulty**: The storage pool is working improperly.
Running Status	Running status of a storage pool. The value can be **Online**, **Reconstruction**, **Precopy**, **Initializing**, **Deleting** or **Offline**.

----End

Troubleshooting

If a storage pool alarm appears on the **Current Alarms** tab page, select the alarm and diagnose the problem according to its details and repair suggestions.

4.2.5.2 Checking LUNs

For application servers, each LUN is an independent disk that provides storage space. You can learn about the health and running status of a LUN by checking its status information on DeviceManager.

Impact on the System

Faulty LUNs may interrupt services and cause data loss on the storage device.

Reference Standard

If LUNs are working properly, the following items are true on DeviceManager:

- All of the LUNs are in the **Normal** health status and **Online** running status.

  NOTE

  If you remove all disks from a storage system, the health status of its LUNs will be **Fault** on DeviceManager. However, the LUN status queried by the host multipathing software may still be normal because the host is not delivering I/Os currently or the conditions for the multipathing software to judge the LUN status to be faulty are not met.

- No LUN alarm appears on the **Current Alarms** tab page.

Precautions

None

Procedure

Step 1 On the navigation bar of DeviceManager, select **Services > LUNs**.

The **LUNs** page is displayed.

Step 2 On the **LUNs** page, view the information about the desired LUN.

Table 4-17 describes associated status parameters.

Table 4-17 LUN status parameters and their meanings

Parameter	Description
Health Status	Health status of a LUN. The value can be: • **Normal**: The functionality and operating performance of the LUN are normal. • **Fault**: The LUN is working improperly. • **Write protect**: LUNs can only be accessed but cannot be written.
Running Status	Running status of a LUN. The value can be **Online** or **Offline**.

----End

Troubleshooting

If a LUN alarm appears on the **Current Alarms** tab page, select the alarm and diagnose the problem according to its details and repair suggestions.

4.2.5.3 Checking Remote Replication CGs

A consistency group centrally manages remote replication tasks so that multiple replication pairs can be synchronized or split in a batch. You can learn about the health and running status of a consistency group by checking its status information.

Impact on the System

- If a consistency group is disabled due to one or more faulty replication pairs, the remote replication services carried by those pairs are interrupted, resulting in data loss.
- If a consistency group is disabled due to a permanently disconnected link between two disk arrays, delete the consistency group.

Prerequisites

A license file is required for enabling the consistency group function.

Reference Standard

If consistency groups are working properly, the following items are true on DeviceManager:

- All of the consistency groups are in the **Normal** health status and **Normal** running status.

- No consistency group alarm appears on the **Current Alarms** tab page.

Precautions

The running status of a consistency group is the same as **Pair Running Status** of the remote replications added to the consistency group. Only remote replications whose **Pair Running Status** is **Split** can be added to a consistency group. When the status of any of the remote replication members contained in a consistency group changes, the status of the remaining members changes accordingly.

Procedure

Step 1 On the navigation bar of DeviceManager, select **Data Protection > Protection Groups**.

The **Protection Groups** page is displayed.

Step 2 On the **Remote Replication CGs** tab, view the information about the desired consistency group.

Table 4-18 describes associated status parameters.

Table 4-18 Consistency group status parameters and their meanings

Parameter	Definition
Health Status	Health status of a consistency group. The value can be: • **Normal**: The functionality and operating performance of the consistency group are normal. • **Faulty**: One or more replication pairs for the consistency group are abnormal. • **About to fail**: The consistency group or the replication link is about to fail. • **Invalid**: The consistency group is useless and cannot be restored. It must be deleted.
Running Status	Running status of a consistency group. The value can be **Normal**, **Synchronizing**, **Split**, **To be recovered**, **Interrupted**, or **Invalid**.

----End

Troubleshooting

If a consistency group alarm appears on the **Current Alarms** tab page, select the alarm and diagnose the problem according to its details and repair suggestions.

4.2.5.4 Checking HyperMetro CGs

Creating a HyperMetro CG assigns multiple HyperMetro pairs to a single consistency group for unified maintenance. You can learn about the health and running status of a consistency group by checking its status information.

Impact on the System

- If a consistency group is disabled due to one or more faulty HyperMetro pairs, the remote replication services carried by those pairs are interrupted, resulting in data loss.
- If a consistency group is disabled due to a permanently disconnected link between two disk arrays, delete the consistency group.

Prerequisites

A license file is required for enabling the consistency group function.

Reference Standard

If consistency groups are working properly, the following items are true on DeviceManager:

- All of the consistency groups are in the **Normal** health status and **Normal** running status.
- No consistency group alarm appears on the **Current Alarms** tab page.

Precautions

The HyperMetro pairs in a consistency group must belong to the same HyperMetro domain and have the same data synchronization direction.

Procedure

Step 1 On the navigation bar of DeviceManager, select **Data Protection > Protection Groups**.

The **Protection Groups** page is displayed.

Step 2 On the **HyperMetro CGs** tab, view the information about the desired consistency group.

Table 4-19 describes associated status parameters.

Table 4-19 Consistency group status parameters and their meanings

Parameter	Definition
Health Status	Health status of a consistency group. The value can be: • **Normal**: The functionality and operating performance of the consistency group are normal. • **Faulty**: One or more replication pairs for the consistency group are abnormal.
Running Status	Running status of a consistency group. The value can be **Normal**, **Synchronizing**, **Invalid**, **Paused**, **Force Start**, or **To be synchronized.**

----End

Troubleshooting

If a consistency group alarm appears on the **Current Alarms** tab page, select the alarm and diagnose the problem according to its details and repair suggestions.

4.3 Collecting Storage System Information

If a fault occurs, you can promptly collect and report basic information, fault information, as well as storage device, network, and application server information to help maintenance engineers quickly locate and rectify faults. Note that you must obtain the customer's consent before collecting the information.

4.3.1 Types of Information to Be Collected

The information to be collected includes the basic information, fault information, storage device information, network information, and application server information.

Types of Information to Be Collected

Collect the types of information specified in **Table 4-20** and send them to maintenance engineers.

Table 4-20 Types of information to be collected

Information Type	Item	Action
Basic information	Device serial number and version	Provide the serial number and version of the storage device. **NOTE** You can log in to DeviceManager and query the serial number and version of the storage device in the **Home** page.
	Customer information	Provide information about the customer's contact person and contact means.
Fault information	Occurrence time	Record the time when a fault occurs.
	Symptom	Record the symptom when a fault occurs, for example, an error dialog box or an event notification.
	Operations performed before a fault occurs	Record the operations performed before a fault occurs.

Information Type	Item	Action
	Operations performed after a fault occurs	Record operations that are performed before reporting the fault to maintenance personnel.
Storage device information	Hardware module configuration	Record the configuration of the hardware modules in the storage device.
	Indicator status	Record the statuses of the storage device indicators, especially the indicators in orange or red. For details about indicator statuses, see the *Product Description*.
	System data	Manually export the configuration information and system logs of the storage device.
	Alarms and logs	Manually export the alarms and logs of the storage device.
Network information	Connection mode	Describe the networking mode between application servers and the storage device, for example, Fibre Channel or iSCSI networking.
	Network topology	Describe the network topology or provide a network diagram.
	IP address information	Describe the IP address allocation rules or provide a list of allocated IP addresses if the iSCSI networking mode is used.
Application server information	Operating system version	Record the types and versions of the operating systems installed on the application servers.
	Port rate	Record the port rates of the application servers connected to the storage device. For details about how to view a port rate, see *Help*.
	Operating system logs	View and export the operating system logs.

4.3.2 Collecting Logs and Alarms Using DeviceManager

You can use DeviceManager to collect the storage system's system data, alarms, and events.

4.3.2.1 Exporting System Data

Periodically export the system data of a storage system and save it in a safe place. This helps you know the operating status of the storage system and take countermeasures against possible system faults and unexpected disasters. If a system failure occurs, the exported system data can be used to locate and analyze the failure. The system data to be exported includes configuration information, system logs, disk logs, diagnostic files, and antivirus log.

Context

- System logs record the information about the configuration information, events, and debugging operations on a storage system and can be used for analyzing the running status of the storage system. The system log file is in *.tgz format.
- Configuration information indicates the real-time running status of a storage system and includes user information and LUN configuration information. The configuration information file is in *.txt format.
- DHA runtime logs are disks' daily running logs, including daily disk health statistics, I/O statistics, and disk service life. The DHA runtime log file is in *.tgz format.
  - DHA runtime logs collect S.M.A.R.T/LogPage information (collected at 2 o'clock every morning), I/O statistics (collected every 2 hours), and disk service life (collected at 2 o'clock every morning). A log package (1 KB) is generated for each disk each day. A controller can generate a maximum of 74 log packages for each of the disks belonging to it within a year (some old log packages will be deleted during the collection). In a log package export, packages corresponding to each controller are generated. Each package contains log packages and one basic information file about each disk belonging to the corresponding controller.

    NOTE

    You can run the **change dha policy collect_start_time=***?* command in developer mode in the CLI to change the start time for collecting DHA runtime logs.
  - The analysis of DHA runtime logs is only performed on samples instead of all logs. The recommended maximum times of export during routine maintenance are listed in the following table.

Disk Quantity in a Storage System	Recommended Maximum Times of Export During an Inspection
0 to 200	3
200 to 500	4
500 to 1000	5
1000 to 2000	6
>2000	6

- HSSD logs are HSSDs' working logs, including the S.M.A.R.T information and disk running logs. The HSSD log file is in *.tgz format.

In the event of downloading system logs, DHA runtime logs, or HSSD logs, the system first collects those logs of controllers and displays the collection progress about each controller. After all logs are collected, you can download your desired logs.

NOTICE

After the system starts collecting system logs, DHA run logs, or HSSD logs, you need to wait for five minutes or download all the collected logs before you collect and download other logs.

- The disk data erasure reports collect the information about the disk on which data erasure is performed, erasure mode, execution time, and verification result. The disk data erasure reports are in *.csv format.
- Diagnostic files collect the device faults. The diagnostic files are in *.tgz format.
- Antivirus logs contain information about files that fail to be scanned by the antivirus service, including file names, error codes, file systems, and tenants. The exported log files are in .tgz format.
- FTDS logs record device latency statistics. The exported FTDS log files are in *.tgz format. (FTDS logs can be exported in 6.1.5 and later versions.)
- Performance files are mainly historical performance files of the device. To export performance files, you must retain historical monitoring data (you can enable this function by choosing **Settings** > **Monitoring Settings** on DeviceManager. The exported performance files are in *.zip format. (Performance files can be exported in 6.1.5 and later versions.)

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose  > **Export Data**.

Step 3 **Optional:** Encrypt data.

NOTE

Encrypts exported logs and configurations. Decryption is required to decompress them. For details about how to decrypt the encrypted logs, see **Follow-up Procedure**.

1. Select **Enable** for **Data Encryption**.
2. Set **Encryption Password** and **Confirm Password**.

NOTE

- A password contains 8 to 16 characters.
- A password must contain special characters. Special characters include !"#$%&'()*+,-./:;<=>?@[\]^`{_|}~ and spaces.
- A password must contain any two types of uppercase letters, lowercase letters, and digits.

Step 4 Export data.

- Select **System Log** area, and click **Recent Log**, **All Logs** or **Key Log**. Confirm the information in the security alert dialog box, select **I have read and understand the consequences associated with performing this operation**, and click **OK**.

  The system starts collecting logs.

  NOTE

  Besides the configuration, event, and debug log information on the device, the system also collects the device's upgrade database file. The file is used for locating upgrade-related problems and does not contain any personal privacy data.

- Select **Disk Log** and click **DHA Runtime Log**, **HSSD Log**, or **Disk Data Erasure Report**. In the warning dialog box that is displayed, select **I have read and understand the consequences associated with performing this operation** and click **OK**.

  The system starts collecting logs and expands the log list.

- In the **Configuration Info** area, click **Export**. Confirm the information in the security alert dialog box, select **I have read and understand the consequences associated with performing this operation**, and click **OK**.

  The configuration information is exported.

- In the **Diagnostic File** area, click **Export**. Confirm the information in the security alert dialog box, select **I have read and understand the consequences associated with performing this operation**, and click **OK**.

  The fault information of the device is exported.

- In the **Antivirus Log** area, click **Export**. Confirm the information in the security alert dialog box, select **I have read and understand the consequences associated with performing this operation**, and click **OK**.

  The antivirus scanning information of the device is exported.

- In the **FTDS Log** area, click **Export**. Confirm the information in the security alert dialog box, select **I have read and understand the consequences associated with performing this operation**, and click **OK**.

  The FTDS log of the device is exported.

- In the **Performance File** area, specify **File Date Range** and click **Export**. Confirm the information in the security alert dialog box, select **I have read and understand the consequences associated with performing this operation**, and click **OK**.

  The performance file of the device is exported.

NOTE

- For **System Log**, if you select **Recent Log**, the system exports the latest logs, including the latest power-on and power-off log and up to six historical message logs. Note that historical messages logs are saved to the **/OSM/coffer_log/log/his_debug** directory. If **All logs** is selected, the system exports all logs on the current node. If **Key Log** is selected, key logs are stored in the **/OSM/coffer_log/log/his_debug/private** directory. The logs include all logs printed by system modules using the key log framework.
- If you export data using the Internet Explorer browser with the default settings, the data will be saved in the download path selected by the user. Take Internet Explorer 11 as an example. You can select **Save As** in the displayed file download dialog box to specify the path for saving the data.
- If you export data using the Firefox browser with the default settings, the data will be saved in the default download path of the browser. You can choose **Tools** > **Options** to open the **Options** dialog box and then choose **General** > **Browser** in the **Options** dialog box to view the default download path.
- If you export data using the Google Chrome browser with the default settings, the data will be saved in the default download path of the browser. You can choose **Settings**. On the **Settings** page that is displayed, choose **Advanced** > **Downloads** to view the default download path.
- When using Chrome to export data for the first time, click **Allow** if the message "This site is attempting to download multiple files. Do you want to allow this message?" is displayed. Otherwise, in the upper right corner of Google Chrome, select **Customize and control Google Chrome** > **Settings** > **Privacy and security** > **Site Settings** > **Automatic downloads**. In the **Block** area, select the desired website and click **Allow**. Then, reopen the current page. Alternatively, you can delete the desired website in the **Block** area. After setting, reopen the page and the message "This website wants to download multiple files. Are you sure you want to continue?" is displayed. Click **Allow** to download multiple files.

----End

Follow-up Procedure

Decrypt the encrypted logs as follows:

Perform the following operations in a Linux system that supports OpenSSL 1.1.1f or later:

Method 1:

Run the **sudo openssl enc -aes-256-ctr -d -k** *Encryption password* **-in** *Name of the file to be decrypted* **-out** *Name of the file after being decrypted* command.

Example: **sudo openssl enc -aes-256-ctr -d -k ABCDEFG@123 -in /test/Encrypt.tgz -out /test/Decrypt.tgz**

Method 2:

1. Run the **sudo openssl enc -aes-256-ctr -d -in** *Name of the file to be decrypted* **-out** *Name of the file after being decrypted* **-pass stdin** command.
2. Enter the encryption password.

4.3.2.2 Exporting Alarms and Events

Alarms and events record the faults and events that occurred during storage system operation. If the storage device is faulty, view the alarms and events to locate and rectify the fault.

Context

Specify the alarms to be exported by setting the alarm severity or time of occurrence.

This document uses Internet Explorer on a Windows server as an example. If you are using other web browsers, adjust the operations accordingly.

Precautions

Alarms and system events are saved in ***.xls** files. After they are exported, do not modify the file content.

Procedure

Step 1 Choose **Insight > Alarm and Events**.

The **Alarms and Events** page is displayed.

Step 2 Export alarms and events.

1. Click the **Current Alarms** or **All Events** tab. In the list, choose alarms and events that you want to export.

   NOTE

   - On the **Current Alarms** tab page, critical alarms, major alarms, and warnings are displayed.
   - You can export all or specified entries on the **Current Alarms** tab page.
   - The **All Events** tab page includes critical, major, warning, and info events. Alarms on the **Current Alarms** tab page are also included in **All Events**.
   - You can export all or specified entries on the **All Events** tab page.
   - To export alarms or events of a specific severity, set the filter condition before exporting them.

2. Click  .

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

----End

4.3.3 Collecting Storage System Configuration Data Using the CLI

You can use the CLI to back up or import device configuration data.

4.3.3.1 Exporting Storage System Configuration Data

All configuration information of a storage system must be exported before a system upgrade or capacity expansion. Exported data can be used to restore the storage system if the upgrade or capacity expansion fails.

Prerequisites

- The FTP or SFTP server is accessible to the storage system. Log in to the server, and run **ping ip**. If the server receives data packets from the front-end

port, the communication between the storage system and server is normal. If the communication is abnormal, you can replace cables, change the IP addresses of the server ports, or add routes. For details about how to change the IP address of a server port and add a route, see the DeviceManager online help.

- The FTP or SFTP service on the server has been enabled.
- A folder has been created for saving configuration files.

Context

Configuration data of the storage system can be collected only using the CLI.

Precautions

- Configuration data of the storage system is exported in a **.dat** file. Do not modify any content in this file.
- If the storage system serves as a server in the file transfer with external systems, it supports the SFTP service only. If the storage system serves as a client, it supports both the FTP and SFTP services.
- If the system is abnormal and configuration files must be imported, contact technical support engineers.

Procedure

Step 1 Log in to the CLI of the storage system as a super administrator.

Step 2 Run the **export configuration_data ip=***?* **user=***?* **password=***?* **db_file=***?* [**port=***?*] [**protocol=***?*] [**clean_device_file=***?*] command to export configuration files to an FTP or SFTP server.

Table 4-21 Parameter description

Parameter	Description	Value
ip=*?*	IP address of an FTP or SFTP server to which you want to import a configuration file.	-
user=*?*	User name for logging in to an FTP or SFTP server.	The value contains 1 to 64 characters.
password=*?*	Password for logging in to an FTP or SFTP server.	The value contains 1 to 63 characters.
db_file=*?*	File name of and path to a configuration file on an FTP or SFTP server.	The file name extension must be **.dat**. If you specify a file name, the file name cannot contain any of the following characters: \ / : * ? " < > |.

Parameter	Description	Value
port=*?*	ID of the port used on an FTP or SFTP server.	The value ranges from 1 to 65535. • If **protocol=FTP**, the default value is 21. • If **protocol=SFTP**, the default value is 22.
protocol=*?*	Protocol type.	The value can be **FTP** or **SFTP**. The default value is **SFTP**. To ensure the security of data transfer, you are advised to use SFTP.
clean_device_file=*?*	After the configuration file is exported to an FTP server or an SFTP server, whether to delete the temporary configuration file cached in the storage system memory during configuration file export.	The value can be **yes** or **no**, where: • **yes**: immediately deletes the temporary configuration file cached in the storage system memory. • **no**: deletes the temporary configuration file cached in the storage system memory after five minutes. The default value is **yes**.
forcible_export=*?*	Whether an export is forcibly performed.	The value can be **yes** or **no**, where: • If **forcible_export=yes**, the configuration data is forcibly exported without checking whether there are ongoing configuration tasks on the system. Configuration files forcibly exported cannot be imported to the storage system for restoring configuration. • If **forcible_export=no**, whether there is any ongoing configuration task on the system is checked before the export. If any, the export is prohibited.

----End

4.3.3.2 Importing Storage System Configuration Data

If a system fails to be upgraded or malfunctions, you can import backed up system configuration data to restore system configurations.

Prerequisites

- Storage systems can access a File Transfer Protocol (FTP) server over the network.
- The FTP service has been enabled on the FTP server.
- The selected system configuration file is a correct backup.

Context

Storage system configuration information can be imported only using the CLI.

Precautions

- The type of a configuration file to be imported is ***.dat**. Do not modify exported configuration file contents.
- Do not perform any operation when importing a configuration file.

Procedure

Step 1 Log in to the CLI as the super administrator.

Step 2 Run the **import configuration_data ip=***xxx.xxx.xxx* **user=***?* **password=***?* **db_file=***?* command to import a configuration file from the FTP server to the storage system.

NOTE

For details about this command, see the *Advanced O&M Command Reference*.

----End

4.3.4 Collecting Information Using SmartKit

You can use SmartKit to collect system data, archive information, and host information.

4.3.4.1 Exporting System Data

After installing the SmartKit information collection tool on a storage system, you can use the tool to customize information collection policies and collect information about the storage system in real time.

Prerequisites

The SmartKit information collection tool has been installed on the maintenance terminal.

Context

After starting SmartKit, you can obtain tool use instructions by clicking  in the upper right corner of the user interface.

Procedure

Step 1 Start SmartKit.

The **SmartKit** page is displayed.

Step 2 Add a device.

1. Click **Devices** and then **Add**.

   The **Add device step 2-1: Basic Information** dialog box is displayed.

2. Enter basic information, including the IP address and proxy. In the **Add Policy** and **Select Proxy** areas, select **Specify IP Address (add a device by the IP address)** and **No Proxy**, respectively.

3. Enter configurations, including the user name, password, and port of the device. Click **Next**. In the **Login Information** area, enter **Username**, **Password**, and **Port** of the device to be added. The default value of **Port** is **22**.

4. Click **Finish**.

   The newly added device is displayed in the device list.

Step 3 Collect information.

1. On the main page, choose **Troubleshooting** > **Storage Information Collection** > **Information Collection**.

   The **Information Collection** dialog box is displayed.

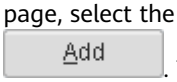
2. In the device list, select the device whose information you want to collect and click **Setting**.

   The **Set Device Information Collection** dialog box is displayed.

3. On the **Base Setup** tab page, set items to be collected for the device and click **OK**.

   The device information collection setting is complete.

   NOTE

   - The storage system can collect information such as system logs, FTDS logs (used for tracking the I/O process, collecting I/O counts and latency, and collecting performance statistics), diagnostic information, alarm information, config info, electronic label, disk logs, and CLI command info.
   - SmartKit can collect device information by node. On the **Advanced Settings** tab page, select the node whose information you want to collect and click  . The selected node is displayed in the list on the right.

4. In the **Information Collection** dialog box, click **Collect**.

   Information about the selected node starts to be collected. The information collection status is displayed at the bottom of the page.

Step 4 Check the information collection result.

Click **Open Directory** to check collected device information.

----End

4.3.4.2 Exporting Historical Performance Data

After the SmartKit historical performance monitoring tool is installed on a storage system, you can use the tool to collect historical performance data of the storage system to keep abreast of device information in real time.

Prerequisites

The SmartKit historical performance monitoring tool has been installed on the maintenance terminal.

Context

After starting SmartKit, you can obtain tool use instructions by clicking in the upper right corner of the user interface.

Procedure

Step 1 Start SmartKit.

The **SmartKit** page is displayed.

Step 2 Add a device.

1. Click **Devices** and then **Add**.
   The **Add device step 2-1: Basic Information** dialog box is displayed.

2. Enter basic information, including the IP address and proxy. In the **Add Policy** and **Select Proxy** areas, select **Specify IP Address (add a device by the IP address)** and **No Proxy**, respectively.
3. Enter configurations, including the user name, password, and port of the device. Click **Next**. In the **Login Information** area, enter **Username**, **Password**, and **Port** of the device to be added. The default value of **Port** is **22**.
4. Click **Finish**.

   The newly added device is displayed in the device list.

Step 3 Export historical performance data.

1. Choose **Troubleshooting** > **Historical Performance Monitoring** > **Device Selection** from the main menu.

   The **Select Devices** dialog box is displayed

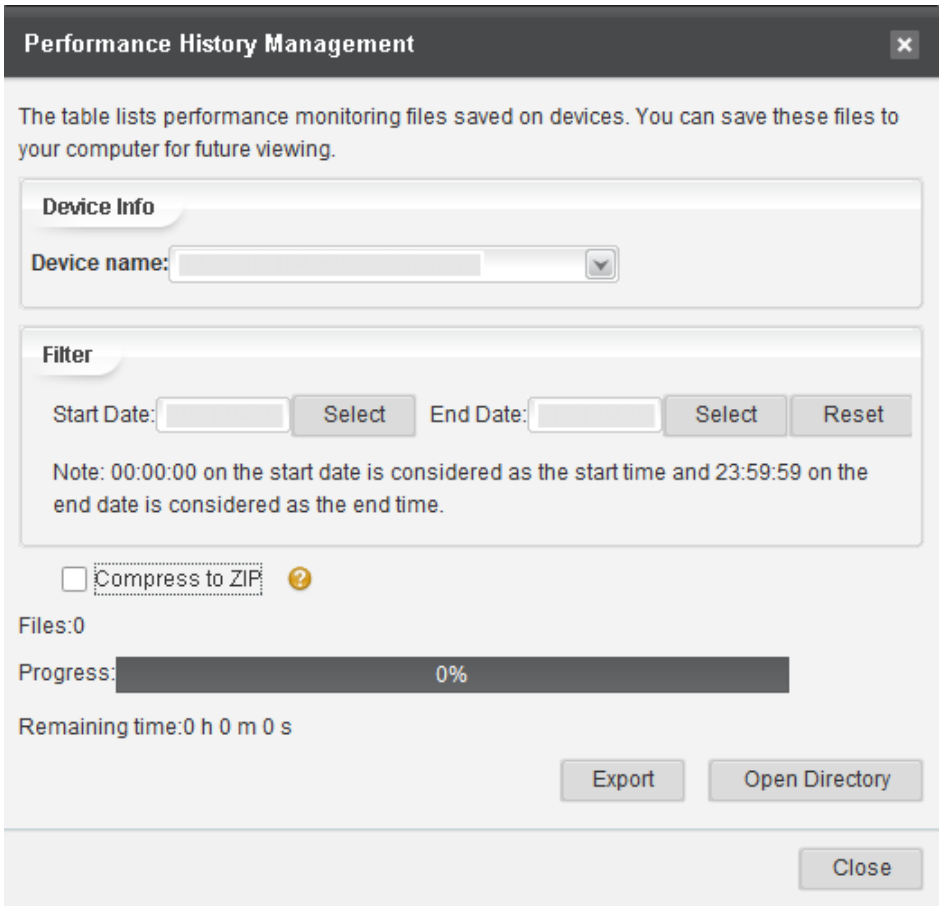
   a. Select a device.
   b. (Optional) In **Result Folder**, select a path for exporting the historical performance data of the storage device.
   c. Click **OK**.
2. Click **Historical Performance Monitoring**.

   The **Historical Performance Monitoring** dialog box is displayed.

   a. Click **Export**.

      The **Select Export File Type** dialog box is displayed.
   b. Select **HisPerfstat** from the drop-down list box.
   c. Click **OK**.

      The **Performance History Management** dialog box is displayed.



d. In the **Filter** area, select the time period for exporting historical performance data.

   - Click **Select** next to **Start Date** to select the start time for exporting historical performance data.
   - Click **Select** next to **End Date** to select the end time for exporting historical performance data.

e. (Optional) Select **Compress to ZIP**.

   If this parameter is selected, you can view the historical performance of the device after the generated compressed package is imported to eService.

f. Click **Export**.

   The tool starts exporting historical performance data.

g. When the message **Collect information succeeded.** is displayed next to **Progress**, the historical performance data collection is complete.

h. (Optional) Click **Open Directory** to view the exported data.

i. Click **Close**.

   NOTE

   After collecting historical performance data, contact Huawei technical support engineers for fault locating and analysis.

Step 4 (Optional) Combine multiple historical performance data files into one file.

Click **Combine** and then you can perform operations as prompted.

Step 5 (Optional) Use SmartKit to view historical performance data.

Click **Add to List** and perform operations as prompted.

----End

4.3.4.3 Collecting Device Archive Information

After installing the SmartKit archive information collection tool on a storage system, you can use the tool to collect the configuration and deployment information about the storage system and generate archives.

Prerequisites

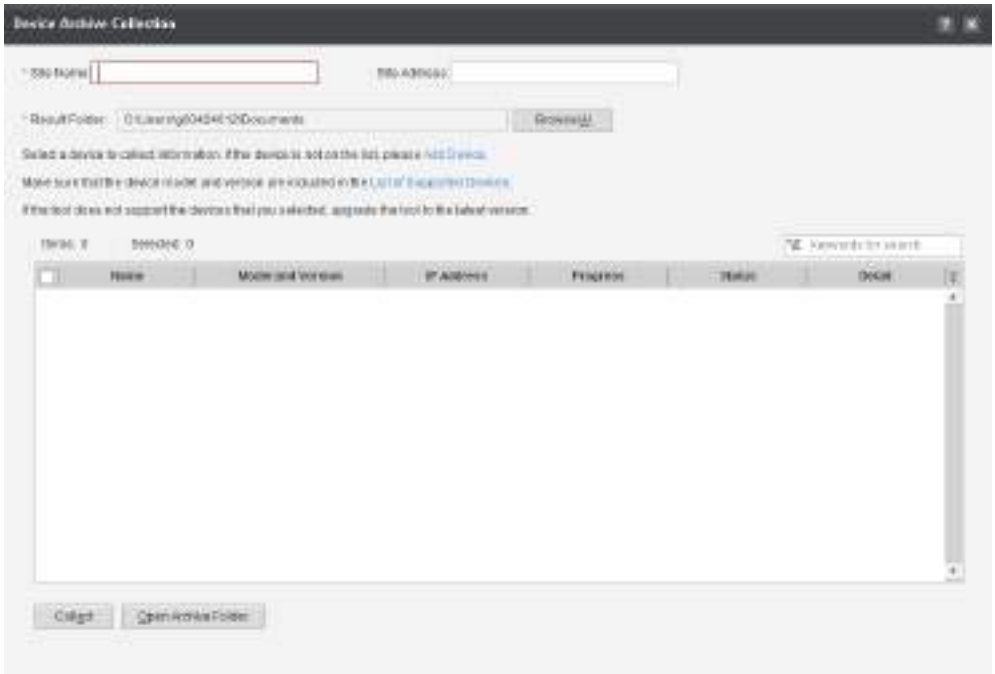
SmartKit has been installed on the maintenance terminal and an archive information collection tool has been loaded.

Procedure

Step 1 Start SmartKit.

Step 2 Choose **Troubleshooting** > **More** > **Device Archive Collection**.

The device archive information collection page is displayed.



Step 3 For details about how to collect device archive information, click ? in the upper right corner for help.

----End

4.3.4.4 Collecting Host Information

When a host information collection tool is installed on a storage system, the tool can be used for one-click information collection of hosts and database systems.

Prerequisites

- SmartKit has been installed on the maintenance terminal and a host information collection tool has been loaded.
- To add devices, the super administrator account is required for connections.

Procedure

Step 1 Start SmartKit.

Step 2 Choose **Troubleshooting** > **More** > **Host Information Collection**.

The host information collection page is displayed.

Step 3 For details about host information collection operations, click **Help** in the upper-right corner to obtain help.

----End

5 Routine Management

This chapter describes the routine management items for the storage system.

5.1 Powering on or off the Storage System

Powering on or off a storage system includes powering on or off interface modules and other hardware components. A correct procedure effectively avoids device damage caused by misoperations.

5.1.1 Powering on the Storage System (by Pressing the Power Button)

You can press the power button on the controller enclosure to power on the storage system.

5.1.1.1 OceanStor 5310, OceanStor 5510, OceanStor 5610, and OceanStor 6810

After all devices are installed, power on them and check that they are working correctly.

Prerequisites

Ensure that all devices are properly installed and device installation check is completed. Otherwise, power on them after these devices and hardware are correctly installed.

Context

NOTICE

- Before powering on a storage system, ensure that all expansion cables have been properly connected. If expansion cable connections are adjusted after a storage system is powered on, the storage system may malfunction.
- During the power-on, do not remove or insert optical fibers, network cables, coffer disks, or interface modules to avoid system data loss.
- When powering on a storage system, do not wear an ESD wrist strap to avoid electric shock.

NOTE

The correct power-on sequence is as follows:

1. Turn on the external power switches corresponding to all the devices.
2. Press the power button on each controller enclosure.
3. Power on switches (if any switch is deployed but not powered on).
4. Power on application servers.

Procedure

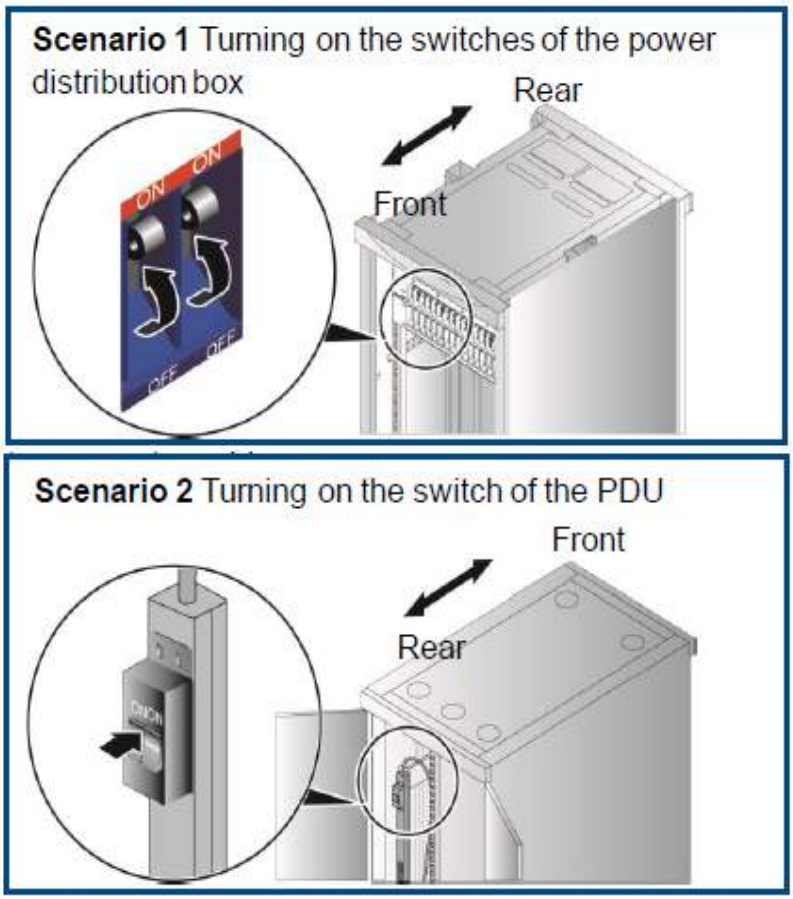
Step 1 Connect the external power supply (PDB or PDU), as shown in **Figure 5-1**.

1. In scenarios where PDB is used, check labels on power cables and match power cables with power switches in the cabinet PDB.

   For example, if the label on the AC power cable connected to a controller enclosure displays **PowerBox Output B_8**, it indicates that the power cable of the controller enclosure corresponds to power switch SW8 on module Output B. You can turn on that power switch to power on the controller enclosure.

2. Connect devices in the cabinet with external power supplies in the following sequence: disk enclosure, controller enclosure, switch (in the SAN network), and application server.

Figure 5-1 Connecting external power supplies



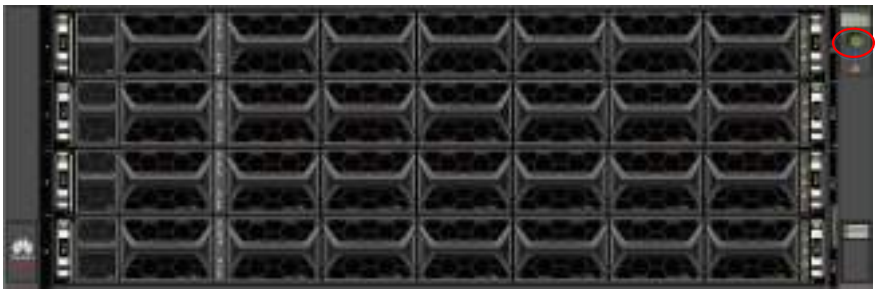
Step 2 Press the power button on each controller enclosure.

NOTE

- You only need to press the power button once. If the power indicator of the controller enclosure is blinking green, the storage system is being started. Do not hold down the power button. If the power button is held for 5 seconds, the system is powered off.
- The power-on process takes 15 to 30 minutes.
- After the controller enclosure is powered on, other disk enclosures connected will be automatically powered on.
- After system power-on, the disk initialization process automatically starts. The time required for the process is dependent on the quantity of the disks to be initialized.

Figure 5-2 Power button on 2 U controller enclosure

Figure 5-3 Power button on 4 U controller enclosure



----End

Follow-up Procedure

After the storage device has been powered on, verify that the indicator of each hardware component is in a normal state by referring to the *Product Description*. If you find an anomaly for any indicator, try to rectify it by referring to the *Event Reference* or *Troubleshooting*.

5.1.1.2 OceanStor 18510 and OceanStor 18810

Before powering on the storage system, complete the installation check to ensure that all devices are correctly installed and all cables are correctly connected. After powering on the storage system by following the correct power-on sequence, observe indicators on bays to check that the storage system is powered on successfully.

Power-On Sequence

Regarding the system power-on sequence, two basic rules must be followed:

- If the system includes disk bays, they must be powered on before the system bays are powered on.
- System bays must be powered on in an ascending sequence from system bay 0 to system bay *n*. Disk bays can be powered on in any sequence.

NOTICE

Devices must be grounded before the storage system is powered on. Otherwise, devices may be damaged.

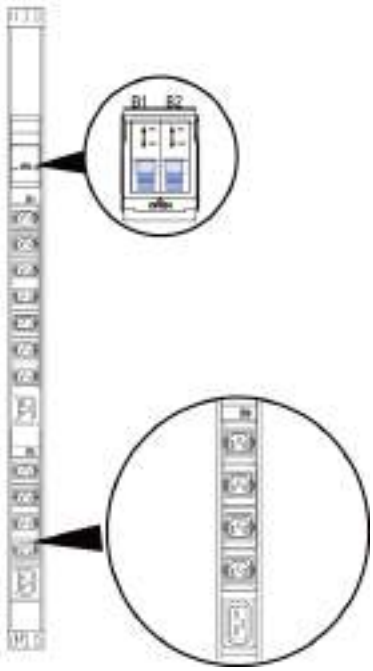
The overall system power is controlled by power switches on power distribution units (PDUs). Each bay is equipped with PDUs that reside at the left and right sides in the rear of the bay. Follow the correct power-on sequence according to the type of PDUs configured.

Power-On Sequence for Systems Configured with European Standard PDUs

For a system configured with European standard PDUs, the correct power-on sequence is as follows:

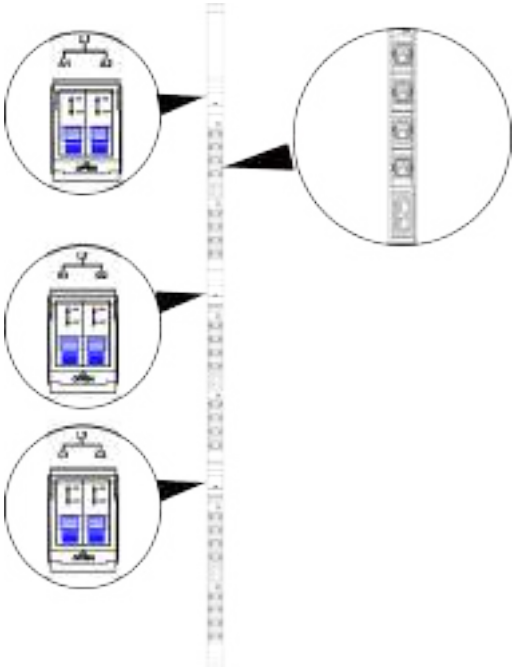
1. Turn on PDU switches of the system bays from system bay 0 to system bay *n* in sequence.
   - For European standard PDU switches (single-phase, 220 V, 32 A), turn on the switches in a sequence of **B1** > **B2**.

     Figure 5-4 PDU that meets the Single-phase AC

   - For European standard PDU switches (three-phase, 380 V, 32 A), turn on the switches in a sequence of **A1** > **A2** > **B1** > **B2** > **C1** > **C2**.

     Figure 5-5 PDU that meets the three-phase AC

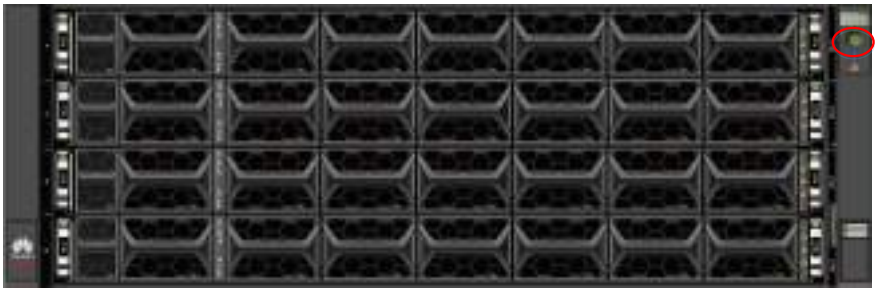
2. Press the power buttons of all controller enclosures, as shown in **Figure 5-6**.

NOTE

In a scenario with multiple controllers, all the controller enclosures must be powered on within three minutes. If the controller enclosures fail to power on within the specified period, the storage system fails to power on. In this case, contact Huawei technical support engineers.

To power on the storage system, press the power button. If the power indicator of the controller enclosure is blinking green, the storage system is being powered on. Do not hold down the power button for more than five seconds; otherwise, the storage system will be powered off.

Figure 5-6 Power button on a controller enclosure



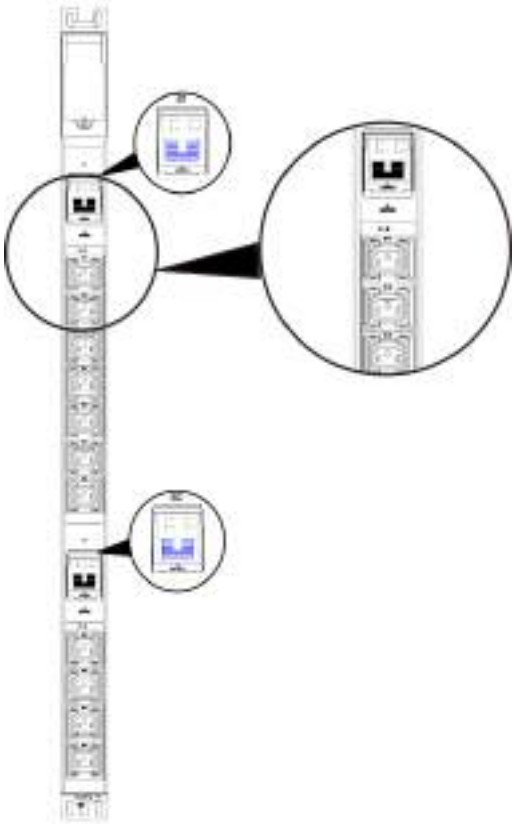
Power-On Sequence for Systems Configured with High Voltage DC PDUs

For a system configured with high voltage DC PDUs, the correct power-on sequence is as follows:

1. Turn on PDU switches of the system bays from system bay 0 to system bay *n* in sequence.

   For HVDC PDU switches, turn on the switches in a sequence of **B1** > **B2**.

Figure 5-7 PDU that meets the high voltage DC



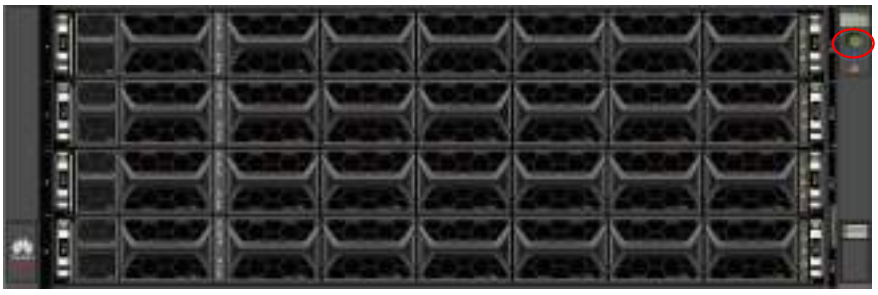
2. Press the power buttons of all controller enclosures, as shown in **Figure 5-8**.

NOTE

In a scenario with multiple controllers, all the controller enclosures must be powered on within three minutes. If the controller enclosures fail to power on within the specified period, the storage system fails to power on. In this case, contact Huawei technical support engineers.

To power on the storage system, press the power button. If the power indicator of the controller enclosure is blinking green, the storage system is being powered on. Do not hold down the power button for more than five seconds; otherwise, the storage system will be powered off.

Figure 5-8 Power button on a controller enclosure



5.1.2 Powering on the Storage System (Remotely on the CLI)

If power cables are connected, the storage system can be remotely powered on by running the power-on command.

5.1.2.1 Application Scenarios

The OceanStor storage system can be remotely powered on by running the power-on command on the CLI.

Scenario 1: None of the Controller Enclosures in the Cluster Are Powered On

If none of the controller enclosures in the cluster are powered on, you can use the BMC system's external management IP address to log in to the BMC system and run the power-on command to power on all controller enclosures in the cluster. The implementation process is as follows:

1. Use the IP address of the management network port to log in to the BMC system.

   NOTE

   The way to log in to the BMC system is the same as the way to log in to the CLI of the storage system through the management network port. If the storage system is not powered on, you will be directly logged in to the BMC system after making an attempt to log in to the CLI of the storage system through the management network port.

2. Run the power-on command to power on all controller enclosures in the cluster.

Scenario 2: Some Controller Enclosures in the Cluster Are Not Powered On

If some controller enclosures in the cluster are not powered on, you can log in to the storage system using the IP address of the management network port and run the power-on command to power on the controller enclosures that are not powered on in the cluster. The implementation process is as follows:

1. Use the IP address of the management network port to log in to the CLI of the storage system.
2. Run the power-on command to power on the controller enclosure that is not powered on in the cluster.

5.1.2.2 Networking Rules and Networking Diagrams

This section describes the networking rules and networking diagrams for powering on a storage system remotely.

Networking Rules

- If a storage system has only one controller enclosure, ensure that:
  - The power cables of the controller enclosure are correctly connected.
  - The maintenance terminal is connected to any management network port on the controller enclosure.
- If a storage system has multiple controller enclosures, ensure that:

- The power cables of all controller enclosures are correctly connected.
- The maintenance terminal is connected to any management network port on any controller enclosure.
- The scale-out cables of all controller enclosures are correctly connected. The maintenance network ports on all controller enclosures are correctly connected according to the standard networking mode.

Networking Diagrams

The cable connections of a single controller enclosure are simple. This section only describes the networking mode in the multi-controller-enclosure scenario.

In the following figures, purple cables are management network cables, and orange and blue cables are scale-out cables. To use the remote power-on function, connect network cables (green cables in the following figures) to maintenance ports on controller enclosures.

NOTE

If green cables are not connected, after the power-on command is executed, only the controller enclosure where the currently logged-in controller resides can be powered on. Other controller enclosures cannot be powered on.

Figure 5-9 OceanStor 5310 four-controller networking diagram

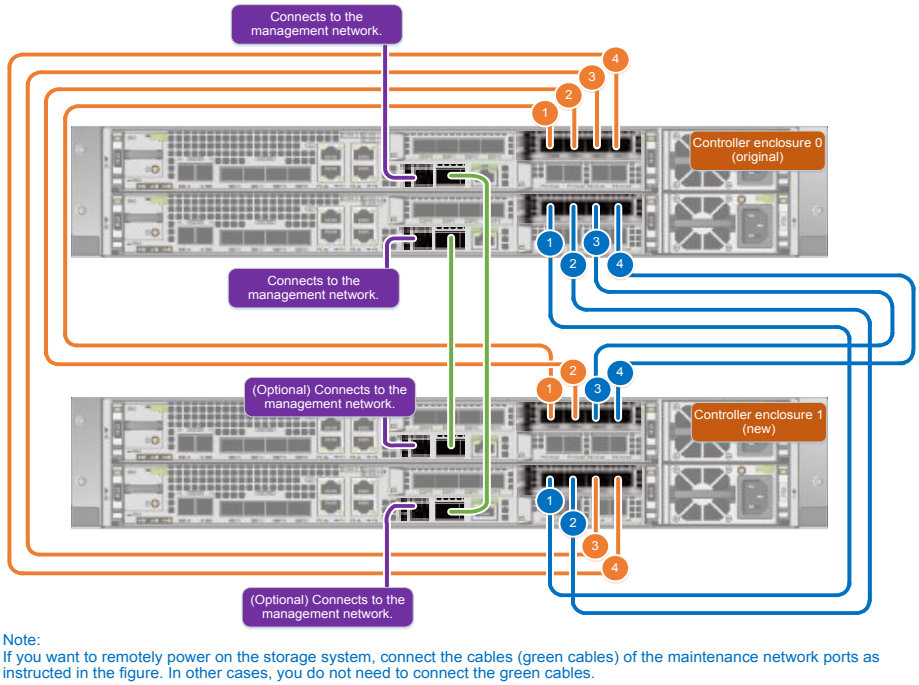
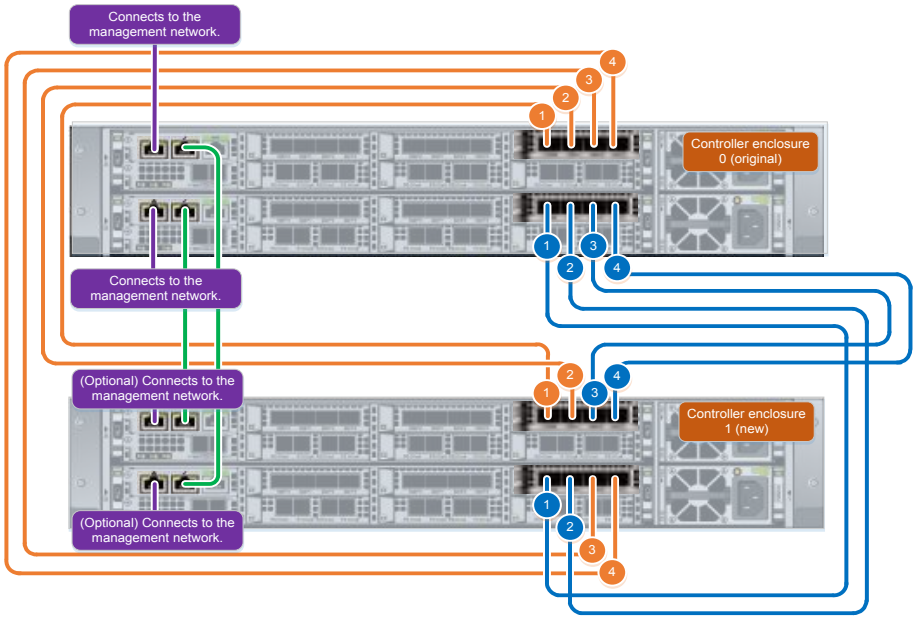
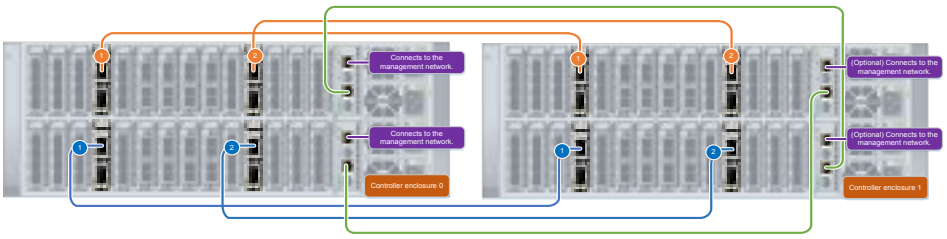


Figure 5-10 OceanStor 5510 and OceanStor 5610 four-controller networking diagram



Note:
If you want to remotely power on the storage system, connect the cables (green cables) of the maintenance network ports as instructed in the figure. In other cases, you do not need to connect the green cables.

Figure 5-11 OceanStor 6810, OceanStor 18510, and OceanStor 18810 eight-controller networking diagram



Note:
If you want to remotely power on the storage system, connect the cables (green cables in the following figure) of the maintenance network ports as instructed in the following figure. Otherwise, you do not need to connect the green cables.

5.1.2.3 Powering on the Storage System (When None of the Controller Enclosures in the Cluster Are Powered On)

This section describes how to remotely power on the storage system when none of the controller enclosures in the cluster are powered on.

Prerequisites

- Cables have been connected according to the standard networking mode.
- The power cables of all controller enclosures in the cluster have been connected.
- None of the controller enclosures in the cluster are powered on.
- This operation should not apply if some controllers in a controller enclosure are not powered on.

- If the password of the storage system super administrator **admin** is not initialized, the BMC administrator cannot access the BMC system through the serial port and cannot use the remote power-on function.

Procedure

Step 1 Log in to the BMC system using the management IP address as the BMC administrator.

NOTE

- This step is the same as the way to log in to the CLI through the IP address of the management network port. If the storage system is not powered on, you will be directly logged in to the BMC system after making an attempt to log in to the CLI of the storage system through the management network port.
- The user name and password of the BMC administrator are the same as those of the super administrator **admin** of the storage system.
- Assume that you remotely log in to the BMC system of the storage system to be powered on from a Linux host or another storage system via SSH. If the system displays a message indicating that the login fails due to the invalid ESDSA host key, see **6.4 How Do I Update the Public Key When a Linux Host Fails to Remotely Log In to the Storage System's BMC System via SSH Due to the Invalid Public Key?**

```
$ ssh admin@XXX.XXX.XXX.XXX
The authenticity of host 'XXX.XXX.XXX.XXX (XXX.XXX.XXX.XXX)' can't be established.
ECDSA key fingerprint is SHA256:RV2Qwdr0wL2XXXXXXXXXXXXXXXXXXXX.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'XXX.XXX.XXX.XXX' (ECDSA) to the list of known hosts.

Authorized users only. All activities may be monitored and reported.
admin@xx.xx.xx.xx's password:
```

Step 2 Run the **cliset -d clusterpoweron 1** command to power on the storage system.

```
iBMC:/->cliset -d clusterpoweron 1
Cluster power on OK.
```

----End

5.1.2.4 Powering on the Storage System (When Some Controller Enclosures in the Cluster Are Not Powered On)

This section describes how to remotely power on the storage system when some controller enclosures in the cluster are not powered on.

Prerequisites

- Cables have been connected according to the standard networking mode.
- The power cables of all controller enclosures in the cluster have been connected.
- Some controller enclosures in the cluster are not powered on.
- In the single-controller-enclosure scenario, if a controller in the controller enclosure is powered off, remote power-on cannot be performed.

Procedure

Step 1 Log in to the CLI of the storage system using the management IP address of any controller enclosure that has been powered on in the cluster.

NOTE

You cannot log in to the storage system using an IPv6 address to run a command to remotely power on the storage system.

Step 2 Run the **change user_mode current_mode user_mode=developer** command to enter the developer mode and then the **minisystem** command to enter the minisystem.

Step 3 Run the **eam.sh poweroncluster** command to power on the rest controller enclosures in the cluster.

```
Storage: minisystem>eam.sh poweroncluster
admin:/diagnose>eam poweroncluster
Power on the cluster successfully.
```

----End

5.1.3 Powering off the Storage System

Respect the correct power-off sequence when you power off the storage device especially for replacing cabinet subracks or removing power link failures.

5.1.3.1 OceanStor 5310, OceanStor 5510, OceanStor 5610, and OceanStor 6810

Respect the correct power-off sequence when you power off the storage device especially for replacing cabinet subracks or removing power link failures.

Prerequisites

No service is running on the storage device.

Context

- Typically, a storage system is powered off in the following sequence: Stop host services, power off the controller enclosure, and then disconnect the external power supply.
- The controller enclosure can be powered off in either of the following ways: Press and hold down the power button on the controller enclosure for 5 seconds, or power off the controller enclosure on its DeviceManager.
- This document describes how to power off the controller enclosure on its DeviceManager.

Procedure

Step 1 Log in to DeviceManager of the controller enclosure.

Step 2 Choose  > **Power Off Device**.

Step 3 Confirm the information in the displayed **Danger** dialog box, enter the password of the currently logged-in user, and then select **I have read and understand the consequences associated with performing this operation**.

NOTICE

If you enter the wrong password more than three times within 5 minutes, the current user will be logged out and exit DeviceManager.

Step 4 Click **OK**.

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

Step 5 Click **OK**. You have powered off the storage device.

----End

5.1.3.2 OceanStor 18510 and OceanStor 18810

Respect the correct power-off sequence when you power off the storage device especially for replacing cabinet subracks or removing power link failures.

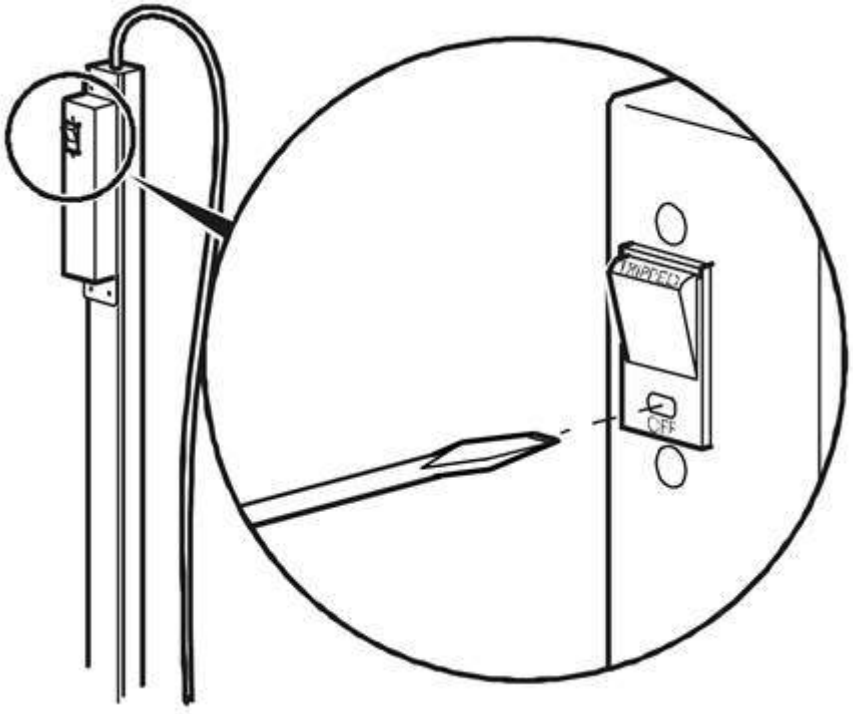
Prerequisites

No service is running on the storage system.

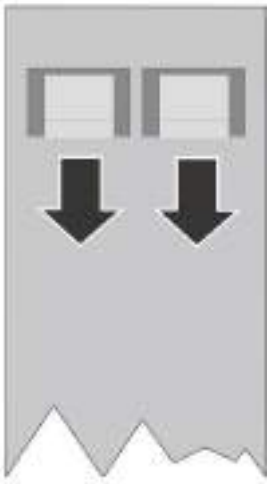
Context

- Typically, a storage system is powered off in the following sequence: Stop host services, power off the controller enclosure, and then disconnect the external power supply.
- The operation of turning off PDU switches varies based on types of PDUs configured.
  - North American standard PDUs:

    Insert a flat-head screwdriver or a clip into the hole located above the word **OFF** on the switch, and push forward gently until the upper part of the switch pops up.



– European standard PDUs and high voltage direct current (HVDC) PDUs: Turn the switch downward.



Procedure

Step 1 Power off the storage device.

NOTE

You can power off the storage system by holding down the engine power button for five seconds or performing power-off operations on DeviceManager. This section uses the operations on DeviceManager as an example.

1. Log in to DeviceManager.
2. Choose > **Power Off Device**.
3. Confirm the information in the displayed **Danger** dialog box, enter the password of the currently logged-in user, and then select **I have read and understand the consequences associated with performing this operation**.

NOTICE

If you enter the wrong password three times in succession within 5 minutes, the current user will be logged out and exit DeviceManager.

4. Click **OK**.

   The **Success** dialog box is displayed, indicating that the operation is successful.
5. Click **OK**. You have powered off the storage device.

Step 2 Turn off the PDU switches in every bay in the right sequence.

NOTE

The sequence to turn off the PDU switches is as follows:

Turn off the PDU switch on all system bays from system bay 0 to system bay *n* in sequence.

- You can turn off the storage system that is configured with European standard PDU switches as follows:

  Turn off PDU switches of the system bays from system bay 0 to system bay *n* in sequence.

  – For European standard PDU switches (single-phase, 220 V, 32 A), turn off the switches in a sequence of **B2** > **B1**.

  – For European standard PDU switches (three-phase, 380 V, 32 A), turn off the switches in a sequence of **C2** > **C1** > **B2** > **B1** > **A2** > **A1**.

  Figure 5-12 and **Figure 5-13** show switches on a European standard PDU switches.

  Figure 5-12 Switches on a European standard PDU (single phase, 220 V, 32 A)

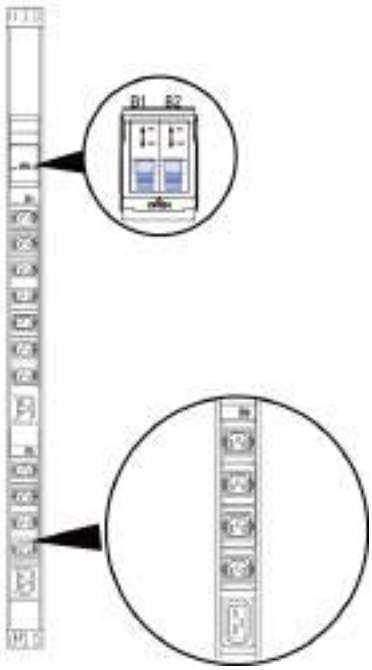
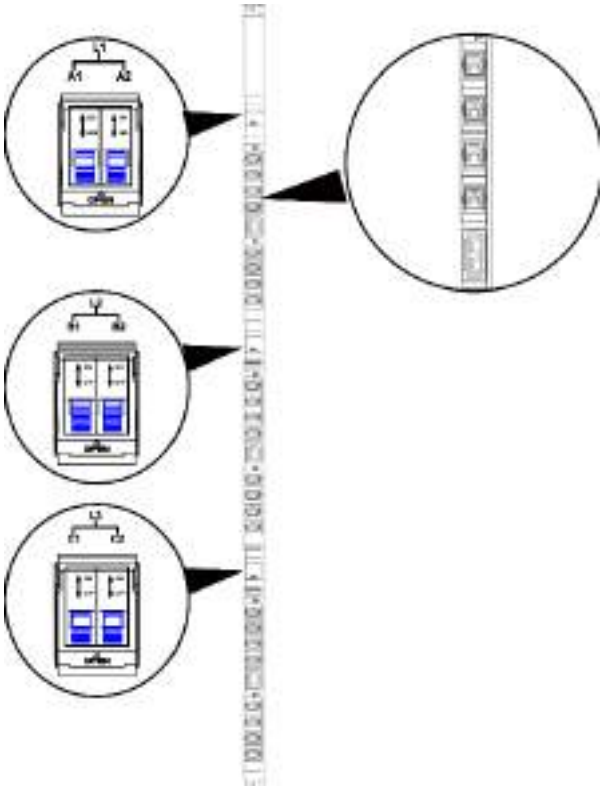


Figure 5-13 Switches on a European standard PDU (three-phase, 380 V, 32 A)



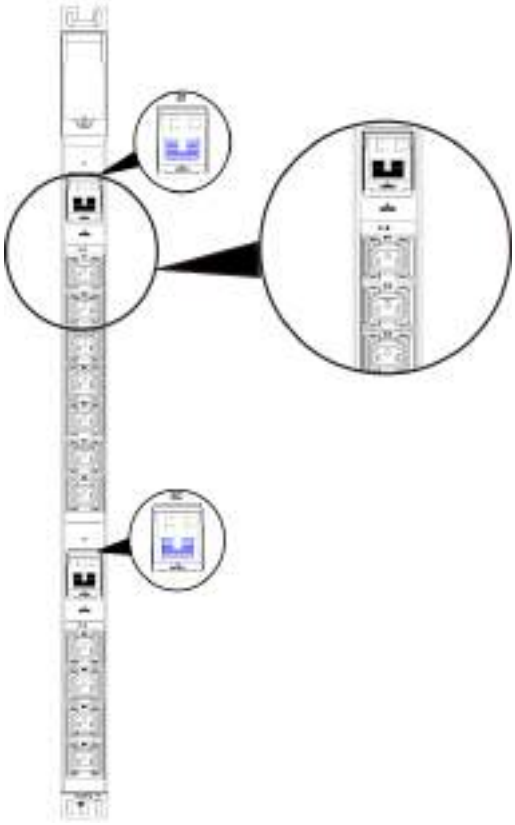
- You can turn off the storage system that is configured with HVDC PDU switches as follows:

  Turn off PDU switches of the system bays from system bay 0 to system bay *n* in sequence.

  For HVDC PDU switches, turn off the switches in a sequence of **B2** > **B1**.

  Figure 5-14 shows the HVDC PDU switch.

Figure 5-14 Switches on an HVDC PDU (240 V, 32 A)



----End

5.1.4 Restarting the Storage Device

If you want to restart the storage device, perform operations described in this section.

Prerequisites

No service is running on the storage device.

Precautions

Exercise caution when you restart the storage device as doing so interrupts the services running on the device.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose  > **Restart Device**.

Step 3 Confirm the information in the displayed **Danger** dialog box, enter the password of the currently logged-in user, and then select **I have read and understand the consequences associated with performing this operation**.

NOTICE

If you enter the wrong password more than three times within 5 minutes, the current user will be logged out and exit DeviceManager.

Step 4 Click **OK**.

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

Step 5 Click **OK**. You have restarted the storage device.

----End

5.1.5 Powering off the Storage Device upon an Emergency

If fire disaster, smoke, or flood occurs in the equipment room, you need to power off the storage system to ensure personal safety and prevent devices from damages.

NOTICE

Powering off the storage device in an irregular way may cause data loss or interrupt the services for other clients.

Follow the electricity guidelines for your equipment room when you power off the storage device.

5.1.6 Re-Powering on the Storage Device After an Emergency Power-off

Re-power on the storage device that was powered off upon on an emergency by learning about the following information.

Re-powering on the storage device that was powered off in an irregular way may incur exceptions. If this happens, record the error messages and contact our technical support engineers for troubleshooting.

To power on a storage system that went through an emergency or unexpected power-off, follow the correct power-on procedure. Note that you do not need to press the power button because the engines will automatically power on after being connected to a power supply.

5.1.7 Powering on an Interface Module

If you want to enable interface modules that have been powered off, power on them on DeviceManager.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **System > Hardware > Devices**.

Step 3 Click  to switch to the rear view.

Step 4 Click the interface module you want to power on.

The **Interface module** dialog box is displayed.

Step 5 Click **Power On**.

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

Step 6 Click **OK**. The interface module is powered on.

----End

5.1.8 Powering off an Interface Module

Before replacing the interface module, power off it at first.

Prerequisites

All services related to the interface module have been stopped.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **System > Hardware > Devices**.

Step 3 Click  to switch to the rear view.

Step 4 Click the interface module you want to power off.

The **Interface module** dialog box is displayed.

Step 5 Click **Power Off**.

The security alert dialog box is displayed.

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

Step 7 Click **OK**.

The interface module is powered off.

----End

5.2 Managing Access Permissions of a Storage System

To ensure device and service data security, the storage systems support security policy adjustment, IP address access control, and user management.

5.2.1 Configuring Security Policies

System security policies include the account policy, login policy, access control, and user account audit. Configuring system security policies helps improve system security.

5.2.1.1 Configuring the Account Policy

The account policy includes the user name, password complexity, and validity period.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **User and Security** > **Security Policies**.

Step 3 Click **Modify** on the right of **Account Policy** to configure the account policy. Related parameters are listed in **Table 5-1**.

NOTE

Click **Advanced** to display the advanced settings of **Account Policy**.

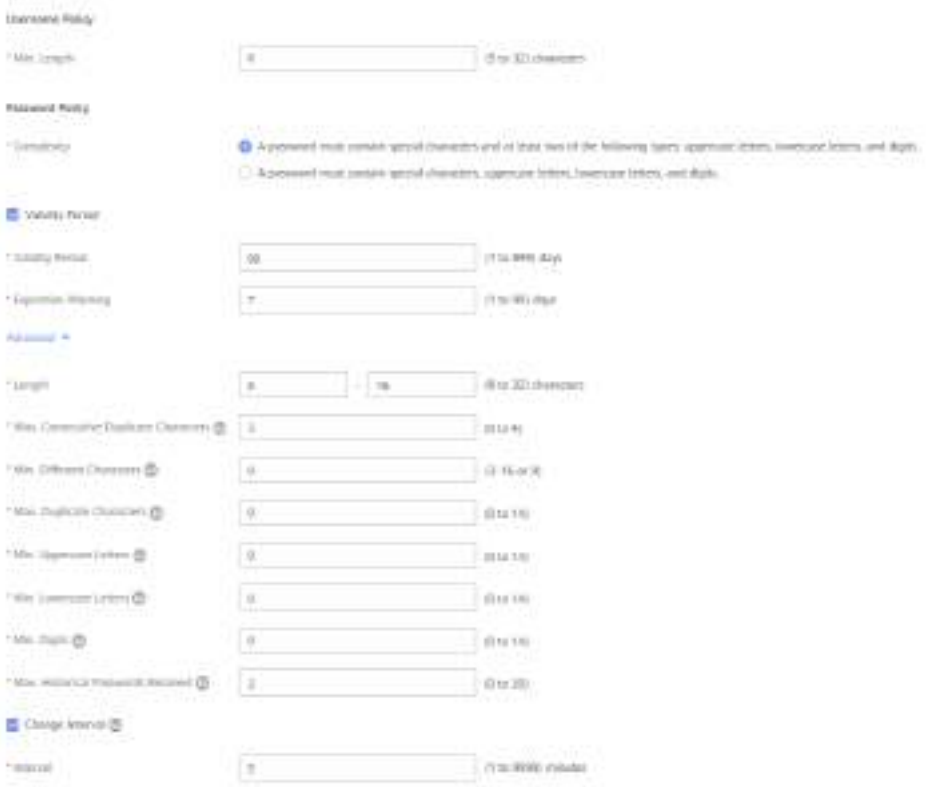


Table 5-1 Account policy parameters

Parameter	Description
Username Policy	

Parameter	Description
Min. Length (characters)	Minimum length of the user name. [Value range] Its value is an integer ranging from 5 to 32.
Password Policy	
Complexity	Complexity of the user password. A complex password is recommended. [Value range] ● A password must contain special characters and at least two of the following types: uppercase letters, lowercase letters, and digits. ● A password must contain special characters, uppercase letters, lowercase letters, and digits.
Validity Period	Indicates whether to set a password validity period. **NOTE** ● If this parameter is disabled, a password never expires. For security purposes, you are advised to enable this parameter. ● If **Validity Period** is enabled, you must set **Validity Period** and **Expiration Warning**.
Validity Period (days)	After the validity period of a password expires, the system asks you to change the password promptly. [Value range] Its value is an integer ranging from 1 to 999.
Expiration Warning (days)	Number of days prior to password expiration that the user receives a warning message. [Value range] Its value is an integer ranging from 1 to 99.
Length (characters)	Length range of a password, preventing the user from setting overly short or long passwords. [Value range] Its value is an integer ranging from 8 to 32.
Max. Consecutive Duplicate Characters	Maximum number of consecutive duplicate characters allowed in a password. Value 0 indicates unlimited. [Value range] Its value is an integer ranging from 0 to 9.
Min. Different Characters	Minimum number of different characters that a password must contain. Value 0 indicates unlimited. [Value range] 0 or an integer from 3 to the maximum password length

Parameter	Description
Max. Duplicate Characters	Maximum number of times that any character can appear in a password. Value 0 indicates unlimited. [Value range] An integer determined by **Length** and **Complexity**
Min. Uppercase Letters	Minimum number of uppercase letters that a password must contain. Value 0 indicates unlimited. [Value range] An integer determined by **Length** and **Complexity**
Min. Lowercase Letters	Minimum number of lowercase letters that a password must contain. Value 0 indicates unlimited. [Value range] An integer determined by **Length** and **Complexity**
Min. Digits	Minimum number of digits that a password must contain. Value 0 indicates unlimited. [Value range] An integer determined by **Length** and **Complexity**
Max. Historical Passwords Retained	Maximum number of retained historical passwords per user. A new password must be different from any of the retained historical passwords. Value 0 indicates unlimited. [Value range] Its value is an integer ranging from 0 to 30.
Change Interval	Indicates whether to enable a password change interval. **NOTE** If **Change Interval** is enabled, you must set **Interval**.
Interval (minutes)	Minimum interval for changing a password. [Value range] Its value is an integer ranging from 1 to 9999.

Step 4 Click **Save**.

----End

5.2.1.2 Configuring the Login Policy

The login policy includes session timeout and account lockout.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **User and Security** > **Security Policies**.

Step 3 Click **Modify** on the right of **Login Policy** to configure a login policy. **Table 5-2** describes the related parameters.

NOTE

Click **Advanced** to display the advanced settings of **Login Policy**.

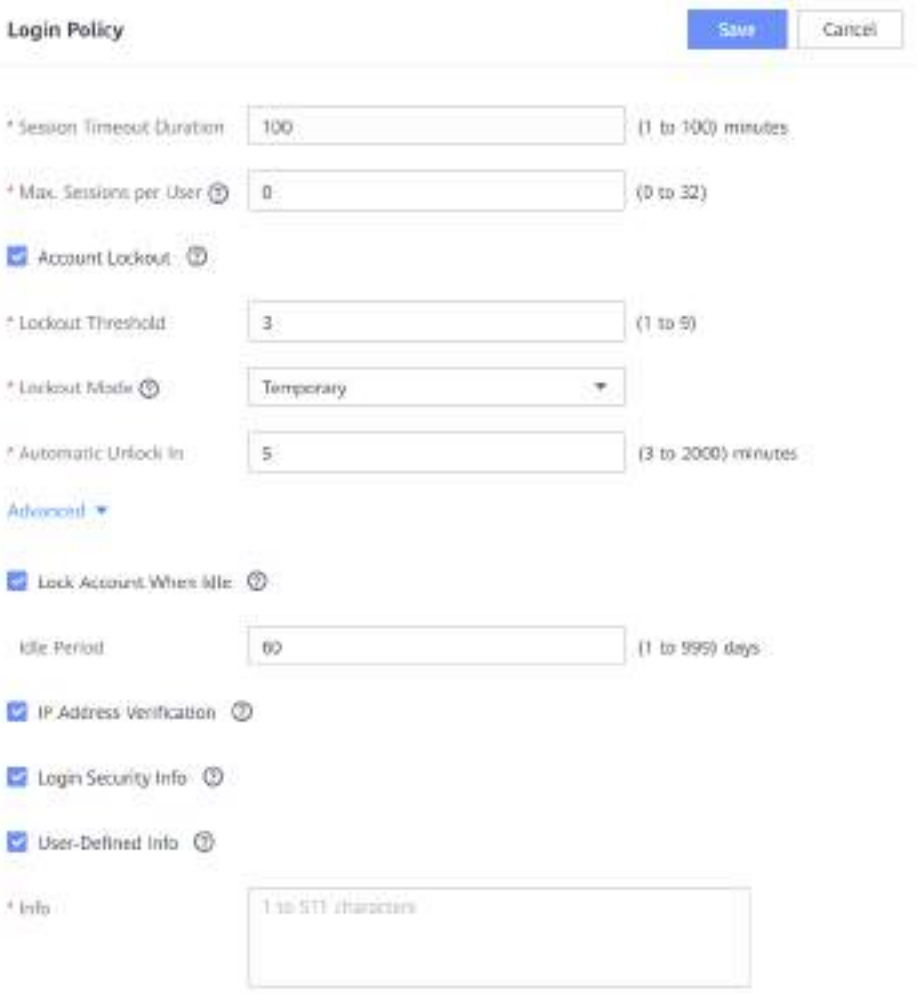


Table 5-2 Login policy parameters

Parameter	Description
Session Timeout Duration (minutes)	A user will be automatically logged out if the user does not perform any operation within the specified time. [Value range] Its value is an integer ranging from 1 to 100.
Max. Sessions per User	Maximum number of concurrent login sessions of a user. If the value is exceeded, the user cannot log in. **NOTE** Value **0** indicates no limit. [Value range] Its value is an integer ranging from 0 to 32.

Parameter	Description
Account Lockout	If **Account Lockout** is enabled and the number of consecutive incorrect password attempts exceeds the value of **Lockout Threshold** within 5 minutes, the user account is locked. **NOTE** • Disabling **Account Lockout** poses security risks. You are advised to enable this function. • If **Account Lockout** is enabled, you need to set **Lockout Threshold**, **Lockout Mode**, and **Automatic Unlock In**. • A locked account can be manually unlocked by the super administrator. If **Lockout Mode** is set to **Temporary**, the system automatically unlocks a locked account after the time specified by **Automatic Unlock In** has elapsed.
Lockout Threshold	Number of consecutive incorrect password attempts. If the number of incorrect password attempts exceeds the value of **Lockout Threshold**, the system automatically locks the account. [Value range] Its value is an integer ranging from 1 to 9.
Lockout Mode	The mode in which a user is automatically locked by the system. **NOTE** • If you select **Permanent**, a super administrator account is automatically unlocked by the system after being locked for 15 minutes, and an administrator account is permanently locked by the system. • If you select **Temporary**, set **Automatic Unlock In** to specify the automatic unlock time. [Value range] **Temporary** or **Permanent**
Automatic Unlock In (minutes)	Period after which a locked account will be automatically unlocked. **NOTE** • The automatic unlock time applies only to automatic lockout. If an account is manually locked, the time does not take effect, and the account can only be manually unlocked. • When **Automatic Unlock In** is set to a value ranging from 3 to 15, the automatic unlock time applies to all accounts. • When **Automatic Unlock In** is set to a value ranging from 16 to 2000, the automatic unlock time applies only to non-super administrator accounts. A super administrator account will be automatically unlocked after 15 minutes. [Value range] Its value is an integer ranging from 3 to 2000.

Parameter	Description
Lock Account When Idle	If an account never logs in to the system within the specified number of days, the account will be locked. **NOTE** If **Lock Account When Idle** is enabled, you need to set **Idle Period**.
Idle Period (days)	Number of days for which an account remains idle. [Value range] Its value is an integer ranging from 1 to 999.
IP Address Verification	If this parameter is selected, the login IP address must be the same as the IP address used to deliver the request. Otherwise, the request fails to be delivered.
Login Security Info	After an account logs in, the system displays information about its last login, including the login time and IP address, to enhance security.
User-Defined Info	After an account successfully logs in to the system, a warning is displayed, showing the preset prompt information. **NOTE** After **User-Defined Info** is enabled, you need to enter prompt information.
Info	This message is used to notify the user that login is successful. [Value range] Its value contains 1 to 511 characters.

Step 4 Click **Save**.

----End

5.2.1.3 Configuring Authorized IP Addresses

To prevent unauthorized IP addresses from accessing storage system, specify the IP addresses or segments that can access the device from storage system.

Prerequisites

You are a super administrator. (Only super administrators have the permission to perform this operation.)

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **User and Security** > **Security Policies**.

Step 3 Click **Modify** on the right of **Access Control** to specify the IP addresses allowed to access the storage system.

1. Enable **Access Control**.
2. Enter the IP addresses or IP address segments that can access the device.

   NOTE

   - An example of an IP address is 192.168.1.100 or fx00::1234.
   - An example of an IP address segment is 192.168.1.10-192.168.1.11.
3. Click **Add** to add the specified IP address segments or IP addresses to the IP address/address segment list.

   NOTE

   - A maximum of 32 IP addresses and IP address segments can be added.
   - After this function is enabled, if you do not allow an IP address or IP address segment to access the storage system, click ✕ next to the IP address or IP address segment. However, you must reserve at least one IP address or IP address segment. You can also click **Clear All** to delete all IP addresses and IP address segments.

Step 4 Click **Save**.

NOTE

If a dialog box is displayed, perform operations as prompted.

----End

5.2.1.4 Configuring User Account Audit

After the user account audit function is enabled, the system periodically sends account audit alarms to remind the super administrator to audit the number of accounts, roles, and status information to ensure account security.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **User and Security** > **Security Policies**.

Step 3 Click **Modify** on the right of **User Account Audit** to configure user account audit.

1. Enable **User Account Audit**.
2. Set **Audit Period**.

   NOTE

   - The value of **Audit Period** ranges from 0 to 999.
   - If **Audit Period** is set to 0 or 1, the system sends a user account audit alarm every day.

----End

5.2.1.5 Configuring the Weak Password Dictionary

Weak passwords are common or simple passwords that are easy to crack. After the weak password dictionary is configured, the passwords of local users on a storage system cannot be set to the character strings in the dictionary.

Background

After the weak password dictionary is configured, the passwords of local users cannot be set to the passwords in the weak password dictionary. This restriction does not apply to passwords of local users set before the weak password dictionary is configured.

Procedure

Step 1 Log in to the CLI as the super administrator.

Step 2 Run the **change weak_password_dictionary switch switch=on** command to enable the weak password dictionary function.

Step 3 Add weak passwords.

- Add one weak password at a time.

  Run the **add weak_password weak_password=?** command to add a user-defined weak password to the weak password dictionary.

  NOTE

  Each weak password contains 1 to 32 characters.

- Add weak passwords in batches.

  Run the **import weak_password_dictionary ip=***?* **user=***?* **password=***?* **file_path=***?* **[protocol=***?* **] [port=***?* **]** command to import the weak password dictionary.

Table 5-3 Parameters

Parameter	Description
ip=*?*	IP address of the FTP or SFTP server. [Value range] The value can be an IP address or a domain name. – When IPv4 addresses are used: ▪ A 32-bit IPv4 address is divided into four 8-bit fields that are expressed in dotted decimal notation. ▪ Each field of the IP address cannot be blank and must be an integer. ▪ The value of the leftmost field ranges from 1 to 223 (excluding 127). ▪ The values of other fields range from 0 to 255. ▪ The IP address cannot be set to a special address such as a network address or broadcast address. – When IPv6 addresses are used: ▪ A 128-bit IPv6 address is divided into eight 16-bit fields. Each 16-bit field consists of four colon-separated hexadecimal numbers. ▪ In each 16-bit field, leading zeros can be omitted for simplicity. However, at least one digit must be reserved in each field. ▪ To achieve further simplicity, you can use a double colon (::) in place of a series of zeros. A double colon can be used only once in an IPv6 address. It can also represent the neighboring consecutive zeros at the beginning or end of an IPv6 address. ▪ An IPv6 address cannot be set to a special one, such as a network address, loopback address, or multicast address. – In the event of using a domain name: ▪ A domain name is case-insensitive and must use the English alphabet. ▪ A domain name contains 1 to 255 characters.

Parameter	Description
	▪ A domain name can only contain letters (a to z and A to Z), digits (0 to 9), periods (.), and hyphens (-), and cannot start or end with a hyphen (-). [Example] 192.168.1.100
user=*?*	User allowed by the FTP or SFTP server. [Value range] The value is a string of 1 to 64 characters, excluding colons (:) [Example] user12345
password=*?*	Password of the user allowed by the FTP or SFTP server. [Value range] The value contains 1 to 64 characters. [Example] a#123456
file_path=*?*	Path for storing the weak password dictionary file on the FTP or SFTP server. [Example] .../weak password dictionary.txt **NOTE** **TXT** is case insensitive.
protocol=*?*	File transfer protocol used for transferring the weak password dictionary file. [Value range] The value can be SFTP or FTP. [Example] SFTP
port=*?*	Port number of the FTP or SFTP server. [Value range] The value ranges from 1 to 65535. [Example] 21 **NOTE** The port number configured on the storage system must be consistent with that configured on the server.

NOTE

- After the command is executed successfully, the system imports a weak password dictionary file from the specified SFTP or FTP server, clears the original weak password dictionary, and saves the weak passwords in the imported weak password dictionary.
- The weak password dictionary file to be imported must be in txt format. Each weak password occupies one line and ends with a carriage return. Each weak password contains 1 to 32 characters.
- A weak password dictionary file can contain a maximum of 1000 weak passwords or weak passwords plus blank lines. If the number of non-blank lines in a weak password dictionary file to be imported exceeds 1000, the file will not be imported.
- Blank lines are allowed. Blank lines are not considered as weak passwords whose length is 0.

----End

5.2.2 Managing Users

To prevent misoperations from affecting device stability and service data security, the storage device defines roles, each with certain permissions. To ensure storage system security, you can set password again.

NOTE

When you configure parameters relating to users, refer to the user name policy and password policy listed in **Configuring a Security Policy**. Ensure that the configured user name and password are secure enough.

5.2.2.1 Creating a Local User

To ensure device stability and service data security, a super administrator can create different levels of users based on service requirements.

Context

For the user levels, see **1 User Levels, Roles, and Permission**.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **User and Security** > **Users and Roles**.

The **Users and Roles** page is displayed.

Step 3 In the right function pane, click **Create**.

The **Create User** dialog box is displayed.

Step 4 Set user information. Select **Local user** in **Type** and configure relevant parameters.

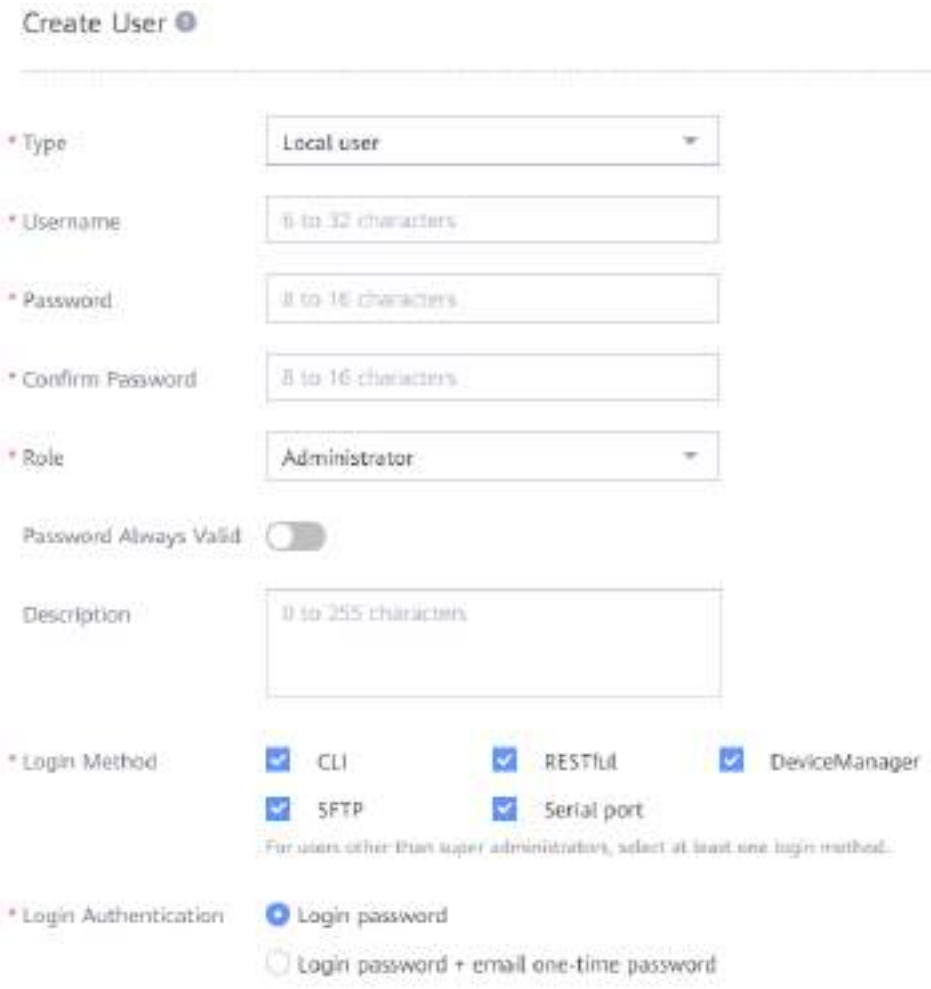


Table 5-4 describes the local user parameters.

Table 5-4 Local user parameters

Parameter	Description
Username	Name of a newly created user. [Value range] • The name contains 6 to 32 characters. • The name can only contain letters, digits, and underscores (_) and must start with a letter. • The username must be unique. **NOTE** You can modify the username policy in **Settings** > **User and Security** > **Security Policies**. [Example] user12345

Parameter	Description
Password	Password of a newly created user. [Value range] ● The password contains 8 to 16 characters. ● The password must contain special characters. Special characters include !"#$%&'()*+,-./:;<=>?@[\]^`{_|}~ and spaces. ● The password must contain uppercase letters, lowercase letters and digits. ● The maximum number of consecutive same characters cannot exceed 3. ● The password cannot be the same as the user name or the reverse of the user name. **NOTE** ● You can modify the password policy in **Settings** > **User and Security** > **Security Policies**. ● Keep your password safe. [Example] a#123456
Confirm password	Password for confirmation. [Value range] The value must be the same as that of **Password**. [Example] a#123456
Password Always Valid	Whether to make a password always valid. **NOTE** ● If this function is enabled, the password validity period is not restricted by **Password Validity Period (Days)** specified in the security policy. ● If this function is enabled, the system does not ask the account to change the password at the first login to the storage system. [Example] Enable
Role	A group of permissions. You can select a built-in role or create a self-defined role. [Example] Administrator

Parameter	Description
Description	Description of a newly created user. [Value range] The description can be left blank or contain up to 255 characters. [Example] User
Login Method	If the role of the account to be created is not super administrator, you must specify the login methods for the account. [Value range] Select at least one of the following five login methods: **CLI**, **DeviceManager**, **RESTful**, **SFTP**, and **Serial port**.
Login Authentication	Login authentication method for a newly created user. [Value range] • **Login password** • **Login password + email one-time password** **NOTE** • To use **Login password + email one-time password**, you must first enable multi-factor authentication by following instructions in **5.2.2.6.1 Enabling Multi-Factor Authentication**. • After you select **Login password + email one-time password**, you need only password authentication if your login method is **RESTful** or **SFTP**.
Recipient Email Address	If you select **Login password + email one-time password**, a one-time password will be sent to this address upon a login attempt.

Step 5 Click **OK**.

----End

5.2.2.2 Creating a Domain User

DeviceManager allows users to log in to the storage system using the Lightweight Directory Access Protocol (LDAP) server to centrally manage user information. A super administrator can create a domain user.

Context

For details about user roles and permissions, see **1 Administrator Roles and Permissions**.

Prerequisites

A domain authentication server has been configured. For details, see "Configuring Domain Authentication for a Storage System" in the *Initialization Guide*.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **User and Security** > **Users and Roles** > **Users**.

The user management page is displayed.

Step 3 Click **Create**.

The **Create User** dialog box is displayed.

Step 4 Set user information. Set **Type** to **LDAP user** or **LDAP user group** and configure the LDAP user or LDAP user group information. **Table 5-5** describes the parameters.

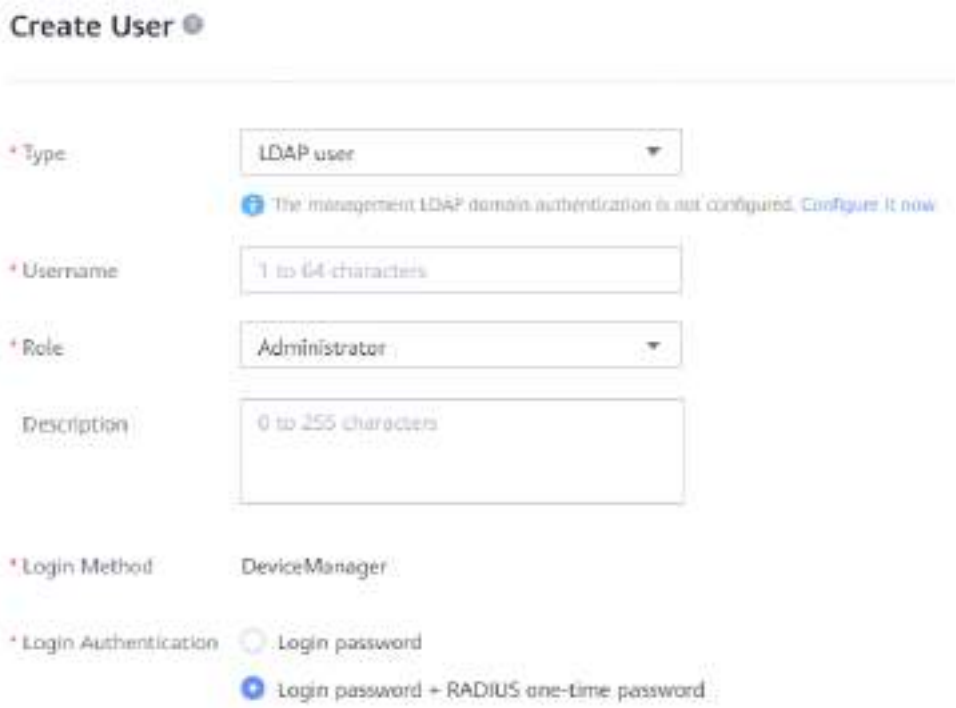


Table 5-5 LDAP user or LDAP user group parameters

Parameter	Description
Username	Name of a new LDAP user or LDAP user group. **NOTE** The new LDAP user or LDAP user group must be on the LDAP domain server. Otherwise, the login will fail. [Value range] ● The name contains 1 to 64 characters. ● The username must be unique. [Example] user12345
Role	A group of permissions. You can select a built-in role or create a self-defined role. [Example] Administrator
Description	Description of the new user. [Value range] The description can be left blank or contain up to 255 characters. [Example] User
Login Method	If the role of the account to be created is not **Super administrator**, you must specify the login methods for the account. [Value range] Select at least one of the following login methods: **CLI**, **DeviceManager**, **RESTful**, **SFTP**, and **Serial port**.
Login Authentication	Login authentication method of the new user. **NOTE** ● If you select **Login password + RADIUS one-time password**, you must enter the RADIUS one-time password during login. ● If you select **Login password + RADIUS one-time password**, only **DeviceManager** is supported in **Login Method**.

Step 5 Click **OK**.

----End

5.2.2.3 Creating a RADIUS User (Applicable to 6.1.5 and Later Versions)

This section describes how the super administrator creates a RADIUS user for a storage system.

Context

For details about user roles and permissions, see **1 Administrator Roles and Permissions**.

Prerequisites

The RADIUS server has been configured. For the configuration method, see **5.2.2.7.1 Configuring the RADIUS server**.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **User and Security** > **Users and Roles** > **Users**.

The user management page is displayed.

Step 3 Click **Create**.

The **Create User** dialog box is displayed.

Step 4 Set user information. Set **Type** to **RADIUS user** and set RADIUS user information. **Table 5-6** describes the parameters.

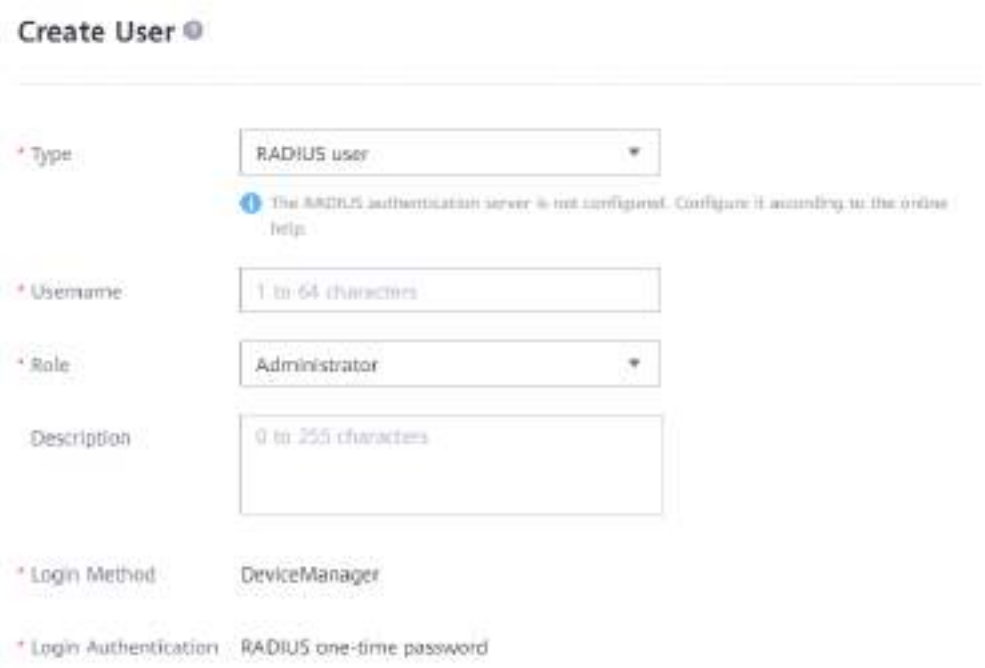


Table 5-6 RADIUS user parameters

Parameter	Description
Username	Name of the RADIUS user. **NOTE** The new RADIUS user must be a user on the RADIUS server. Otherwise, the login fails. [Value range] ● The name contains 1 to 64 characters. ● The username must be unique. [Example] user12345
Role	A group of permissions. You can select a built-in role or create a self-defined role. [Example] Administrator
Description	Description of the new user. [Value range] The description can be left blank or contain up to 255 characters. [Example] User
Login Method	Login method of the new user. For a RADIUS user, this can only be **DeviceManager**.
Login Authentication	Login authentication method of the new user. For a RADIUS user, this can only be **RADIUS one-time password**.

Step 5 Click **OK**.

----End

5.2.2.4 Managing Login Methods

The super administrator can change the login methods of local users and domain users.

Procedure

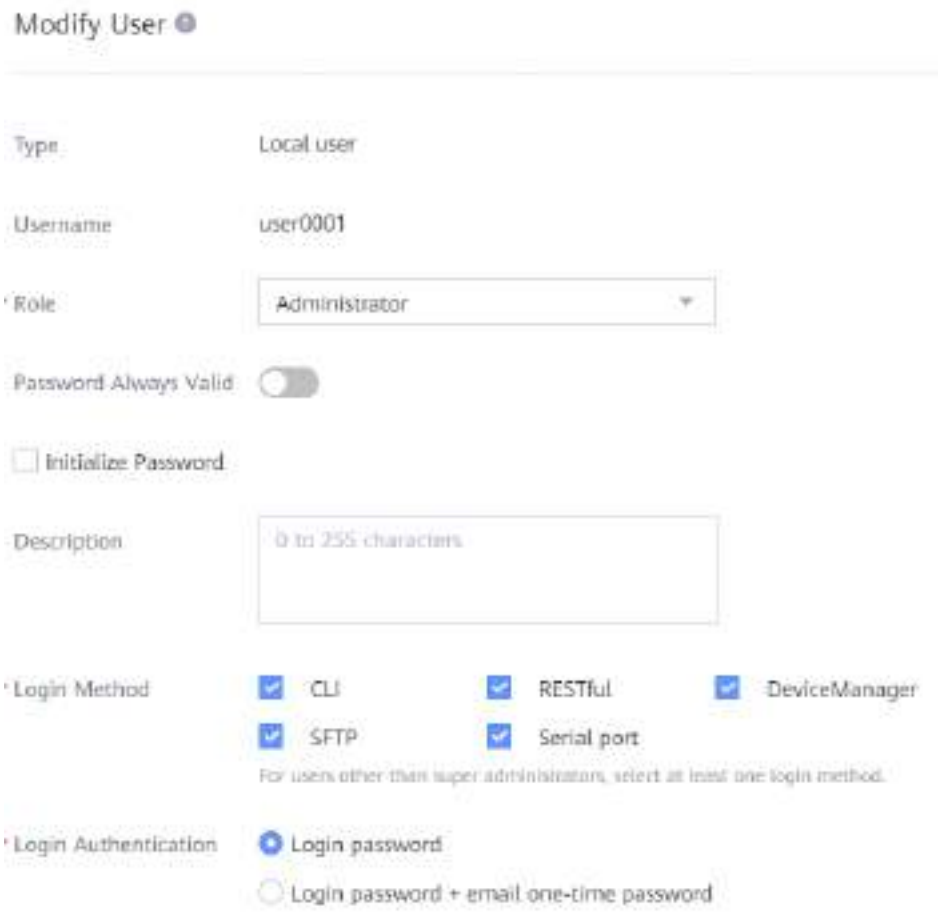
Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **User and Security** > **Users and Roles** > **Users**.

The user management page is displayed.

Step 3 Click **More** on the right side of the desired user account and choose **Modify** from the drop-down list.

The **Modify User** dialog box is displayed.



Step 4 Select the desired login methods and click **OK**.

NOTE

- For the super administrator, select at least one of the following login methods: **CLI**, **DeviceManager**, and **RESTful**.
- For non-super administrators, select at least one of the following login methods: **CLI**, **DeviceManager**, **RESTful**, **SFTP**, and **Serial port**.

Step 5 Confirm the modification of the user login method.

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

----End

5.2.2.5 Managing User Roles

User roles control the scopes of permission for users. A super administrator can change the role of a non-super administrator account to adjust the user's scope of permission according to the actual requirements. After a role is assigned to a user, the user has the permission to access or operate the objects specified by the role.

Prerequisites

The super administrator can only modify the role of a user whose **Status** is **Offline**.

Context

The storage system provides typical default roles. If the default roles cannot meet your requirements, you can create roles.

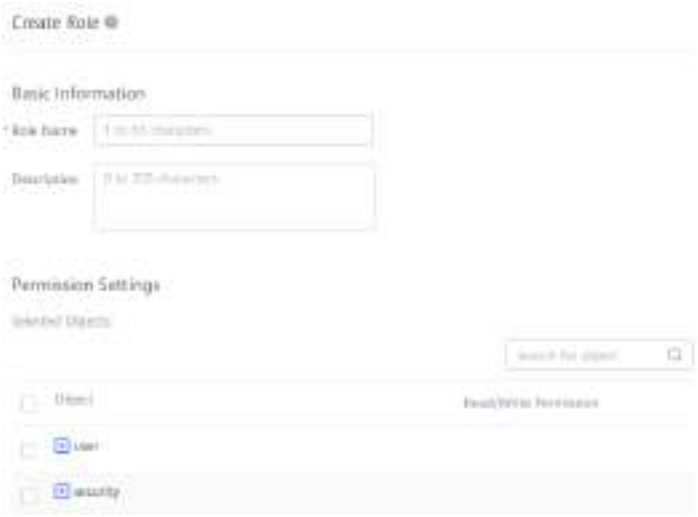
Procedure

Step 1 Log in to DeviceManager.

Step 2 (Optional) Choose **Settings** > **User and Security** > **Users and Roles** > **Roles** and manage user-defined roles.

Table 5-7 details the operations.

Table 5-7 Managing user-defined roles

Operation	Procedure
Adding a user-defined role	1. Click **Create**. The **Create Role** dialog box is displayed.  2. Set relevant parameters. Table 5-8 describes the parameters. 3. Click **OK**.

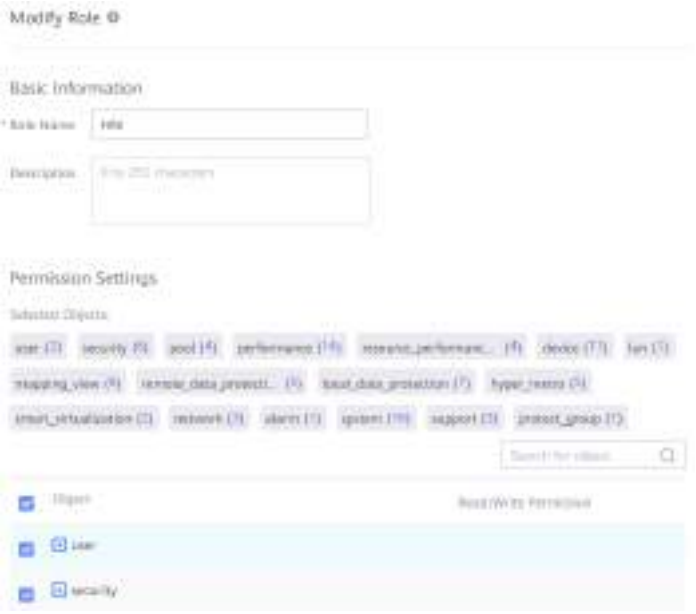
Operation	Procedure
Modifying a user-defined role	1. Click **More** on the right of the role to be modified and choose **Modify** from the drop-down list. The **Modify Role** dialog box is displayed.  2. Modify the parameters as required. **Table 5-8** describes the parameters. 3. Click **OK**.
Deleting a user-defined role	Click **More** on the right of the role to be modified and choose **Delete** from the drop-down list.

Table 5-8 User-defined role parameters

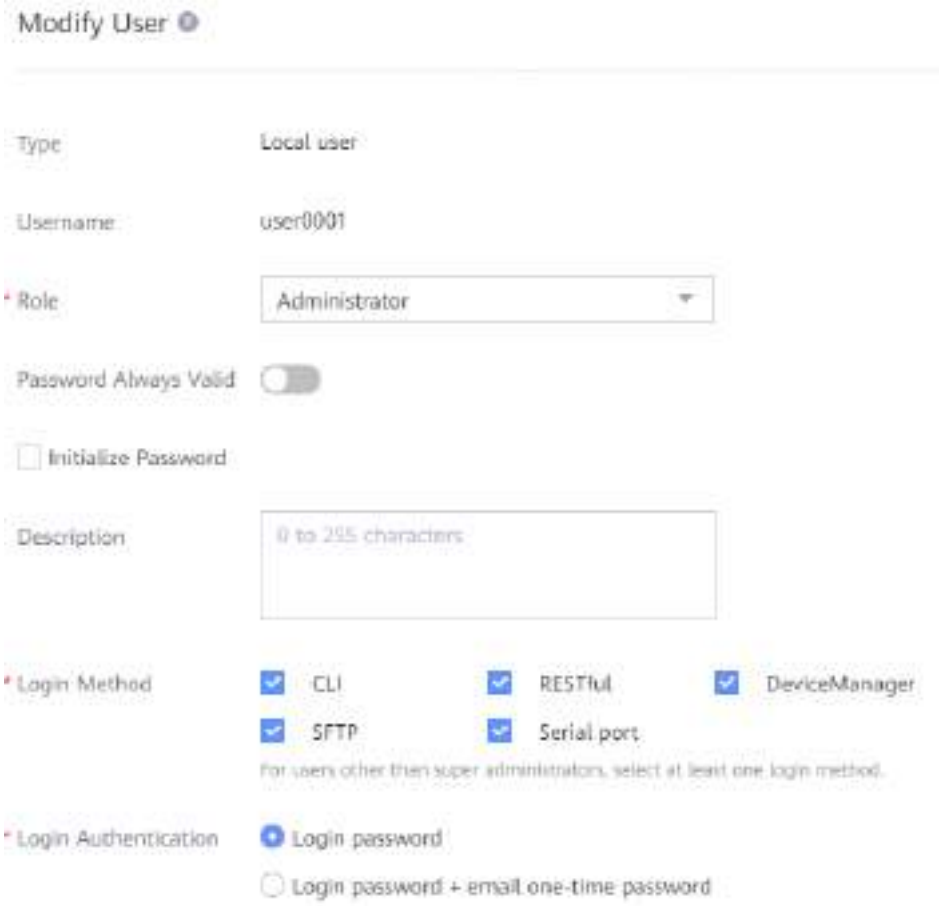
Parameter	Description
Name	Name of a role.
Owning Group	**System group** or **vStore group**
Description	Description of a role.
Object	Required object. For the object functions, see **A Permission Matrix for Self-defined Roles**.
Read/Write Permission	Read/write permission of the selected object. The value can be **Read-only** or **Readable and writable**.

Step 3 Change the user role.

1. Choose **Settings** > **User and Security** > **Users and Roles** > **Users**.
   The **Users** page is displayed.

2. Click **More** on the right of the user name to be modified and choose **Modify** from the drop-down list.

   The **Modify User** dialog box is displayed.



3. Change the user role. Select a desired role from the **Role** drop-down list.

   NOTE

   You can select a built-in or user-defined role based on your actual requirements.

Step 4 Click **OK**. Confirm the user modification.

----End

5.2.2.6 Managing Login Authentication Methods

The storage system supports multi-factor authentication. You can manage the login authentication methods based on the security requirements.

5.2.2.6.1 Enabling Multi-Factor Authentication

After enabling multi-factor authentication, you can set the login authentication method when creating an account or during O&M.

Prerequisites

- The connections between the Simple Mail Transfer Protocol (SMTP) server and all primary and secondary controllers are working properly.

- The SMTP server has been configured and is running properly. Otherwise, specified email addresses cannot receive any authentication messages.
- Before configuring a domain name for the server, ensure that the DNS server can communicate properly with the storage system or third-party server.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **User and Security** > **Multi-Factor Authentication**.

Step 3 Set email authentication.

1. Enable **Email Authentication**.
2. Set email authentication parameters listed in **Table 5-9**.

Table 5-9 Email authentication parameters

Parameter	Description
SMTP Server	IP address or domain name of the SMTP server. This is an SMTP-compliant email-sending server. By using the SMTP server, you can send authentication emails to specified email addresses.
SMTP Port	Port number of the SMTP server. The default value is **25**.

Parameter	Description
Encryption Mode	Indicates whether to encrypt the communication between the storage system and the email server. – **Not encrypted**: Data is not encrypted during transfer. – **SSL/TLS**: SSL and TLS are security protocols for data security and integrity during network communication. After this option is selected, the system selects between the two security protocols according to the email server type to encrypt data. – **STARTTLS**: After this option is selected, TLS encryption will be implemented. Previous communication data will not be retroactively encrypted using this mode. **NOTE** ■ Unencrypted data transfer risks security. Selecting **SSL/TLS** or **STARTTLS** to improve security is recommended. ■ The encryption mode configured on the storage system must be consistent with that configured on the SMTP server. ■ If you choose the SSL/TLS or STARTTLS encryption mode, you can also enable the CA certificate.
CA Certificate	Email OTP certificate. Click ***, select a CA certificate file, and click **OK**. **NOTE** – For details on how to obtain the CA certificate, see **6.3 How Do I Obtain and Import the Email Certificates or Email OTP Certificates?** – You can click **Re-upload** to upload a new CA certificate file.
Authenticate SMTP Server	Indicates whether the SMTP server authenticates a sender's identity. If this option is not selected, **Username** and **Password** are unavailable.
Username	SMTP account name of the sender. If a sender attempts to send authentication emails through an SMTP server, the sender is required by the SMTP server to enter the SMTP user name and password for authentication.
Password	Password of the SMTP account. If a sender attempts to send authentication emails through an SMTP server, the sender is required by the SMTP server to enter the SMTP user name and password for authentication.
Sender Email Address	Email address of the sender.

3. Click **Save**.

   NOTE

   You can click **Test** to test the connectivity between the storage system and SMTP server.

----End

5.2.2.6.2 Modifying the Login Authentication Method

Super administrators can modify the login authentication method of user accounts.

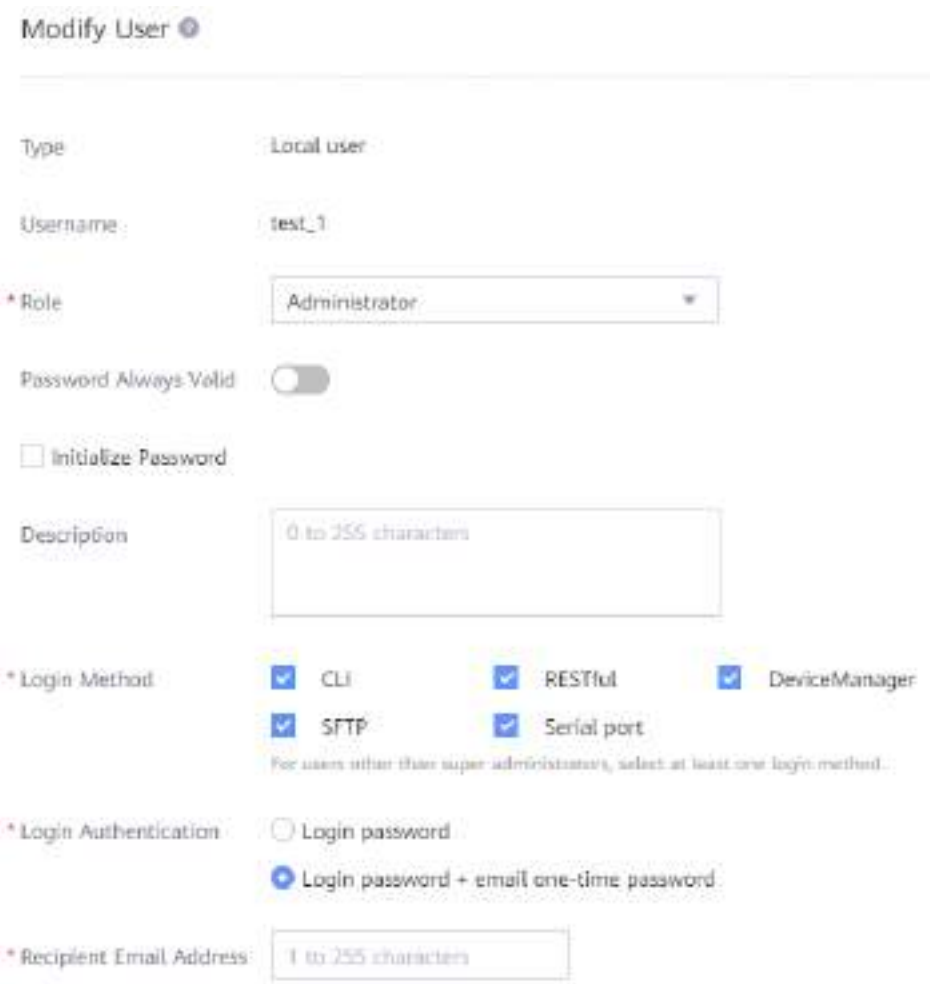
Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **User and Security** > **Users and Roles**.

Step 3 On the **Users** page, click **More** on the right side of the desired user account and choose **Modify** from the drop-down list.

The **Modify User** dialog box is displayed.



Step 4 Specify **Login Authentication**.

NOTE

- To use **Login password + email one-time password**, you must first enable multi-factor authentication by following instructions in **5.2.2.6.1 Enabling Multi-Factor Authentication**.
- After you select **Login password + email one-time password**, you need only password authentication if your login method is **RESTful** or **SFTP**.

Step 5 If you select **Login password + email one-time password**, specify the **Recipient Email Address** to which a one-time password will be sent upon a login attempt.

Step 6 Click **OK**.

----End

5.2.2.6.3 Initializing the Login Authentication Method

If you fail to receive emails due to SMTP server faults or other problems, you can initialize the login authentication method to restore it to **Login password**.

Procedure

1. Log in to the CLI of the storage system via the serial port using the **_super_admin** root administrator account.
2. Run the **initloginfactor** command to initialize the login authentication method.

```
Storage: _super_admin> initloginfactor
please input username:admin
init admin login factor, wait a moment please...
Init admin login factor succeeded
```

5.2.2.7 Managing the Login Authentication Mode of Domain Users

The storage system supports RADIUS login. You can manage the login authentication mode of domain users based on security requirements.

5.2.2.7.1 Configuring the RADIUS server

Remote Authentication Dial-In User Service (RADIUS) is an information exchange protocol based on the client/server structure. It protects networks from unauthorized access and is often applied in various network environments that require high security and allow remote access. After the RADIUS one-time password is configured, when an LDAP user attempts to log in, the storage system transfers the user information to the specified RADIUS server and processes (for example, allows or denies the access) based on the information returned by the server.

Prerequisites

- The LDAP user has been configured on the RADIUS server and LDAP domain server. Otherwise, the login fails.
- Before configuring a domain name for the server, ensure that the DNS server can communicate properly with the storage system or third-party server.

Procedure

Step 1 Log in to the CLI as the super administrator.

Step 2 Run the **change radius configuration switch=***?* **address=***?* **port=***?* **scheme=***?* **secret=***?* command to configure the RADIUS server.

Table 5-10 Parameters

Parameter	Description
switch=*?*	Specifies whether to enable the service. [Value range] The value can be **on** or **off**. [Example] on
address=*?*	RADIUS server address. [Value range] The value can be a domain name or an IP address (IPv4 or IPv6). The domain name is a case-insensitive string of 1 to 255 characters, including letters, digits, and hyphens (-). Domain names at various levels are separated by periods (.). Hyphens (-) cannot be the start or end of the domain name. [Example] 192.168.1.100
port=*?*	Port number of the RADIUS server. [Value range] The value ranges from 1 to 65535. [Example] 1812 **NOTE** The port number configured on the storage system must be consistent with that configured on the RADIUS server.
scheme=*?*	Authentication policy. [Value range] The value can be **PAP** or **CHAP**. **NOTE** Password Authentication Protocol (PAP) is a method of authenticating the identity of a user who attempts to log in to the Point-to-Point Protocol (PPP) service system. Challenge Handshake Authentication Protocol (CHAP) uses the three-way handshake to periodically verify the identity of the peer end. [Example] PAP

Parameter	Description
secret=*?*	Shared key. [Value range] The value is a string of 8 to 64 characters. [Example] a#123456

----End

5.2.2.7.2 Creating Domain Users and Configuring RADIUS One-Time Password Authentication

The super administrator can create domain users and configure RADIUS one-time password authentication.

Prerequisites

- A RADIUS server and an LDAP domain server have been configured on the storage system.
- The LDAP user has been configured on the RADIUS server and LDAP domain server. Otherwise, the login fails.

Procedure

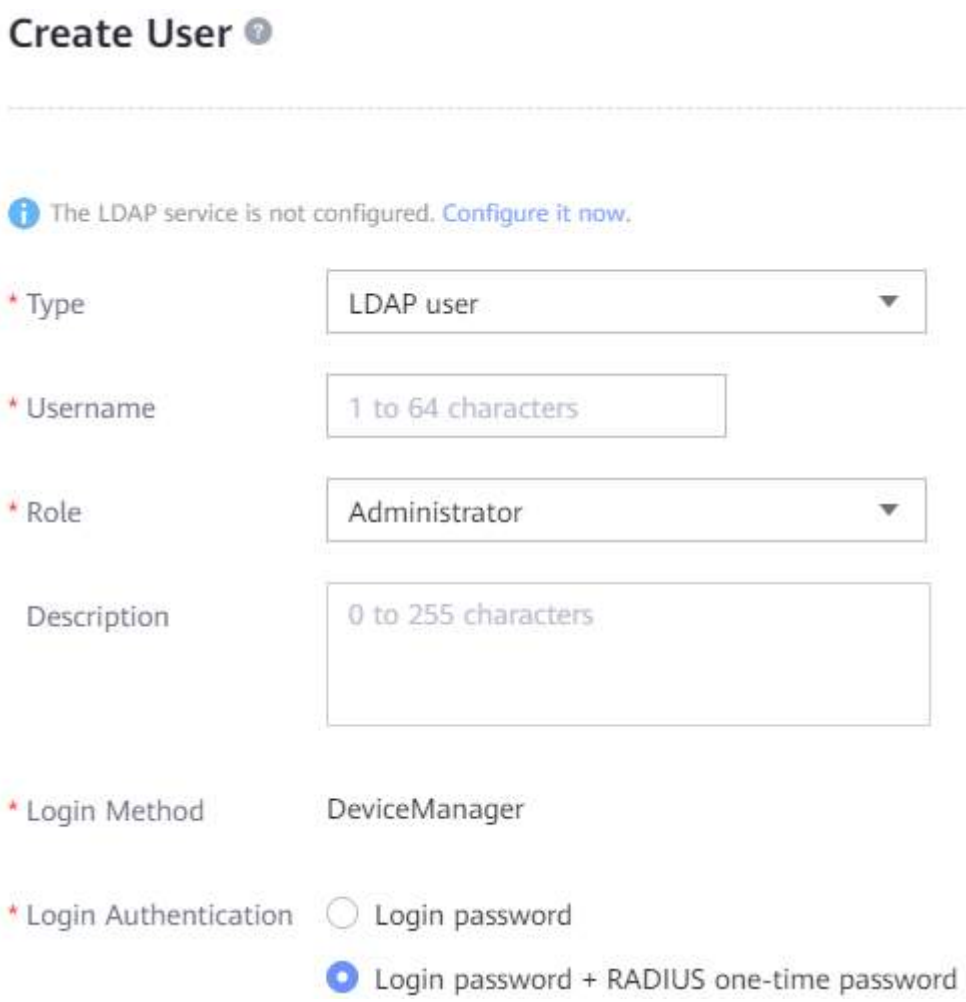
Step 1 Log in to DeviceManager as the super administrator.

Step 2 Choose **Settings** > **User and Security** > **Users and Roles** > **Users**.

The user management page is displayed.

Step 3 Click **Create**.

The **Create User** dialog box is displayed.



Step 4 Set LDAP user information.

Set **Login Authentication** to **Login password + RADIUS one-time password**. **Table 5-11** describes related parameters.

Table 5-11 LDAP user parameters

Parameter	Description
Username	Name of the new LDAP user. **NOTE** The new LDAP user must be a user on the LDAP domain server. Otherwise, the login fails.
Role	Sets the user permission range. You can select a built-in role provided by the system or customize a role.
Description	Indicates the description of the new user.

Parameter	Description
Login Method	Login method of the new user. **NOTE** If **Login password + RADIUS one-time password** is selected, **Login Method** must be set to **DeviceManager**.
Login Authentication	Login authentication mode of the new LDAP user

Step 5 Click **OK.**

----End

5.2.2.7.3 Logging In to the Storage System Using DeviceManager

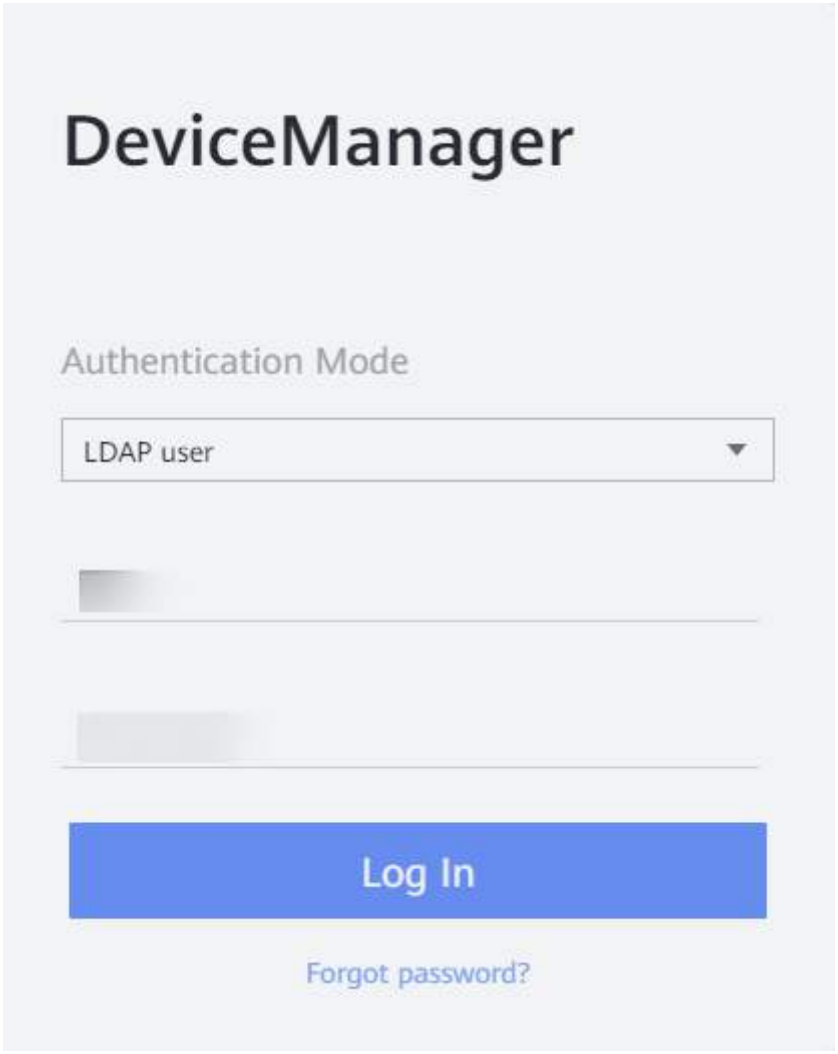
Step 1 Run a browser on the maintenance terminal.

Step 2 In the address box, enter **https://***XXX.XXX.XXX.XXX***:8088** (IP address of the management network port on the controller enclosure) and press **Enter**.

The DeviceManager login page is displayed.

Step 3 Set the login mode and language.

- Select **LDAP user** from the **Authentication Mode** drop-down list.
- You can switch the language in the upper right corner. DeviceManager supports two languages: simplified Chinese and English.



Step 4 Enter the user name and password of the administrator.

Step 5 Click **Log In**.

The system prompts you to enter the RADIUS one-time password for login.

Step 6 On the DeviceManager login page, enter the RADIUS one-time password and click **Log In**.

NOTE

When the RADIUS server uses RSA SecurID, the RADIUS one-time password consists of the PIN and token code.

- PIN is a static password string. The initial value needs to be obtained from the RADIUS server provider.
- The token code is periodically generated by the RSA SecurID hardware device. The RSA SecurID hardware device needs to be obtained from the RADIUS server provider.

  The RADIUS one-time password format is as follows: for example, the PIN is **123456** and the token code is **87654321**, the one-time password is **12345687654321**.

Step 7 (Optional) According to the settings of the RADIUS server and the status of the LDAP user, Step 7 may be repeated for multiple times. In this case, you need to enter the related information for verification according to the packet until all the information passes the verification.

NOTE

- The prompt message comes from the packet returned by the RADIUS server.
- The prompt message can be displayed in English, and contains a maximum of 4096 characters.

----End

5.2.2.8 Managing the Password

To ensure storage system security, periodically manage the login password.

5.2.2.8.1 Changing a Password

To ensure storage system security, periodically change the login password.

Context

- Super administrators and non-super administrator accounts only have the permission to change their own passwords. Super administrators have the permission to initialize the passwords of non-super administrator accounts.
- If your password has expired or is initialized, the system will prompt you to change your password when you log in to DeviceManager.
- If your password is about to expire, the system will prompt you to change your password after you log in to DeviceManager.
- To prevent security risks caused by password leaks, super administrators and non-super administrator accounts must change their default passwords at the first login and periodically in the future.
- If a non-super administrator account encounters a security problem, super administrators can set the password properties of the non-super administrator account. The password of the non-super administrator account then must be changed before it is used to log in to the system.
- Do not change the password during information collection or capacity expansion. Otherwise, information collection or capacity expansion fails.

Precautions

For a storage system configured with HyperMetro or remote replication, if a remote device has been added to the local device, you cannot perform **Offline**, **Lock**, **Modify Password Next Login**, **Password Always Valid**, **Initialize Password**, or **Delete** operations for the authentication user (whose role is **Remote device administrator**) on the remote device. Otherwise, the replication link of the remote device will fail to recover when the device is authenticated again, affecting remote replication and HyperMetro services.

Procedure

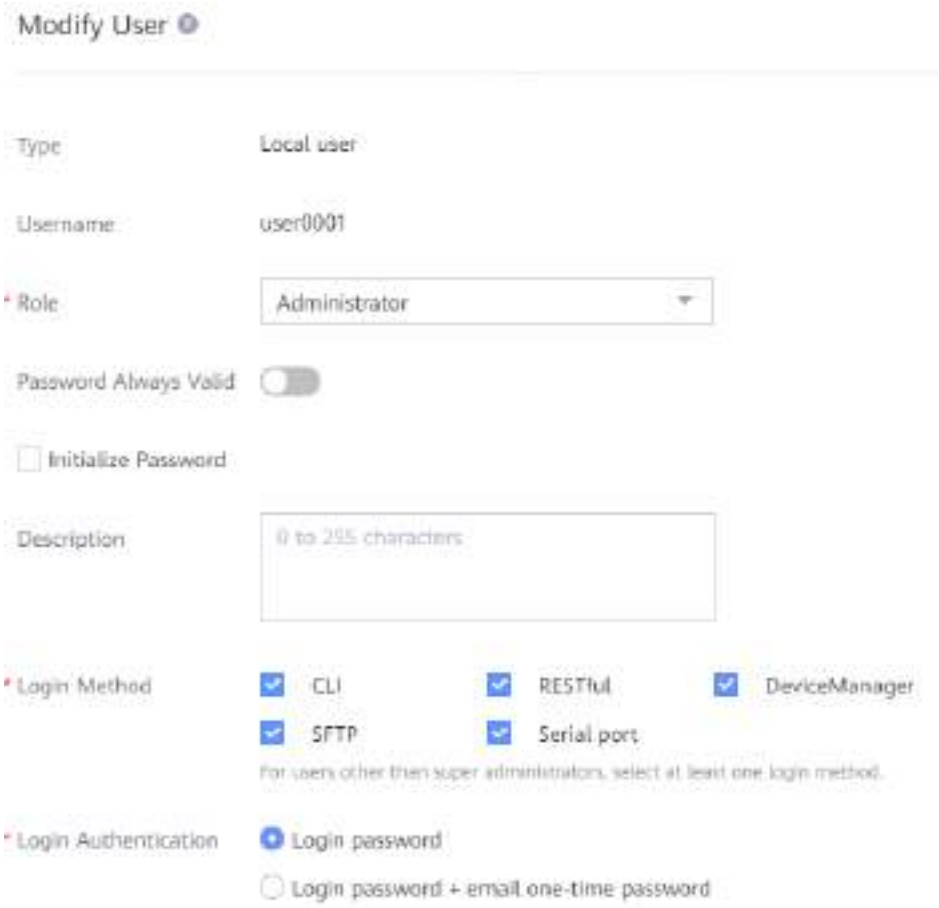
Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **User and Security** > **Users and Roles** > **Users**.

The **Users** page is displayed.

Step 3 Click **More** on the right of the user name and choose **Modify** from the drop-down list.

The **Modify User** dialog box is displayed.



Step 4 Select **Initialize Password**. Enter **Old Password**, **New Password** and **Confirm Password**.

NOTE

For security purposes, change your default password at the first login and periodically in the future.

Step 5 Click **OK** to finish modifying the password.

----End

5.2.2.8.2 Forcing the User to Change the Password

If the super administrator discovers that the password of a user encounters security risks (for example, the login IP addresses vary and incorrect passwords are entered for many times), the super administrator can force the user to change its password upon the next login.

Context

Only the super administrator can force a user to change its password upon the next login.

Precautions

For a storage system configured with HyperMetro or remote replication, if a remote device has been added to the local device, you cannot perform **Offline**, **Lock**, **Modify Password Next Login**, **Password Always Valid**, **Initialize Password**, or **Delete** operations for the authentication user (whose role is **Remote device administrator**) on the remote device. Otherwise, the replication link of the remote device will fail to recover when the device is authenticated again, affecting remote replication and HyperMetro services.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **User and Security** > **Users and Roles** > **Users**.

The **Users** page is displayed.

Step 3 Click **More** on the right of the user name to be modified and choose **Modify Password Next Login** from the drop-down list.

Step 4 Carefully read the information of the security alert dialog box that is displayed and select **I have read and understand the consequences associated with performing this operation**.

Step 5 Click **OK**.

You have finished forcing the user to change its password upon the next login.

----End

5.2.2.8.3 Managing the Password Always Valid Policy

The storage system allows you to enable the password of a user account to never expire.

Context

- If **Password Always Valid** is enabled for a user account, the system does not ask the account to change the password at the first login to the storage system. If the account never changes the password during O&M and **Password Always Valid** is disabled, the system will ask the account to change the password at the next login to the system.
- If **Password Always Valid** is enabled for a user account whose **Password Status** is **Initial password. Please change it.**, the system does not ask the account to change the password at the next login to the system.

Precautions

For a storage system configured with HyperMetro or remote replication, if a remote device has been added to the local device, you cannot perform **Offline**, **Lock**, **Modify Password Next Login**, **Password Always Valid**, **Initialize Password**, or **Delete** operations for the authentication user (whose role is **Remote device administrator**) on the remote device. Otherwise, the replication link of the remote device will fail to recover when the device is authenticated again, affecting remote replication and HyperMetro services.

Procedure

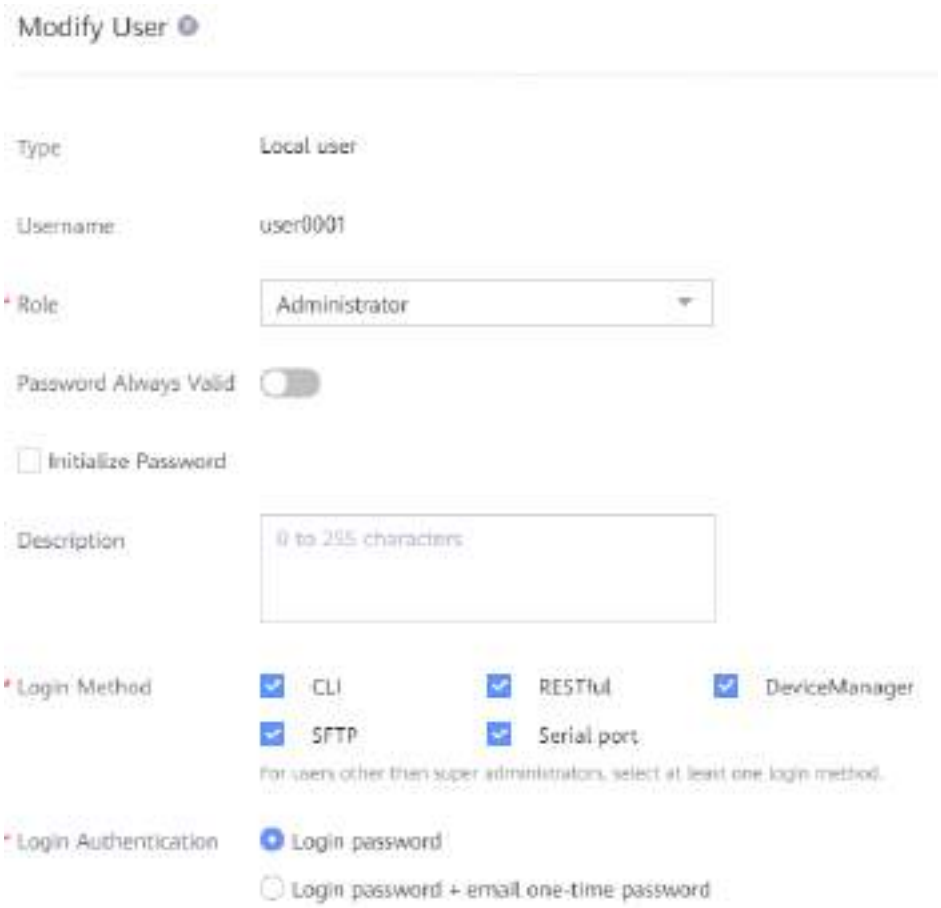
Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **User and Security** > **Users and Roles** > **Users**.

The **Users** page is displayed.

Step 3 Click **More** on the right of the user name and choose **Modify** from the drop-down list.

The **Modify User** dialog box is displayed.



Step 4 Enable or disable **Password Always Valid**.

----End

5.2.2.8.4 Resetting the Password of an Administrator or a Non-Super Administrator

This section describes how to retrieve or reset user passwords.

Context

If an administrator or a non-super administrator account forgets the password, the super administrator **admin** can reset the password on DeviceManager or the CLI.

Precautions

For a storage system configured with HyperMetro or remote replication, if a remote device has been added to the local device, you cannot perform **Offline**, **Lock**, **Modify Password Next Login**, **Password Always Valid**, **Initialize Password**, or **Delete** operations for the authentication user (whose role is **Remote device administrator**) on the remote device. Otherwise, the replication link of the remote device will fail to recover when the device is authenticated again, affecting remote replication and HyperMetro services.

Procedure

Step 1 Log in to DeviceManager as the super administrator.

NOTE

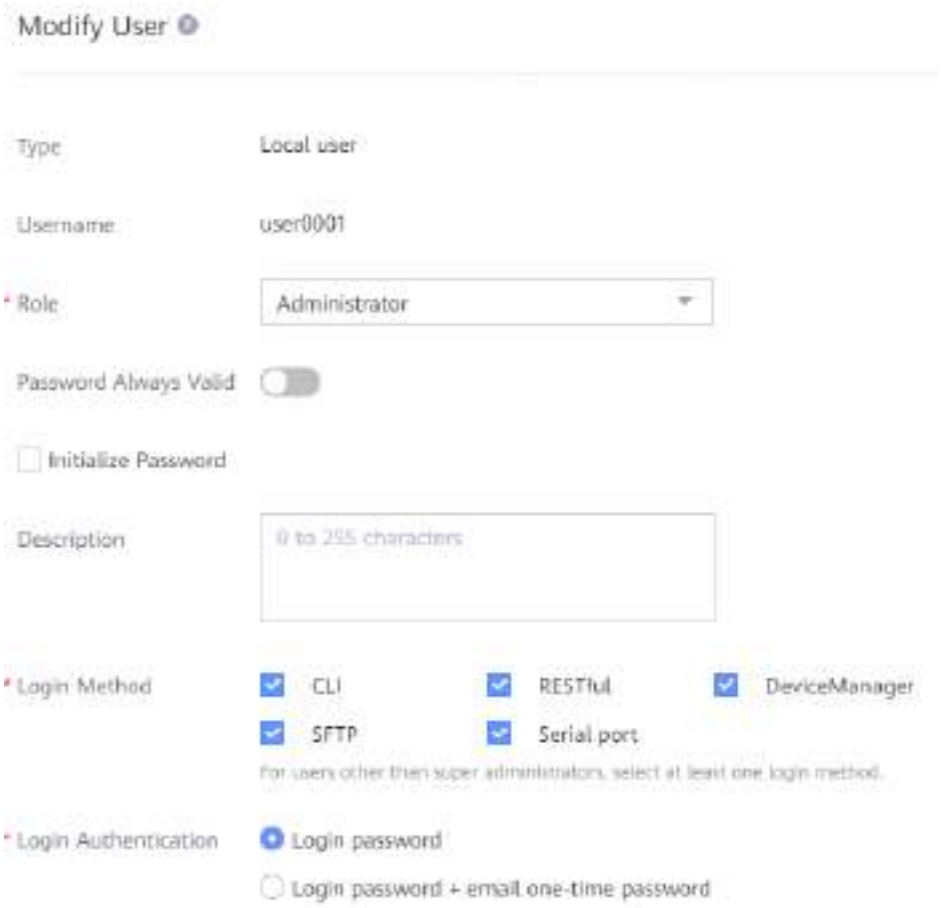
The default super administrator name is **admin**.

Step 2 Choose **Settings** > **User and Security** > **Users and Roles** > **Users**.

The **Users** page is displayed.

Step 3 Click **More** on the right of the user name to be modified and choose **Modify** from the drop-down list.

The **Modify User** dialog box is displayed.



Step 4 Select **Initialize password**. Input **Password of Current Login User**, **New Password**, and **Confirm Password**.

NOTE

The passwords of LDAP users cannot be initialized.

Step 5 Click **OK**.

----End

5.2.2.8.5 Resetting the Password of a Super Administrator

This section describes how to reset the password of a super administrator.

Context

If the password of the super administrator **admin** is lost, another root administrator **_super_admin** can log in to the CLI through a serial port and run **initpasswd** to reset the password.

Procedure

1. Use **_super_admin** to log in to the CLI through a serial port.

   NOTE

   For the default password of **_super_admin**, see the **Account List**.

2. Run the **initpasswd** command to reset the password of the super administrator **admin**.

```
Storage: _super_admin> initpasswd
please input username:admin
init admin passwd,wait a moment please...
*****please enter new password for admin :*****
*****please re-enter new password for admin :*****
Init admin passwd succeeded
```

5.2.2.9 Locking a User

A super administrator can prevent a user from logging in to the storage device by locking the user. If you lock users who are currently online, they can continue using DeviceManager but will not be able to log in again after they log out.

Context

- Only super administrators have the permission to perform this operation.
- **Lock Status** of the user to be locked is **Unlock**.

Precautions

For a storage system configured with HyperMetro or remote replication, if a remote device has been added to the local device, you cannot perform **Offline**, **Lock**, **Modify Password Next Login**, **Password Always Valid**, **Initialize Password**, or **Delete** operations for the authentication user (whose role is **Remote device administrator**) on the remote device. Otherwise, the replication link of the remote device will fail to recover when the device is authenticated again, affecting remote replication and HyperMetro services.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **User and Security** > **Users and Roles** > **Users**.

The **Users** page is displayed.

Step 3 Click **More** on the right of the user name to be locked and select **Lock** from the drop-down list.

----End

5.2.2.10 Unlocking a User

A super administrator can unlock a locked user.

Prerequisites

- Only a super administrator can unlock a user.
- The **Lock Status** of the user to be unlocked is **Lock**.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **User and Security** > **Users and Roles** > **Users**.

The **Users** page is displayed.

Step 3 Click **More** on the right of the user name to be unlocked and choose **Unlock** from the drop-down list.

The **Authenticate Permission** dialog box is displayed.

Step 4 Enter the password of the current logged-in account and click **OK**.

----End

5.2.2.11 Logging Out a User

A super administrator can prevent a logged-in user from using the storage device by forcibly logging the user out of DeviceManager.

Prerequisites

- Only a super administrator has the permission to perform this operation.
- Users whose **Status** is **Online** can be logged out.

Precautions

For a storage system configured with HyperMetro or remote replication, if a remote device has been added to the local device, you cannot perform **Offline**, **Lock**, **Modify Password Next Login**, **Password Always Valid**, **Initialize Password**, or **Delete** operations for the authentication user (whose role is **Remote device administrator**) on the remote device. Otherwise, the replication link of the

remote device will fail to recover when the device is authenticated again, affecting remote replication and HyperMetro services.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **User and Security** > **Users and Roles** > **Users**.

Step 3 Click **More** on the right of the user to be brought offline and choose **Offline** from the drop-down list.

The security alert dialog box is displayed.

Step 4 Confirm the logout of the user.

1. Carefully read the content in the dialog box and select **I have read and understand the consequences associated with performing this operation** to confirm the information.
2. Click **OK**.

----End

5.2.2.12 Removing a User

This operation enables you to remove an unwanted user.

Context

- Only a super administrator has the permission to remove the administrators and non-super administrator accounts.
- An online user cannot be removed.

Precautions

For a storage system configured with HyperMetro or remote replication, if a remote device has been added to the local device, you cannot perform **Offline**, **Lock**, **Modify Password Next Login**, **Password Always Valid**, **Initialize Password**, or **Delete** operations for the authentication user (whose role is **Remote device administrator**) on the remote device. Otherwise, the replication link of the remote device will fail to recover when the device is authenticated again, affecting remote replication and HyperMetro services.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **User and Security** > **Users and Roles** > **Users**.

The **Users** page is displayed.

Step 3 Click **More** on the right of the user name to be removed and choose **Delete** from the drop-down list.

The security alert dialog box is displayed.

Step 4 Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation**.

Step 5 Click **OK**.

----End

5.2.3 Configuring a CAS Server

After a Central Authentication Service (CAS) server is configured on the storage system, eSight users can directly access the storage system through Single Sign-On (SSO).

Context

- As a part of identity management, SSO allows a user to access protected resources of applications on the same server after the user logs in to any one of the applications. In other words, after passing the security verification of an application, the user does not need to log in to other applications again for verification when accessing protected resources of these applications.
- CAS is a single sign-on protocol for the web. Its purpose is to permit users to access multiple applications by providing their credentials (such as user names and passwords) only once.
- For more information, see **SSO Integration** in the *eSight Product Documentation*.
- CAS on the storage system is controlled by the SSO certificate.

Prerequisites

The storage system has been added to eSight for management. For details about how to add a storage system to eSight for management, see **Storage Management** in the *eSight Product Documentation*.

Procedure

Step 1 Stop the eSight service. For details, see **Starting and Stopping the eSight Server** in the *eSight Product Documentation*.

Step 2 Log in to the eSight server.

- In Windows, log in as user **Administrator**.
- In Linux, log in as user **ossuser**.
- In the event of a dual-node system, log in to the active server as user **ossuser**.

Step 3 Add the storage system to the whitelist in the SSO configuration file of eSight.

1. Use **Notepad** to open the **sso.xml** file in eSight installation directory **.../eSight/AppBase/etc/oms.sso**.
2. Add the IP address of the storage system to the **<param name="client-trusted-ip">XX.XX.XX.XX</param>** tag.

```
<param name="client-trusted-ip">XX.XX.XX.XX,YY.YY.YY.YY</param>
```

NOTE

If there are multiple IP addresses, use commas (,) to separate them.

3. Save the configuration file and start eSight.

Step 4 Enable SSO.

1. Open the **config.xml** file in eSight installation directory **.../eSight/AppBase/etc/esight.storage**.
2. Set **<param name="devicemanager.ssologin">XXX</param>** to **true**.
   ```
   <param name="devicemanager.ssologin">true</param>
   ```

Step 5 Enable the eSight service. For details, see **Starting and Stopping the eSight Server** in the *eSight Product Documentation*.

Step 6 Obtain the CAS server's SSO certificate named **ca.crt** from eSight installation directory **.../eSight/AppBase/etc/certificate/application/ca**.

Step 7 Configure the CAS server on the storage system.

1. Log in to DeviceManager.
2. Choose **Settings** > **User and Security** > **CAS Server Settings**.
3. Configure the CAS server.
   a. Enable **CAS Server Settings**.
   b. Enter the CAS server's **Server Address** and **Port**.

      NOTE

      - The address of the CAS server is that of the eSight server.
        - If eSight is used in the multi-subnet management scenario, use the IP address of the eSight server that is in the same network segment as that of the storage system.
        - If eSight is used in the southbound and northbound isolation scenario, use the southbound IP address.
      - The default port number is 31942.

   c. Import the SSO certificate into the storage system.
   d. Click **Save**.
   e. (Optional) Click **Test** to check whether the configured CAS server is available.

Step 8 Log in to eSight. On the **Storage Device** tab page, click  to log in to the DeviceManager of the storage system.

----End

Follow-up Procedure

To enable eSight users to log in to the storage system through SSO, you must establish a mapping relationship between eSight user roles and storage system user roles. An eSight user has the same storage system permissions as the storage system user role corresponding to the eSight user role. By default, the storage system has created a mapping relationship between two groups of roles. See **Table 5-12**.

Table 5-12 Role mapping

eSight User Role	Storage System User Role
Administrator	Super administrator
Monitor	Administrator

NOTE

- If you want to use another eSight user role, create a storage system user role with its name set to that of the eSight user role on the storage system so that a mapping relationship between the two roles is established.

  For example, if the role of an eSight user is **role1**, create the **role1** role on the storage system. Then, the eSight user has the same storage system permissions as **role1** created on the storage system.
- If an eSight user has multiple roles and all of them have mapping relationships with storage system user roles, the storage system randomly assigns a mapped role when the eSight user logs in through SSO. You can choose **Settings** > **User and Security** on DeviceManager and check the current user role on the **Users** page.

5.2.4 Configuring a Third-Party NMS to Use a Token to Log In to DeviceManager in Password-Free Mode

After the preset account is configured for the third-party NMS, the DeviceManager page is directly displayed. You do not need to manually enter the account for login.

Procedure

Step 1 The client obtains the token using the following path, and records and pastes it in subsequent requests.

URL: **https://${ip}:${port}/deviceManager/rest/***xxxxx***/sessions**

Access method: PUT

```
Request:PUT /deviceManager/rest/xxxxx/sessions
{
    "username": "admin",
    "password": "Admin@123",
    "scope": "0"
}

Response:
{
  "data": {
    "passphrase": "066D6BB7AE342A3C87D0D5F11925E938CDC197F5C05A94E57D1279E78EA2425C"
  },
  "error": {
    "code": 0,
    "description": "0"
  }
}
```

NOTE

For details about how to use the APIs, see the *REST API Reference* of the specific product model.

Step 2 Log in to DeviceManager using the following path:

https://${ip}:${port}/deviceManager/devicemanager/feature/login/crossDomainLogin.html?passphrase=${*Token obtained in* ***Step 1****, which is the content following the* ***passphrase*** *field*}**&language=en**

----End

5.3 Managing Alarms and Events

To better manage and handle alarms and events, read this chapter to learn the alarming mechanism, alarms and events notification methods, and alarm dump function.

An alarm severity indicates the impact of an alarm on user services. **Table 5-13** describes the four severity levels.

Table 5-13 Alarm severity levels

Alarm Severity	Icon	Definition	Way of Handling
Critical		Interrupts services or causes the system to break down.	Must be cleared immediately. Otherwise, the system may break down.
Major		Affects part of the device in a limited range or impacts the system performance.	Must be cleared as soon as possible. Otherwise, important functions will be affected.
Warning		Has no impact on the device. The system detects a potential or imminent fault that may affect services.	A warning is reported to instruct maintenance personnel to promptly find the alarm cause and rectify the potential fault.
Info		Information about operations without any effect on the device.	Lets maintenance personnel know the running status of the network and devices. They are handled based on the actual condition.

5.3.1 Managing Email Notification

This section describes how to modify the SMTP server and email address for receiving notifications.

5.3.1.1 Managing the Sender Email Address

This section describes how to manage the SMTP server and sender email address.

Prerequisites

- The connections between each SMTP server and primary and secondary controllers are normal.
- The storage system's alarm and event email notification function supports the PLAIN and LOGIN authentication mechanisms. Therefore, when configuring the email server, ensure that at least one of the two authentication mechanisms is supported.
- You have logged in to DeviceManager as a user who has necessary operation permissions.
  - Super administrator
  - Administrator
- The DNS server communicates properly with the storage array or third-party server.

Precautions

- The storage system sends the SMTP server only the alarms and events that are generated after email notification is configured.
- To ensure that emails can be sent successfully, the sender email address must match the SMTP server address. In addition, ensure that the sender email address can send emails to the recipient email addresses.

  For example, if the SMTP server in use is a Gmail SMTP server, the sender email address must be a Gmail email address.
- If two SMTP servers are configured, the sender email address must match the two SMTP servers' addresses. In addition, ensure that the sender email address can send emails to the recipient email addresses.

  For example, if the sender email address is a Gmail address, the two SMTP servers must come from a Gmail mailbox provider.

  NOTE

  You are advised to deploy only one SMTP server on a host. Otherwise, you may be unable to receive email notification due to port conflict.
- If the IP addresses or networks between a storage system and an SMTP server are blocked (for example, by firewalls or IP address whitelists), ensure that the storage system's all management IP addresses communicate properly with the SMTP server.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Basic Information** > **Email Service**.

Step 3 Click **Modify** to set SMTP server and sender information. **Table 5-14** describes the parameters.

Figure 5-15 Sender settings

Table 5-14 Email notification parameters

Parameter	Description
SMTP Server	IP address or domain name of the SMTP server. This is an SMTP-compliant email-sending server. The emails containing alarm information can be sent to specified email boxes through the SMTP server. **NOTE** • A maximum of two SMTP servers can be added. If one of the SMTP servers cannot send notification emails, the other SMTP server will be used to send notification emails again. • To test whether the server is available, choose **Settings** > **Alarm Settings** > **Alarm Notification**, add a recipient email address, and click **Test**. [Example] 192.168.1.100
SMTP Port	Indicates the port setting of SMTP. The value ranges from 1 to 65535. The default value is 25. **NOTE** The SMTP port number configured on a storage system must be consistent with that configured on the SMTP server. [Example] 25

Parameter	Description
Encryption Mode	The encryption mode used for network communication between the storage system and email server. • Not encrypted: Data transfer is not encrypted. • SSL/TLS: SSL and TLS are two different security protocols used to ensure the security and data integrity during network communication. If you select SSL/TLS, the system automatically selects one of them for encryption according to the email server type. • STARTTLS: After the **STARTTLS** command is executed, TLS encryption is implemented. Communication data is not encrypted before the **STARTTLS** command is executed. **NOTE** • For security purposes, you are advised to select an encryption mode. • The encryption mode configured on the storage system must be consistent with that configured on the SMTP server. • If you choose the SSL/TLS or STARTTLS encryption mode, you can also enable the CA certificate. For details on how to obtain the CA certificate, see **6.3 How Do I Obtain and Import the Email Certificates or Email OTP Certificates?**. [Example] STARTTLS
Authenticate SMTP Server	Indicates whether the SMTP server needs to authenticate senders. If it is not selected, **Username** and **Password** are unavailable.
Username	SMTP account name of the sender. When emails are sent through the SMTP server, the sender is prompted to type the SMTP account name and password for authentication. **NOTE** The value cannot be blank, and contains 1 to 63 characters. It cannot contain a single quotation mark ('). [Example] testuser
Password	Password of the SMTP account. When emails are sent through the SMTP server, the sender is prompted to type the SMTP account name and password for authentication. **NOTE** • The value cannot be blank, and contains 1 to 63 characters. • A valid password cannot contain extended ASCII characters or Unicode characters. It is recommended that a password contain characters in the following categories: base 10 digits (0 to 9), English characters (a to z and A to Z), spaces, and [\]^_{|}~`@!"#$%&'()*+,-./:;<=>?. [Example] aJ1p23dySQ

Parameter	Description
Sender Email Address	Sender's email address. **NOTE** The sender email address must match the SMTP server address. For example, if a Gmail SMTP server is used, the sender email address must be a Gmail address. [Example] username@domain.com
Max. Size of Email Attachment	Maximum size of an email attachment. The value ranges from 1 MB to 100 MB.

Step 4 Click **Save**.

----End

5.3.1.2 Managing Recipient Email Addresses and Notification Types

This section describes how to configure recipients.

Prerequisites

- You have logged in to the system as an administrator that has operation permissions.
- The email notification function has been enabled.
- An SMTP server is available and configured.

Context

For this version, emails are sent for notification when an alarm is reported or cleared.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Alarm Settings** > **Alarm Notification** > **Email Notification**.

Step 3 Set **Email Title Prefix** which is a sender-defined email title field. If there are too many emails, users can search for desired emails using this field.

Figure 5-16 Setting **Email Title Prefix**

NOTE

- The length ranges from 0 to 511 bytes and cannot contain single quotation marks (').
- In addition to custom fields, you can also select **Device name**, **Alarm ID**, **Alarm severity**, or **Alarm description**. If these options are selected, the information about the selected options is displayed in the title of an alarm notification email.

Step 4 Click **Modify** and manage recipient email addresses. **Figure 5-17** details the operations.

Figure 5-17 Recipient Settings

Table 5-15 Relevant operations

Operation	Procedure
Adding a recipient email address	1. Click **Add** below the **Recipient Settings** list. 2. Set **Recipient Email Address**, **Alarm Severity**, and **Event Notification**. **NOTE** – A recipient email address is a string of 1 to 255 characters. – Possible values of **Alarm Severity** are **Warning**, **Major**, and **Critical**. – After the event notification function is enabled, you can enable or disable the notification mode of certain events by referring to **5.3.8 Managing Event Notification**. 3. Click ✓.

Operation	Procedure
Editing a recipient email address	1. In the **Recipient Settings** list, select the email address to be modified and click . 2. Modify **Recipient Email Address**, **Alarm Severity**, and **Event Notification**. **NOTE** – A recipient email address is a string of 1 to 255 characters. – Possible values of **Alarm Severity** are **Warning**, **Major**, and **Critical**. – After the event notification function is enabled, you can enable or disable the notification mode of certain events by referring to **5.3.8 Managing Event Notification**. 3. Click .
Removing a recipient email address	In the **Recipient Settings** list, select the email address to be deleted and click .

Step 5 **Optional:** You can add a recipient email address and click **Test** to check whether an alarm notification can be sent.

The **Information** dialog box is displayed. Read the information in the dialog box carefully and click **OK**.

Step 6 Click **Save**.

----End

5.3.2 Managing SMS Notification

DeviceManager can send alarms and events to specific mobile phones using SMS, allowing easy device monitoring.

5.3.2.1 Managing Recipient Phone Numbers and Notification Types

If the phone numbers used to receive alarms and events are changed, update them immediately so that users can receive alarms and events about the storage system through SMS messages.

Prerequisites

- You have logged in to the system as an administrator that has operation permissions.
- The SMS notification function has been enabled.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings > Alarm Settings > Alarm Notification > SMS Notification**.

Step 3 Click **Modify** to set the recipient information. **Table 5-16** details the operations.

Figure 5-18 Recipient Settings

Table 5-16 Relevant operations

Operation	Procedure
Adding a recipient	1. Click **Add** below the **Recipient Settings** list. 2. Set **Recipient Phone Number**, **Alarm Severity**, and **Event Notification**. **NOTE** – A recipient number contains 3 to 31 digits. – Possible values of **Alarm Severity** are **Warning**, **Major**, and **Critical**. – After the event notification function is enabled, you can enable or disable the notification mode of certain events by referring to **5.3.8 Managing Event Notification**. 3. Click ✓.

Operation	Procedure
Changing a recipient	1. In the **Recipient Settings** list, select the email address to be modified and click  . 2. Set **Recipient Phone Number**, **Alarm Severity**, and **Event Notification**. **NOTE** – A recipient email address is a string of 1 to 255 characters. – Possible values of **Alarm Severity** are **Warning**, **Major**, and **Critical**. – After the event notification function is enabled, you can enable or disable the notification mode of certain events by referring to **5.3.8 Managing Event Notification**. 3. Click  .
Removing a recipient	In the **Recipient Settings** list, select the phone number to be deleted and click  .

Step 4 **Optional:** Select a recipient phone number and click **Test** to check whether an SMS notification can be sent.

Step 5 Click **Save**.

----End

5.3.2.2 Configuring a GSM Modem

This section describes how to configure a GSM modem. You can configure short message notification only after configuring a GSM modem.

Prerequisites

You have installed a GSM modem.

Context

NOTICE

- If the GSM modem is not hot-swappable, do not insert or remove it when it is running.
- If short message notification is enabled on the storage system, the serial port on the controller enclosure serves only the GSM.
- For a storage system with eight or more controllers, GSM modems can only be configured for the first eight controllers.
- You are advised to connect the GSM modem to the serial port of the management modules 0. If the serial port of the management modules 0 fails, connect the GSM modem to the serial port of the management modules 1.

To demonstrate how to configure a GSM modem, the COM1 serial port (baud rate = 115200 bit/s) on the host and the DB9 serial port on the GSM modem (default baud rate = 9600 bit/s) are used as an example.

Procedure

Step 1 Insert a SIM card into the GSM modem.

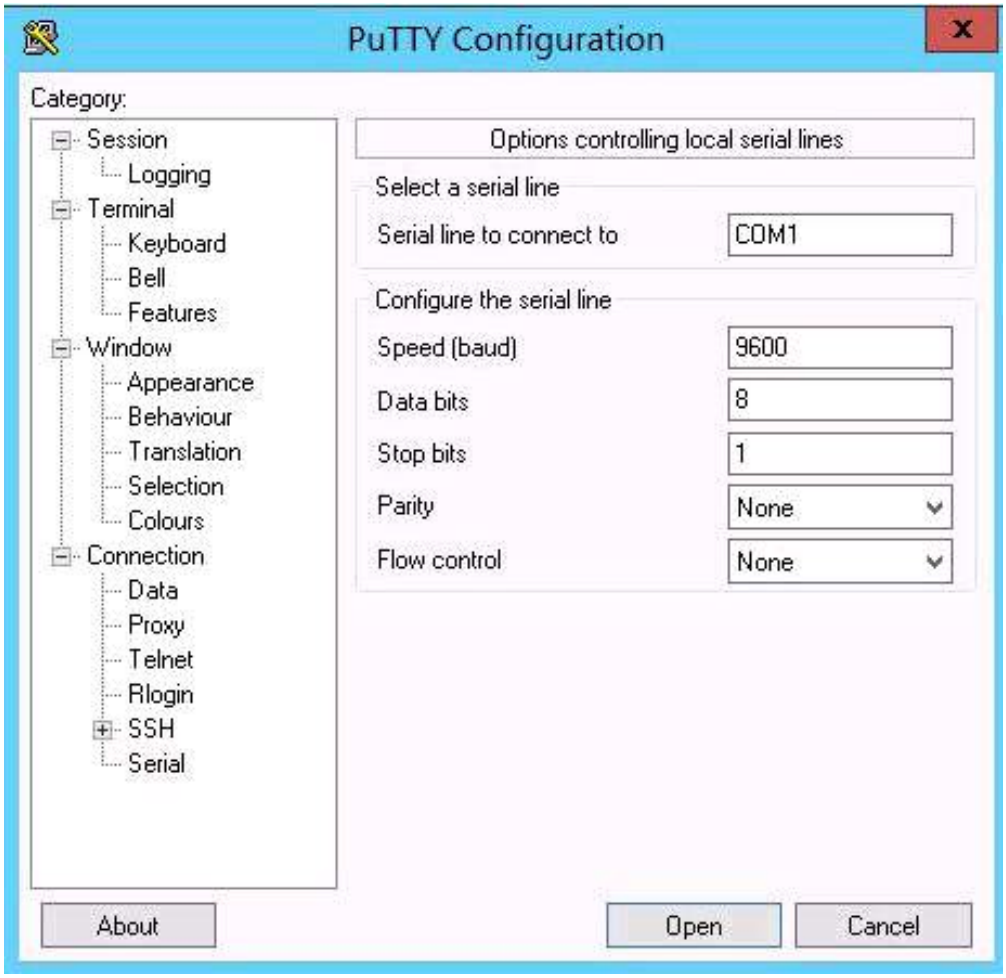
Step 2 Connect GSM modem to the maintenance terminal serial port through a DB9 serial cable.

Step 3 Insert the power cable of the GSM modem into the power supply outlet, and then power on the GSM modem.

If the red indicator blinks, the GSM modem is successfully installed.

Step 4 Run PuTTY. In the **Category** navigation tree, choose **Connection** > **Serial**. The **Options controlling local serial lines** page for configuring the GSM modem is displayed, as shown in **Figure 5-19**.

Figure 5-19 Page for **Options controlling local serial lines**

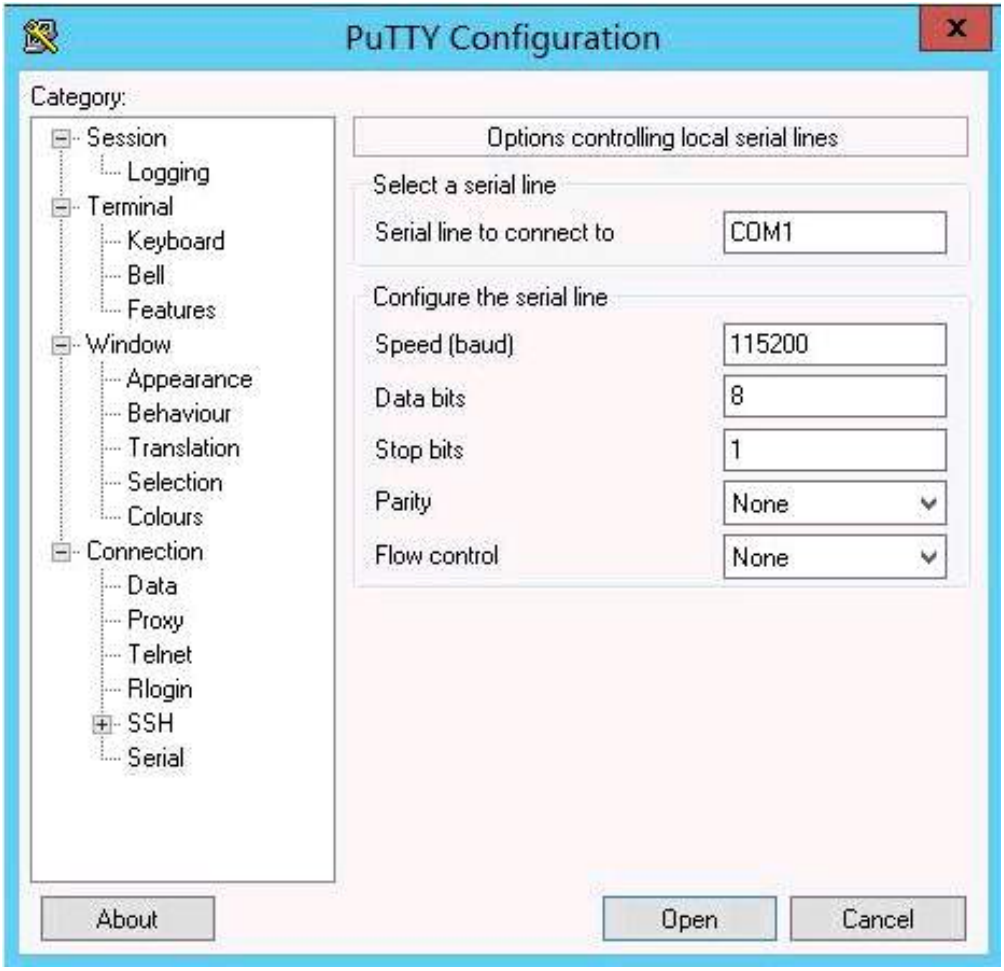


Step 5 Click **Open**.

Step 6 Run the **at** command on the **COM1-PuTTY**. If **OK** appears in the output, the GSM modem has connected to the host through the serial port. In this case, go to **Step 9**. If the system does not respond to the command, the GSM modem has been disconnected from the serial port. In this case, go to **Step 7**.

Step 7 Re-log in to the page for configuring the GSM modem, as shown in **Figure 5-20**.

Figure 5-20 Page for configuring the GSM modem



Step 8 Reset the baud rate of the GSM modem until running the **at** command responds with **OK**.

NOTE

- If the baud rate of the GSM modem is not confirmed, reconfigure it to ensure that the baud rate of the GSM modem and that of the serial port are consistent. In this condition, the PuTTY can be used to configure the GSM modem.
- The baud rate can be configured using the command **at+ipr=115200**.

Step 9 Configure other parameters, for example whether to reply automatically.

Step 10 Click **OK** to save and exit. Run the related commands to verify the configuration. The following is an example.

```
at
OK
at+ipr=115200
```



```
OK
ats0=1
OK
at&w
OK
```

Step 11 Upon successful configuration, connect the GSM modem to the serial port of the storage system for use.

NOTE

For details about configuring the GSM modem, see the corresponding manual supplied with the GSM modem.

----End

5.3.3 Managing Syslog Notification

You can modify the recipient server address, notification type, and alarm severity of Syslog notifications based on service requirements.

5.3.3.1 Modifying the Syslog Notification Policy

You can modify the Syslog notification type and severity based on service requirements.

Prerequisites

- You have enabled Syslog notification.
- You have logged in to DeviceManager as a super administrator or an administrator who has necessary operation permissions.
- For sending alarms to the Syslog server, a storage system only sends the alarms generated after the Syslog server is configured and does not send alarms generated before the configuration.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Alarm Settings** > **Alarm Notification** > **Syslog Notification**.

Step 3 Configure the Syslog notification type and severity. **Table 5-17** describes the parameters.

Figure 5-21 Syslog notification settings

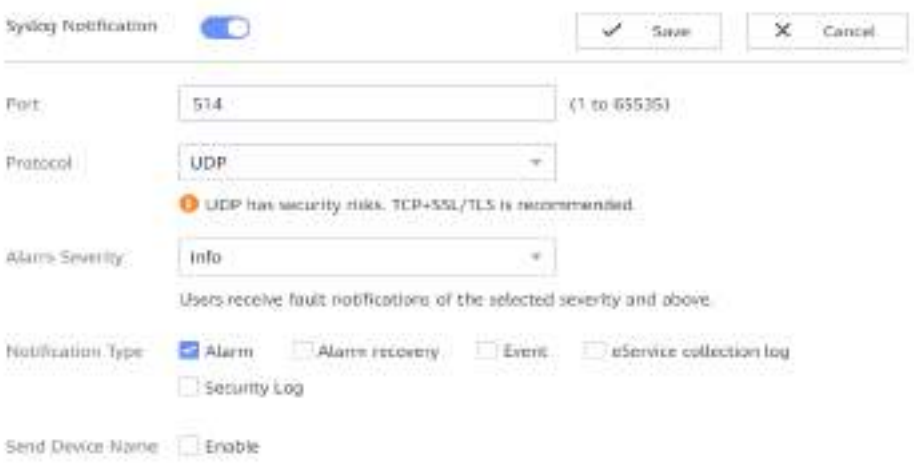


Table 5-17 Syslog notification parameters

Parameter	Description
Port	Syslog port number. The value ranges from 1 to 65535, and the default value is 514. **NOTE** The port number configured on the storage system must be consistent with that configured on the Syslog server.
Protocol	Protocol through which the Syslog notification is sent. Possible options are **UDP**, **TCP**, and **TCP+SSL/TLS**. The default value is **TCP+SSL/TLS**. **NOTE** • Ensure that the **UDP**, **TCP**, **TCP+SSL/TLS** protocols have been configured on the Syslog server. Security risks arise if **Protocol** is set to **UDP** or **TCP**. You are advised to select **TCP+SSL/TLS**. • The protocol configured on the storage system must be consistent with that configured on the Syslog server. • If you select **UDP**, ensure that the Syslog servers can properly respond to ping packets. – If all configured servers fail to respond to ping packets, the storage system will not send Syslog notifications. – If any server responds to the ping packets, the storage system sends Syslog notifications to all servers in sequence.
Alarm Severity	Indicates the lowest severity of a Syslog alarm that can be sent. Possible values are **Info**, **Warning**, **Major**, and **Critical**.
Notification Type	Possible values are **Alarm**, **Alarm recovery**, **Event**, **eService collection log**, and **Security Log**.

Parameter	Description
Send Device Name	Indicates whether the device name should be sent to the Syslog server. **NOTE** After **Send Device Name** is enabled, the system sends device names to the Syslog notification server. You can choose > **Device Information** to view device names.

Step 4 Click **Save**.

----End

5.3.3.2 Managing the Recipient Server Addresses of Syslog Notifications

The Syslog server can send device alarms to specified servers. You can modify the server addresses that receive Syslog notifications based on service requirements.

Prerequisites

- You have enabled Syslog notification.
- You have logged in to DeviceManager as a super administrator or an administrator who has necessary operation permissions.
- For sending alarms to the Syslog server, a storage system only sends the alarms generated after the Syslog server is configured and does not send alarms generated before the configuration.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Alarm Settings** > **Alarm Notification** > **Syslog Notification**.

Step 3 Manage the recipient server addresses of Syslog notifications. **Table 5-18** details the operations.

Figure 5-22 Recipient server address settings

Table 5-18 Relevant operations

Operation	Procedure
Adding an address	1. Specify the server address that you want to add. **NOTE** An IPv4 address has the following requirements: – The 32-bit address is evenly divided into four fields. Each 8-bit field is expressed in dotted-decimal. – Each field of the IP address cannot be blank and must be an integer. – The value of the first field ranges from 1 to 223 (excluding 127). – The values of other fields range from 0 to 255. – The IP address cannot be a special address such as the broadcast address. An IPv6 address has the following requirements: – The 128-bit address is evenly divided into eight fields. Each 16-bit field is expressed in hexadecimal and separated with colons. – In each 16-bit field, zeros before integers can be removed. However, at least one digit must be reserved in each field. – If the IP address contains a long string of zeros, you can represent the neighboring zeros with double colons (::) in the colon-separated hexadecimal field. Each IP address contains only one double-colon (::). The double-colons (::) can also be used to represent neighboring zeros of the IP address. – The IP address cannot be a special address such as network address, loop address, or multicast address. The domain name has the following requirements: – A domain name is not case-sensitive and must be an English domain name. – An English domain name contains 1 to 255 characters. – An English domain name can only contain letters (a to z and A to Z), digits (0 to 9), periods (.), and hyphens (-). It cannot start or end with a hyphen (-). 2. Click **Add**.
Removing a recipient server address	Select the recipient server addresses that you want to remove and click ×.

Step 4 **Optional:** Click **Test** to test the connectivity between the storage system and Syslog server.

Step 5 Click **Save**.

----End

5.3.4 Managing Trap Notification

You can modify the addresses that receive trap alarm notifications and events based on service requirements. The storage system's alarms and events will be

sent to the network management systems or other storage systems specified by the trap servers.

5.3.4.1 Managing SNMP Community Strings

If SNMPv1 or SNMPv2c is used, you must configure SNMP community strings on the storage system for interworking with a third-party network management tool. To ensure SNMPv1 and SNMPv2 protocol security, you are advised to maintain the SNMP community strings regularly.

Prerequisites

You have logged in to the CLI of the storage system.

You have enabled **SNMPv1&SNMPv2c**.

Context

If you use SNMPv1 or SNMPv2c, you must configure community strings. A third-party network management tool uses community strings to interwork with the SNMP service of the storage system.

On a storage system, the default SNMP read-only community string is **storage_public** and the default read-write community string is **storage_private**.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **SNMP Management** > **SNMP Protocol**.

Step 3 Click **Modify** on the right of **SNMP Protocol Settings**.

Step 4 Click **Modify** on the right of **Community**. **5.3.4.1-Managing SNMP Community Strings** describes the related parameters.

Table 5-19 Community parameters

Parameter	Description
Read Community	• Read community, which is used to read device information. • A read community must meet the security policy. For details, see **5.3.4.3 Managing the SNMP Security Policy**.
Confirm Read Community	Set it to the same value as **Read Community**.
Write Community	• Read-write community, which is used to read device information or configure a device. • A read-write community must meet the security policy. For details, see **5.3.4.3 Managing the SNMP Security Policy**.
Confirm Write Community	Set it to the same value as **Write Community**.
NOTE To ensure compatibility, the system supports SNMPv1 and SNMPv2c. However, to ensure data security, it is strongly recommended that you use SNMPv3.	

Step 5 Click **Save**.

Step 6 Use a third-party network management tool to check whether the newly configured community can be properly connected.

----End

5.3.4.2 Managing USM Users

If SNMPv3 is used, USM users are used to access upper-level external network management systems (such as the SNMP network management system). To ensure SNMPv3 protocol security, you are advised to maintain the USM user list regularly.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **SNMP Management** > **SNMP Protocol**.

Step 3 Manage USM users. **Table 5-20** details the operations.

Figure 5-23 USM user management

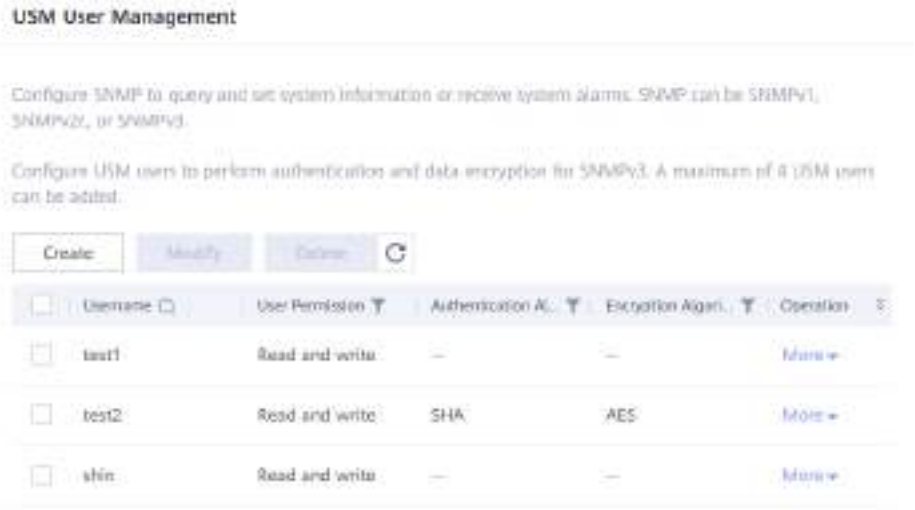


Table 5-20 Relevant operations

Operation	Procedure
Adding a USM user	1. Click **Create**. The **Create USM User** dialog box is displayed. 2. Set USM parameters. For related parameters, see **Table 5-21**. 3. Click **OK**. The USM user list displays the newly added USM user.
Modifying a USM user	1. Select the USM user that you want to modify and click **Modify**. The **Modify USM User** dialog box is displayed. 2. Modify USM parameters. **Table 5-21** describes the related parameters. 3. Click **OK**. The USM user list displays the modified USM user.
Removing a USM user	Select the USM user that you want to remove and click **Delete**.

Table 5-21 USM user parameters

Parameter	Description
Username	Name of a USM user. [Value range] **Username** is a 4- to 32-character string, can contain only letters, digits, underscores (_), and hyphens (-), and must start with a letter. [Example] usm001
User Permission	User level of a USM user. [Value range] • Read-only • Read and write
User Authentication	Whether to enable user authentication.
Authentication Algorithm	Authentication protocols of a USM user, include **MD5**, **SHA**, **SHA224**, **SHA256**, **SHA384** and **SHA512**. **NOTE** SHA is more secure than MD5. For security purposes, you are advised to select SHA for authentication.
Authentication Password	Authentication password of a USM user. [Default rules] The password must meet the following complexity requirements: • Contains 8 to 32 characters. • Must contain special characters. Special characters include !"#$%&'()*+,-./:;<=>?@[\]^`{_|}~ and spaces. • Must contain two types of the following characters: uppercase letters, lowercase letters, and digits. • Cannot be the same as the username or the username written backwards. **NOTE** You can modify the default rule. For details, see **5.3.4.3 Managing the SNMP Security Policy**. [Example] usmuser@123
Confirm Authentication Password	Confirming authentication password of a USM user. [Example] usmuser@123
Data Encryption	Whether to enable data encryption.

Parameter	Description
Encryption Algorithm	Encryption protocols of a USM user, including **3DES**, **DES**, **AES**, **AES192** and **AES256**. **NOTE** Security performance order of three encryption protocols is as follows: AES > 3DES > DES. For security purposes, you are advised to select AES.
Data Encryption Password	Password used by a USM user to encrypt data. [Default rules] The password must meet the following complexity requirements: • Contains 8 to 32 characters. • Must contain special characters. Special characters include !"#$%&'()*+,-./:;<=>?@[\]^`{_|}~ and spaces. • Must contain two types of the following characters: uppercase letters, lowercase letters, and digits. • Cannot be the same as the username or the username written backwards. **NOTE** You can modify the default rule. For details, see **5.3.4.3 Managing the SNMP Security Policy**. [Example] dataencrypt@123
Confirm Data Encryption Password	Confirm the data encryption password used by a USM user.

Step 4 Click **OK**.

Step 5 Click **Save**.

----End

5.3.4.3 Managing the SNMP Security Policy

The storage system allows you to modify the security policy about the SNMP service to improve the SNMP service security.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **SNMP Management** > **SNMP Security Policy**.

Step 3 Click **Modify**. Table 5-22 describes the related parameters.

Table 5-22 SNMP security policy parameters

Parameter	Description
Min. Password Length	Minimum length of the community and USM user password. [Value range] Its value is an integer ranging from 8 to 32.
Max. Password Length	Maximum length of the community and USM user password. [Value range] Its value is an integer ranging from 8 to 32.
Password Complexity	Complexity of the community and USM user password. [Value range] • High: containing at least one special character (!"#$%&'()*+,-./:;<=>?@[\]^`{_\|}~ and space), uppercase letter, lowercase letter, and digit • Medium: containing at least one special character (!"#$%&'()*+,-./:;<=>?@[\]^`{_|}~ and space) and two of the following types: uppercase letter, lowercase letter, and digit • Low: containing at least one of the following types: special character (!"#$%&'()*+,-./:;<=>?@[\]^`{_|}~ and space), uppercase letter, lowercase letter, and digit
Password Policy	• Allow the authentication password and data encryption password to be the same: if this parameter is selected, the authentication password and data encryption password of the USM user can be the same. • Allow the USM username and password to be the same: if this parameter is selected, the password of the USM user can be the same as the USM username and the reverse order of the USM user name.

Parameter	Description
Community Strings Policy	Set different read and write community strings: if this parameter is selected, the read community and read-write community cannot be the same.
Statistic Collection Interval of Authentication Failures (s)	Interval for collecting statistics about the number of consecutive authentication failures. [Value range] Its value is an integer ranging from 1 to 600, in units of seconds.
Allowed Consecutive Authentication Failures	Allowed number of consecutive authentication failures. [Value range] Its value is an integer ranging from 3 to 100.
IP Address Lockout Time (s)	Length of time for locking the network management software's IP address. [Value range] Its value is an integer ranging from 10 to 3600, in units of seconds.

Step 4 Click **Save**.

----End

5.3.4.4 Managing Trap Server Addresses

To ensure that the storage system's alarms and events can be sent to the application servers or maintenance terminals specified by the trap servers in a timely manner, you are advised to maintain the trap server addresses regularly.

Prerequisites

- The SNMP service has been enabled on the storage system. If the service has not been enabled, run the **change snmp status** command in the developer view to enable it. For details about how to use the command, see the *Advanced O&M Command Reference*.
- The server has enabled the SNMP service.
- The USM user has been created.
- For sending alarms to the trap server, a storage system only sends the alarms and events generated after the trap server is configured and does not send alarms and events generated before the configuration.
- Before configuring a domain name for the server, ensure that the DNS server can communicate normally with the storage array or third-party server.
- If the server address is not on the management network segment, configure routes to interconnect the storage devices with the servers linked to the server addresses.

NOTICE

Before changing server addresses, ensure that no alarm message or event is being reported to network management systems or storage devices linked to those addresses. Alarm messages being reported at the time of the change will be lost.

Context

- Trap is a Simple Network Management Protocol (SNMP) message type used to indicate the occurrence of an event. This type of message is sent to a recipient through User Datagram Protocol (UDP), which is not fully reliable. Specify trap service addresses if SNMP is used to report alarms and events. After a trap server IP address is configured, alarm and event notifications will be sent to the specified application servers or maintenance terminals.
- DeviceManager provides the trap function to send the alarms and events of managed storage devices to another network management system or to a device at a specific server address. If alarms and events are reported in SNMP mode, you must configure Trap server addresses.

NOTE

To enable the trap function, install the **MIB** interface files on application servers. For details, you can log in to Huawei's technical support website (**https://support.huawei.com/enterprise/**) and enter the product model and document name in the search box to search for, browse, and download the desired *MIB Interface Files* of the corresponding product model.

- To report alarms and events to other network management systems or storage devices, add or change the existing server addresses to the server addresses of those systems or devices.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Alarm Settings** > **Alarm Notification**.

Step 3 Manage trap server addresses. **Table 5-23** details the operations.

Figure 5-24 Trap server address management area

Table 5-23 Relevant operations

Operation	Procedure
Adding a server IP address	1. Click **Add**. The **Add Trap Server** dialog box is displayed. 2. Set the parameters for creating trap server addresses. **Table 5-24** lists related parameters. 3. Click **OK**. The server list displays the newly added server IP address.
Modifying a server IP address	1. In the trap server address list, select the trap server address that you want to change and click **Modify**. The **Modify Trap Server** dialog box is displayed. 2. Change the trap server addresses. **Table 5-24** lists related parameters. 3. Click **OK**. The server list displays the modified server IP address.
Removing a server IP address	In the list, select a server address that you want to remove and click **Remove**.

Table 5-24 Server address parameters

Parameter	Description
Server IP Address	The address of a network management system or storage device for receiving alarms and events. [Value range] The value can be an IP address or a domain name. ● An IPv4 address has the following requirements: – The 32-bit address is evenly divided into four fields. Each 8-bit field is expressed in dotted-decimal. – Each field of the IP address cannot be blank and must be an integer. – The value of the first field ranges from 1 to 223 (excluding 127). – The values of other fields range from 0 to 255. – The IP address cannot be a special address such as a network address or broadcast address. ● An IPv6 address has the following requirements: – The 128-bit address is evenly divided into eight fields. Each 16-bit field is expressed in hexadecimal and separated with colons. – In each 16-bit field, zeros before integers can be removed. However, at least one digit must be reserved in each field. – If the IP address contains a long string of zeros, you can represent the neighboring zeros with double colons (::) in the colon-separated hexadecimal field. Each IP address contains only one double-colon (::). The double-colons (::) can also be used to represent neighboring zeros of the IP address. – The IP address cannot be a special address such as network address, loop address, or multicast address. ● A domain name has the following requirements: – Be case-insensitive and must be an English domain name. – Contains 1 to 255 characters. – Only contains letters, digits, periods (.), and hyphens (-), and not start or end with a hyphen (-). [Example] 192.168.100.11 fc00::1234

Parameter	Description
	domain.com
Port	Server port information. [Value range] 1 to 65535 [Example] 2234
Version	Server version information. The possible value can be **SNMPv1**, **SNMPv2c**, or **SNMPv3**. **NOTE** To ensure the data security, you are advised to use SNMPv3. [Example] SNMPv3
USM User	The user that reports alarms and events from SNMP. [Example] usm001
Type	Type of an alarm and event sent by a storage device to the trap server. • Parsed: alarms and events that have been resolved. • Original: alarms and events that have not been resolved. • Parsed time string: parsed alarms and events whose IDs correspond to the same OID. The data type of event fields generated by alarms or events is OCTET STRING. • Original time string: original alarms and events that have not been parsed. The data type of alarm or event occurring time (character string) and clearing time (character string) is OCTET STRING. • All: all alarms including the **Parsed** and **Original** alarms and events. [Example] Parsed

Step 4 Click **OK**.

Step 5 Click **Save**.

----End

Follow-up Procedure

A storage device can send multiple types of alarms and events to the trap server and each alarm has its own push format. For details, you can log in to Huawei's

technical support website (**https://support.huawei.com/enterprise/**) and enter the product model and document name in the search box to search for, browse, and download the desired *MIB Interface Files* of the corresponding product model.

5.3.5 Managing the Notification Sending Cycle and Customer Information

This section describes how to set a notification sending cycle. Emails, SMS messages, and syslogs are sent to the remote maintenance center according to the specified cycle to help monitor the current system status.

Prerequisites

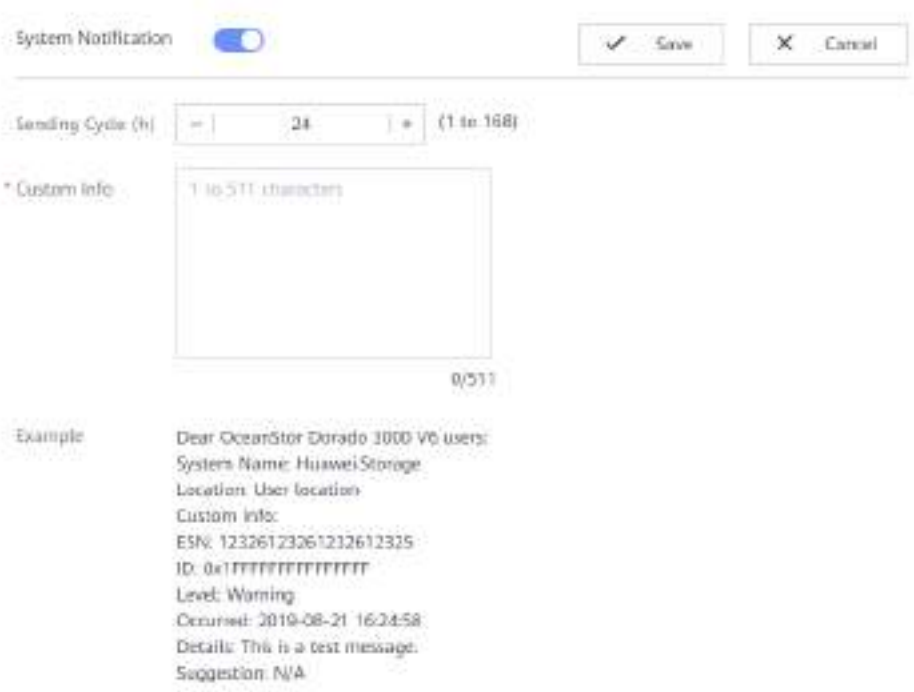
- The email notification, SMS notification, and Syslog notification functions are correctly set.
- The system notification function has been enabled.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings > Alarm Settings > Alarm Notification > System**.

Step 3 Click **Modify** to set the notification sending cycle and customer information.



1. Set **Sending Cycle (h)** to an integer ranging from 1 to 168. The unit is hour.
2. In the **Customer Information** text box, enter the customer's company name and contact information to help maintenance engineers locate faults more easily.

NOTE

The **Customer Information** text box allows you to enter 1 to 511 characters. The value cannot contain single quotation marks (').

Step 4 Click **Save**.

----End

5.3.6 Managing Alarm Dump

After you enable the alarm dump function, alarm messages will be dumped automatically to a specific FTP or SFTP server when they exceed a system-definable threshold.

5.3.6.1 Configuring an FTP Server

FTP servers store alarm files dumped from storage systems. You are required to re-configure an FTP server due to services change. You can install and configure a wide range of FTP servers.

Prerequisites

- The FTP server software installation package is ready.
- The IP address to be configured can properly communicate with the storage system.
- This section describes how to configure an Xlight FTP server. For details about how configure other FTP servers, see the related configuration documentation.

Procedure

Step 1 Start the Xlight FTP server software.

The **Xlight FTP Server** page is displayed.

Step 2 Configure a virtual server.

1. On the **Xlight FTP Server** page, click  .
   The **New Virtual Server** dialog box is displayed.
2. In the **New Virtual Server** dialog box, set **IP Address**, **Port**, and **Protocol** to the local IP address, **21**, and **FTP**, respectively.
3. Click **OK**.
   The added virtual server is displayed in the **Xlight FTP Server** page that is displayed.

Step 3 Start the virtual server.

Select the added virtual server and click  to start the server.

NOTE

You can select the added virtual server, right-click, and choose **Start Server** to start the server.

Step 4 Add a user.

1. On the **Xlight FTP Server** page, click  .
   The user list is displayed.
2. Click  .
   The adding users dialog box is displayed.
3. In the dialog box, enter **Username** and **Password** and set **Home Directory**.
4. Click **OK**.
   The user is added, and user information is displayed on the user page.

Step 5 Set virtual directory permissions.

1. In the user list, select the added user and click  .
   The user name page is displayed.
2. On the navigation bar on the left, click  .
   The user directory management page is displayed.
3. Select the access directory of the added user and click  .
   The **Virtual Directory** dialog box is displayed.
4. In the **Permission** area, set permissions.
5. Click **OK**.
   Virtual directory permissions are configured.

----End

5.3.6.2 Modifying Alarm Dump Settings

This section describes how to modify alarm dump settings. You can modify the alarm dump settings based on service requirements to ensure the integrity of alarm information recorded by a storage system.

Prerequisites

- The alarm dump function has been enabled.
- If alarm information is stored on an FTP server, communication must be normal between the server and the storage system. To improve communication reliability, you are advised to configure them both on the same LAN and their IP addresses in the same network segment.
- If alarm information is stored on an SFTP server, communication must be normal between the server and the storage system. To improve communication reliability, you are advised to configure them both on the same LAN and their IP addresses in the same network segment.
- If alarm information is stored on an FTP server and a firewall is configured on the network, port 21 is enabled.
- If alarm information is stored on an SFTP server and a firewall is configured on the network, port 22 is enabled.

- Before configuring a domain name for the server, ensure that the DNS server can communicate normally with the storage array or third-party server.

Context

- If the number of alarms, operation logs, or run logs generated by the storage system where alarm dump is not configured exceeds 45,000, the alarm **The Space That Stores Event Logs Is To Be Used Up** will be generated. If the number of alarms, operation logs, or run logs generated by the storage system reaches the upper limit of 50,000, the earliest 10,000 alarms, operation logs, or run logs will be automatically deleted.
- After alarm dump is configured on the storage system:
  - If the number of alarms, operation logs, or run logs generated by the storage system exceeds 45,000, the alarm **The Space That Stores Event Logs Is To Be Used Up** will not be triggered. If the number of alarms, operation logs, or run logs generated by the storage system reaches the upper limit of 50,000, the earliest 10,000 alarms, operation logs, or run logs are automatically dumped to the specified FTP or SFTP server.
  - If the number of login and logout logs generated by the storage system exceeds 20,000, the earliest 10,000 logs will be automatically dumped to the specified FTP or SFTP server.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Alarm Settings > Alarm Dump**.

Step 3 Click **Modify** to modify parameters for the alarm dump. **Table 5-25** lists related parameters.

Figure 5-25 Page for alarm dump settings

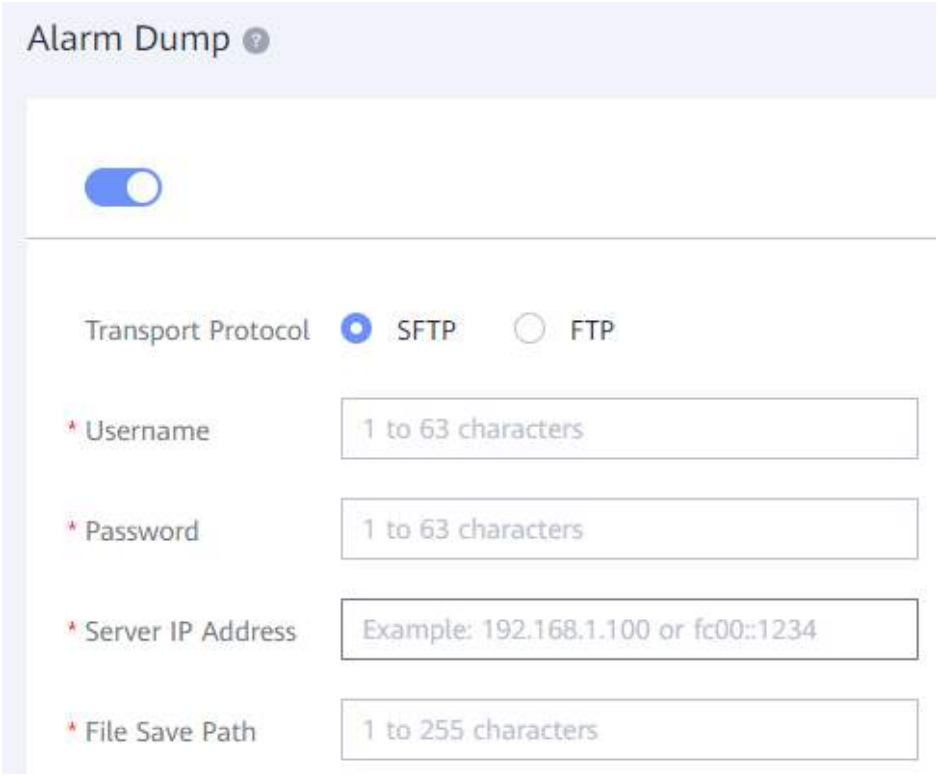


Table 5-25 Parameters for the alarm dump

Parameter	Description
Transport Protocol	The transport protocol of the alarm dump. The values are **SFTP** or **FTP**. **NOTE** To ensure the security of data transfer, you are advised to use Secure File Transfer Protocol (SFTP). [Example] FTP
Username	Name of the user on the server that will be used to store the alarm information. [Value range] • The username must contain 1 to 63 characters. • The username cannot contain single quotation marks ('). [Example] files

Parameter	Description
Password	Password for logging in to a server. [Value range] The value must contain 1 to 63 characters. [Example] 123456
Server IP Address	IP address of a server. [Value range] ● An IPv4 address has the following requirements: – The 32-bit address is evenly divided into four fields. Each 8-bit field is expressed in dotted-decimal. – Each field of the IP address cannot be blank and must be an integer. – The value of the first field ranges from 1 to 223 (excluding 127). – The values of other fields range from 0 to 255. – The IP address cannot be a special address such as the broadcast address. ● An IPv6 address has the following requirements: – The 128-bit address is evenly divided into eight fields. Each 16-bit field is expressed in hexadecimal and separated with colons. – In each 16-bit field, zeros before integers can be removed. However, at least one digit must be reserved in each field. – If the IP address contains a long string of zeros, you can represent the neighboring zeros with double colons (::) in the colon-separated hexadecimal field. Each IP address contains only one double-colon (::). The double-colons (::) can also be used to represent neighboring zeros of the IP address. – The IP address cannot be a special address such as network address, loop address, or multicast address. [Example] 192.168.1.100 fc00::1234

Parameter	Description
File Save Path	Path to a directory for storing dumped performance monitoring data. To enable this parameter, you must set up a path and create a folder under it, and type the name of the folder in **File Save Path** on DeviceManager. [Value range] A file save path must contain 1 to 255 characters. [Example] If you set the path to **G:** and create a folder named **alarm** on the FTP server, type **alarm** in **File Save Path**.

Step 4 **Optional:** Click **Test** to verify parameter values.

- If an error dialog box is displayed, at least one parameter value is incorrect. Modify the parameter and retry.
- If a success dialog box is displayed, the alarm dump parameters have been configured correctly.

Step 5 Click **Save**.

----End

5.3.7 Managing Alarm Masking

After alarm masking is enabled or disabled for a device, the device will not or will report its alarms to the network management system.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Alarm Settings** > **Alarm Masking**.

Step 3 View all alarms in the system. **Table 5-26** describes the parameters.

Table 5-26 Alarm masking parameters

Parameter	Description
Name	Name of an alarm. **NOTE** Some alarms have the same name but different IDs. When setting alarm masking, set all alarms with the same name.
Alarm ID	ID of an alarm.
Object	Type of the object for which the alarm is generated.
Severity	Alarm severity. Possible values are **Critical**, **Major**, **Warning**, and **Info**.
Alarm Masking	Whether alarm masking is enabled.
Unhandled Alarms	Indicates whether an alarm is unhandled.

NOTE

- Select one or more alarms and click **Enable**. The system will not report the selected alarms.
- Select one or more alarms and click **Disable**. The system will not mask the selected alarms.

----End

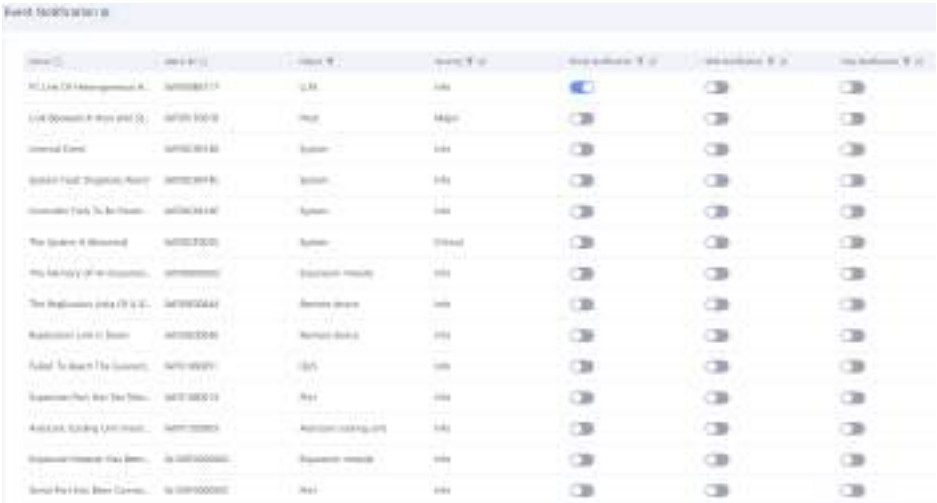
5.3.8 Managing Event Notification

After setting email, SMS, and trap notification for events, you can enable or disable these notification methods for the events.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Alarm Settings** > **Event Notification**.



Step 3 Click under a notification mode for an event to enable this mode.

NOTE

- After email notification is enabled, the system will send event information to recipient email addresses configured in the **Email Notification** area on the **Alarm Notification** page. If event notification is disabled for the recipient email addresses in the **Email Notification** area on the **Alarm Notification** page, the system will not send the event information.
- After SMS notification is enabled, the system will send event information to recipient phone numbers configured in the **SMS Notification** area on the **Alarm Notification** page. If event notification is disabled for the recipient phone numbers in the **SMS Notification** area on the **Alarm Notification** page, the system will not send the event information.
- After trap notification is enabled, the system will send event information to trap servers through server addresses configured in the **Trap** area on the **Alarm Notification** page using SNMP Trap mode.
- Click under a notification mode for an event to disable this mode.

----End

5.3.9 Modifying the Alarm Severity

This section describes how to modify the severity of an alarm.

Procedure

Step 1 Choose **Settings** > **Alarm Settings** > **Alarm Severity**.

Step 2 View the alarms that may be generated in the system and their severities. **Table 5-27** describes the parameters.

Table 5-27 Alarm parameters

Parameter	Description
Name	Name of an alarm. **NOTE** Some alarms have the same name but different IDs. When setting alarm severities, set all alarms with the same name.
Alarm ID	ID of an alarm.
Object	Type of the object for which an alarm is generated.
Severity	Severity of an alarm. Possible values are **Critical**, **Major**, **Warning**, and **Info**.

Step 3 Modify the severity of an alarm.

1. Select the desired alarm and click **Modify Alarm Severity**.
   The **Modify Alarm Severity** page is displayed on the right.
2. In **Alarm Severity**, select a severity.
3. Click **OK**.

Confirm your operation as prompted.

----End

5.4 Viewing Historical Tasks

This section describes how to view information about tasks in a storage system.

Context

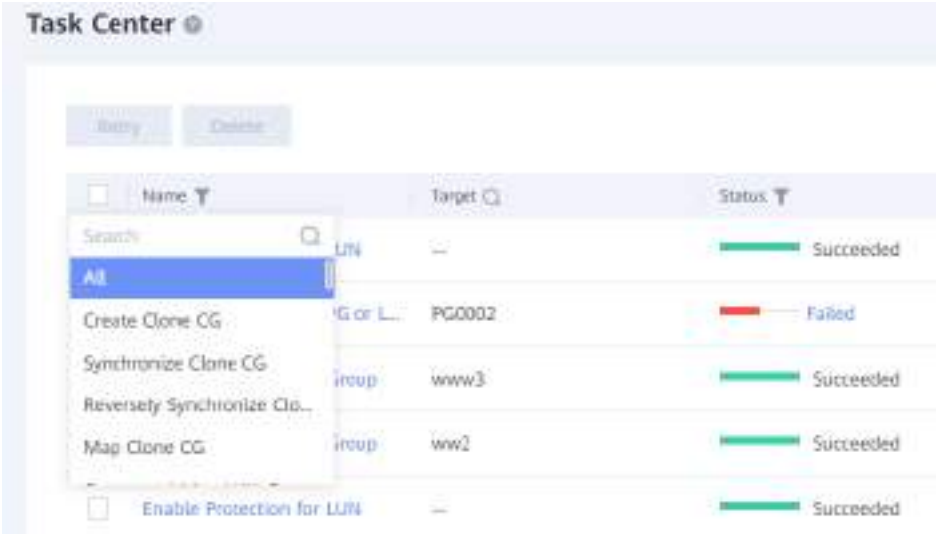
- For this version, vStore administrators can view historical tasks in the system.
- The system administrator can view historical tasks of all vStores. A vStore administrator can view only historical tasks of the vStores it manages.

Procedure

Step 1 Choose **Insight** > **Task Center**.

Step 2 Select a type of task information.

1. Click next to **Name**. In the drop-down list, you can view the types of task information supported by the storage system.
2. Select a type of task information from the drop-down list.



Step 3 View task information of the system listed in **Table 5-28**.

Table 5-28 Task parameters

Parameter	Description
Name	Name of a task.
Target	Object of a task.
Status	Current task status.
vStore Name	Name of a vStore.

Parameter	Description
Creator	Task creator.
Start Time	Task start time.
End Time	Task end time.
Duration	Task duration.

NOTE

- You can click the name of a task to view its details.
- You can click to select desired task parameters to be displayed on the menu bar.

Step 4 You can also perform the following operations on tasks:

- Retrying a task
  a. Select a task whose **Status** is **Failed**, and click **Retry**.

     NOTE

     You can also click **More** on the right of the desired task and select **Retry**.

  b. Confirm your operation as prompted.
- Deleting a task
  a. Select a task whose **Status** is **Succeeded**, **Failed**, **Waiting**, **Rollback succeeded**, or **Rollback failed**, and click **Delete**.

     NOTE

     You can also click **More** on the right of the desired task and select **Delete**.

  b. Confirm your operation as prompted.

----End

5.5 Configuring and Managing eService

eService enables a storage system to upload its alarms and logs to the eService cloud system. The eService cloud system then uses AI technologies to implement intelligent fault reporting, real-time health analysis, intelligent fault prevention, and intelligent optimization, minimizing device running risks and reducing operational costs.

5.5.1 About eService

eService enables a storage system to upload its alarms and logs to the eService cloud system. The eService cloud system then uses AI technologies to implement intelligent fault reporting, real-time health analysis, intelligent fault prevention, and intelligent optimization, minimizing device running risks and reducing operational costs.

Positioning

Traditionally, alarms and logs are manually collected from storage systems and cannot be sent to Huawei technical support center in a timely manner. As a result, faults cannot be discovered promptly. The eService enables a storage system to periodically report alarms and logs. This helps eService analyze storage system's health status in real time, identify potential risks, automatically locate faults, and provide troubleshooting solutions, facilitating fault discovery and shortening troubleshooting time.

The eService securely connects a storage system and the eService cloud system remotely deployed in Huawei technical support center.

- The storage system encrypts alarms and logs and sends them to eService through encrypted channels over Internet. eService can receive alarm and log information from storage systems on a 24/7 basis, create orders within minutes, and automatically notify Huawei technical support personnel of exceptions in a timely manner.
- Uploading of system logs must be manually configured. After technical support personnel configure system log collection tasks for a storage system on eService, the storage system periodically sends requests to eService for uploading system logs. If the eService is enabled, the storage system can upload collected system logs.

Huawei eService can be deployed on DeviceManager or eService Client. This section describes how to deploy eService on DeviceManager. For details about how to deploy eService on eService Client, see the *eService Client User Guide*.

The eService uses the secure Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS). The eService allows a storage system to communicate with eService directly or through an internal HTTP proxy server. **Figure 5-26** and **Figure 5-27** illustrate the two types of networking.

Figure 5-26 Direct-connection networking

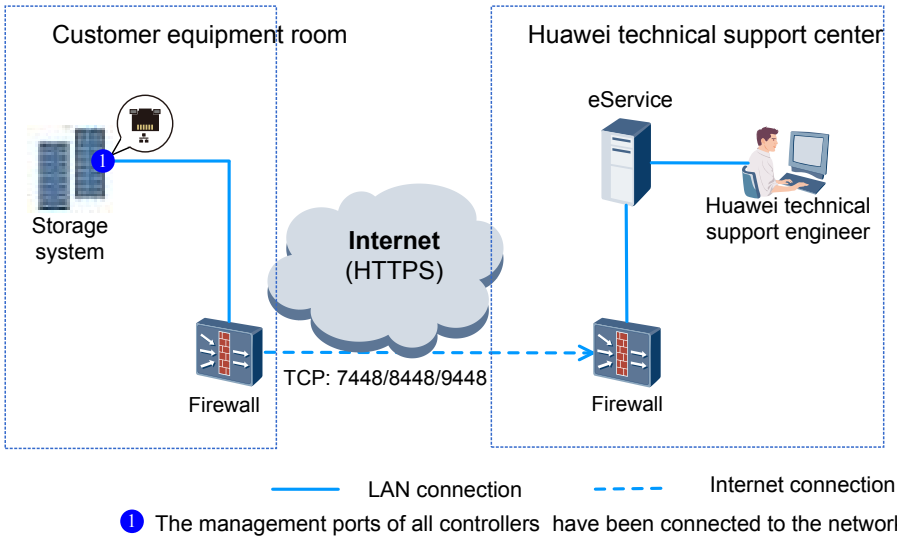
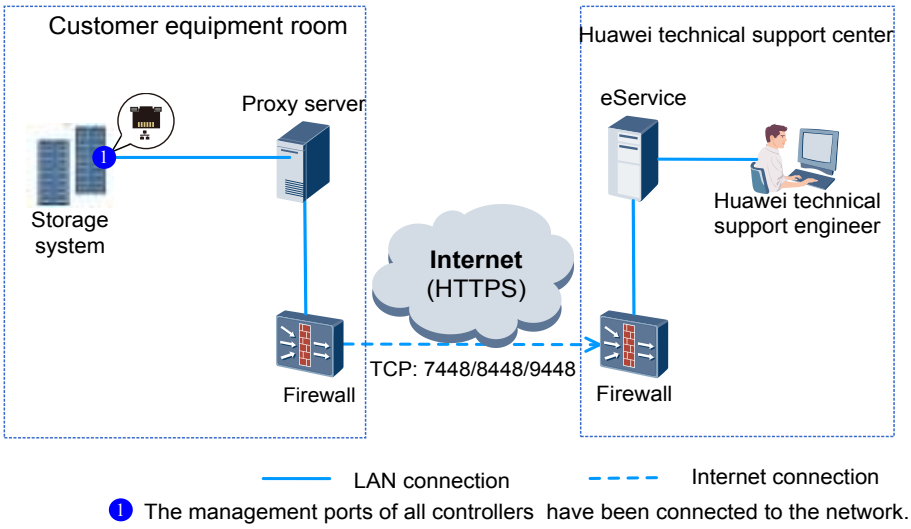


Figure 5-27 Internal HTTP proxy server deployed



NOTE

- If an internal HTTP proxy server is deployed for network access, ensure that the server is secure and reliable.
- If neither of these two types of networking is supported, the eService Client can be deployed to upload storage alarms and logs to eService. For details, see the *eService Client User Guide*.

Supported Data Types

After the eService is enabled, alarms and logs of storage systems can be uploaded to Huawei technical support center. **Table 5-29** describes the data.

Table 5-29 Supported data types

Data Type	Description	Uploading Interval
Performance log	• A **.txt** file in the JSON format • Performance logs of disks, controllers, LUNs, front-end ports, and storage pools	New performance logs are uploaded to eService every 5 minutes.

Data Type	Description	Uploading Interval
Operation log	• A **.txt** file in the JSON format • Operation logs about device status and function modules. Function modules include controllers, enclosures, power supplies, BBUs, fans, disks, cascade modules, interface modules, ports, storage pools, and LUNs.	Operation logs are uploaded to eService every 24 hours.
Alarm information	• A **.txt** file in the JSON format • HTTP POST request, with the media type being **application/json** • Alarm information including the alarm ID, serial number, severity, parameters, time, and type	Uploaded periodically. • File New alarm information is uploaded to eService every 5 minutes. • HTTP POST request New alarm information is uploaded to eService every minute.
System log	• A **.tgz** file • System logs including configuration information, event information, and debug logs about the storage system	Huawei technical support engineers manually trigger the uploading of system logs from eService to Huawei technical support center. In the current version, all system logs and system logs in the latest one hour, latest two hours, latest 24 hours, or a specific time period can be uploaded.
Diagnosis file	• A **.tgz** file • Diagnosis file including device fault information	• If alarms are generated on a storage system, the storage system uploads a diagnostic file at the maximum frequency of one time per hour. • If no alarm is generated on a storage system, the storage system uploads a diagnostic file every 24 hours.

Data Type	Description	Uploading Interval
DHA operation log	• A **.tgz** file • DHA operation logs record daily operation information about disks, including health statistics, self-monitoring, analysis, and reporting technology (SMART), I/O statistics, and disk life information.	New DHA operation logs are uploaded to eService every 5 minutes.

NOTE

- The performance logs uploaded a time must not exceed 5 MB.
- The DHA operation logs uploaded a time per controller must not exceed 2 MB.
- There is no limit on the size of alarms, operation logs, system logs, and diagnosis logs to be uploaded.

5.5.2 Preparations

The following table describes preparations that you are advised to make before configuring the eService.

Item	Description
Obtaining the Equipment Serial Number (ESN) and site name of a storage device	When configuring eService on DeviceManager, you need to enter the ESN and site name of the storage device. You can obtain the ESN based on either of the following procedures: • On the navigation bar of DeviceManager, click **Home**. In the function pane, locate **SN** in the **Basic information** area. • Log in to the command-line interface (CLI). Run the **show system general** command and locate **SN**.
Preparing the network	The network bandwidth is greater than or equal to 10 Mbit/s.
Enabling ports 7448/TCP, 8448/TCP, and 9448/TCP on the firewall to allow outgoing traffic from the firewall to the Internet	The eService cloud system uses server ports 7448/TCP, 8448/TCP, and 9448/TCP. Enable the three ports on the firewall to allow storage systems to send HTTP requests to the eService cloud system.

Item	Description
(Optional) Obtaining the address, port, user name, and password of the HTTP proxy server	This information is required if an internal HTTP proxy server is used for network access.
Obtaining a Support account and password	During eService configuration, a Support account is required for device authentication. Apply for an account at the Support website if you do not have one.
Obtaining contact details about Huawei technical support center	After configuring eService on DeviceManager, contact Huawei technical support center for eService authentication so that a ticket is automatically created for an alarm. To obtain contact details about Huawei technical support center: • Carrier users: **https://support.huawei.com/carrier/docview!docview?nid=IN0000034614&path=NN-000005#click=myApply** • Enterprise users: **https://e.huawei.com/en/service-hotline**
Customer code	When performing eService authentication, technical support center personnel need to enter the customer code.

5.5.3 Configuring the eService

This section describes how to prepare and configure eService.

Prerequisites

Ports 7448/TCP, 8448/TCP, and 9448/TCP have been enabled on the firewall, which are used by the eService server to receive HTTP requests from the storage system.

Procedure

Step 1 Choose **Settings** > **eService Settings**.

NOTE

- When you access the **eService Settings** page for the first time, the system prompts the **eService Connection Statement** dialog box. Confirm the information in the dialog box, select **I have read and understand the consequences associated with performing this operation**, and click **OK**. If you click **Cancel**, eService cannot be configured. In this case, if you enable **Connect to eService and support OTA upgrades** or when you enter the **eService Settings** page next time, you can re-confirm the information after the **eService Connection Statement** dialog box is displayed.
- If **Connect to eService and support OTA upgrades** is enabled, you can click the eService icon in the upper right corner to access the eService official website.

Step 2 Enable **Connect to eService and support OTA upgrades**.

NOTE

If **Connect to eService and support OTA upgrades** has been enabled, click **Modify** in the upper right corner directly.

Step 3 Click **Modify**.

Step 4 Select the eService site to which the storage system data will be sent. **Table 5-30** describes the sites.

Table 5-30 eService sites

Site Name	Application Scenario
Carrier in Chinese mainland	Carriers in the Chinese mainland. **NOTE** If you select this site, the device information collected by eService will be sent to the cloud in China.
Carrier outside Chinese mainland	Carriers outside the Chinese mainland. **NOTE** • If you select this site, the device information collected by eService will be sent to the cloud in Germany. • For carriers in Hong Kong, Macao, and Taiwan regions, select this site.
Enterprise in Chinese mainland	Enterprises in the Chinese mainland. **NOTE** If you select this site, the device information collected by eService will be sent to the cloud in China.
Enterprise outside Chinese mainland	Enterprises outside the Chinese mainland. **NOTE** • If you select this site, the device information collected by eService will be sent to the cloud in Germany. • For enterprises in Hong Kong, Macao, and Taiwan regions, select this site.

Step 5 Configure the connectivity between the storage system and external networks.

1. Click **Configure Network**.

   The **Configure Network** page is displayed.

2. (Optional) Configure a proxy server.

   If a storage system accesses the Internet through the internal HTTP proxy, a proxy server must be configured. **Table 5-31** describes the parameters.

Table 5-31 Proxy server parameters

Parameter	Description
Proxy Server	Indicates whether to enable the proxy server. [Value range] Select or deselect the **Enable** check box. [Example] Select **Enable**.
HTTP Proxy Server Address	Address of the HTTP proxy server. [Value range] The value can be an IPv4 address or a domain name. – In the event of using an IPv4 address: ▪ A 32-bit IPv4 address is divided into four 8-bit fields that are expressed in dotted decimal notation. ▪ Each field of the IPv4 address must be an integer. ▪ The value of the first field ranges from 1 to 223. ▪ The values of the other fields range from 0 to 255. ▪ The IP address cannot be a special address such as the broadcast address. – In the event of using a domain name: ▪ A domain name is case-insensitive and must use the English alphabet. ▪ A domain name contains 1 to 255 characters. ▪ A domain name can only contain letters (a to z and A to Z), digits (0 to 9), periods (.), and hyphens (-), and cannot start or end with a hyphen (-).
Port	Port number of the HTTP proxy server. [Value range] 1 to 65535
Username	User name of the HTTP proxy server. [Value range] – A user name contains 1 to 63 characters. – A user name cannot contain single quotation marks ('').

Parameter	Description
Password	Password of the user. [Value range] A password contains 1 to 63 characters.

3. (Optional) Configure the DNS server.

   After the DNS service is configured, the storage system can resolve and access external domain names.

   NOTE

   - If direct connections are used (without using the customer's internal HTTP proxy), configure the DNS service. The common IP addresses of external DNS servers are 8.8.8.8 and 114.114.114.114.
   - If the customer's internal HTTP proxy is used and the proxy address is a domain name, configure the DNS service.
   - If the customer's internal HTTP proxy is used and the proxy address is an IP address, you do not need to configure the DNS service.
   - Ensure that the configured DNS server can resolve external domain names.

   a. Set **Active DNS IP Address**.
   b. (Optional) Set **Standby DNS IP Address 1**.
   c. (Optional) Set **Standby DNS IP Address 2**.

      NOTE

      Set **Standby DNS IP Address 1** first and then **Standby DNS IP Address 2**.

4. Click **OK**.

   The network configuration is complete.

Step 6 Enter a site name.

NOTE

- The site name contains 1 to 127 characters.
- The site name can contain only letters, digits, underscores (_), hyphens (-), periods (.), and spaces.

Step 7 Obtain, import, and activate an authorization letter.

NOTE

- The authorization letter will be uploaded to eService for archiving.
- If the scanned copy or photo of the authorization letter cannot be uploaded through DeviceManager, send the authorization letter to the eService mailbox for archiving after the authorization letter is signed. To obtain the eService mailbox, see **Configuring the eService** in the *Administrator Guide*.

1. Click **Obtain Template**.

   The page for downloading the *Authorization Letter for Deploying eService and Processing [Customer]'s Network Data* is prompted.

2. Download the authorization letter, fill in it, and then save it in the ***.jpg** format by photographing or scanning.

3. Click ..., select the authorization letter in the ***.jpg** format, and click **Open**.

Step 8 Set the transmission protocol.

1. Click **Modify**

   The **Modify Transport Protocol** page is displayed.

2. Select a transport protocol, which can be **HTTPS** or **SMTP**.

   If **SMTP** is selected, you need to set the SMTP server. You can click **Configure Email Service** to set the SMTP server.

   If **SMTP** is selected, you can set **eService Data Recipient Address**. After a backhaul email address is configured, the system sends device data to the email address when uploading device data to eService. You can add, modify, test, and remove the email address.

   - Add an email address.

     NOTE

     The recipient email address contains 1 to 255 characters.

     i. Click **Add**.

     ii. Enter the recipient email address in the text box of **Recipient Email Address**.

     iii. Click ✓.

   - Modify an email address.

     i. Click ✎ on the right of the desired recipient email address.

     ii. Enter the recipient email address in the text box of **Recipient Email Address**.

     iii. Click ✓.

   - Delete an email address.

     Click 🗑 on the right of the desired recipient email address.

   - Test an email address.

     Select the configured recipient email address and click **Test**. The system sends a test email to the email address. After the test email is sent successfully, check whether the SMTP server or other network management systems (NMSs) receive the test email. If not, check whether the network configuration is correct.

Step 9 Set contacts. You can add, modify, and remove contacts.

- To add a contact

  NOTE

  A contact is an administrator of the storage device in eService who can receive notifications from eService.

  a. Click **Add**.

  b. Set the contact information listed in **Table 5-32**.

Table 5-32 Contact parameters

Parameter	Description
First Name	■ The name contains 1 to 63 characters. ■ The name contains only letters, digits, underscores (_), hyphens (-), and periods (.).
Last Name	■ The name contains 1 to 63 characters. ■ The name contains only letters, digits, underscores (_), hyphens (-), and periods (.).
Email Address	Email address for receiving messages from eService.
Country Code	■ International area code of the country where the phone number that receives messages from eService is located. ■ The value can contain only digits, asterisks (*), pound signs (#), plus signs (+), brackets, and hyphens (-).
Phone	■ Phone number used to receive messages from eService. ■ The value can contain only digits, asterisks (*), pound signs (#), plus signs (+), brackets, and hyphens (-).

c. Click .

- To modify a contact

a. Click on the right of the desired contact.

b. Set the contact information listed in **Table 5-33**.

Table 5-33 Contact parameters

Parameter	Description
First Name	■ The name contains 1 to 63 characters. ■ The name contains only letters, digits, underscores (_), hyphens (-), and periods (.).
Last Name	■ The name contains 1 to 63 characters. ■ The name contains only letters, digits, underscores (_), hyphens (-), and periods (.).

Parameter	Description
Email Address	Email address for receiving messages from eService.
Country Code	■ International area code of the country where the phone number that receives messages from eService is located. ■ The value can contain only digits, asterisks (*), pound signs (#), plus signs (+), brackets, and hyphens (-).
Phone	■ Phone number used to receive messages from eService. ■ The value can contain only digits, asterisks (*), pound signs (#), plus signs (+), brackets, and hyphens (-).

c. Click ✓.

- To remove a contact

  Select the desired contact and click **Remove**.

Step 10 Save the settings and authenticate eService.

1. Click **Save and Authenticate**.

   The **Access Authentication** page is displayed.

2. Enter your **Support Account** and **Password**.

   NOTE

   If you do not have a support account, apply for one from the technical support center.

3. Click **OK**.

   After the authentication is complete, **Access Authentication** changes to **Authenticated**.

4. (Optional) Click **Test Network** to check whether eService can be used properly.

   NOTE

   The eService availability can be tested only after the device authentication is complete.

Step 11 Contact the technical support center to authenticate the site.

1. The installation personnel call the maintenance personnel of the technical support center to authenticate the site.
2. Maintenance personnel of the technical support center perform eService authentication on the eService cloud system.
3. After the authentication is complete, the maintenance personnel of the technical support center notify the installation personnel that the device authentication is successful.

Step 12 After the configuration is complete, log in to the eService cloud management system by following the instructions in the *eService Intelligent Cloud Management System User Guide*.

----End

5.5.4 Exporting a Data Package to Be Uploaded

If eService becomes unavailable, you can manually export data packages to be uploaded to Huawei technical support center.

Context

- If eService becomes unavailable, data in the last 24 hours is saved. After eService recovers, data uploading resumes. Before eService recovers, you can manually export data packages to be uploaded.
- Exported data packages include performance, running, and alarm data.

Procedure

Step 1 Log in to the CLI as an administrator or a super administrator.

Step 2 Run the **export event event_type=call_home ip=***?* **user=***?* **password=***?* **path=***?* command to export data packages to be exported.

Table 5-34 Parameters

Parameter	Description	Value
ip=*?*	IP address of a File Transfer Protocol (FTP) or Secure File Transfer Protocol (SFTP) server. **NOTE** To export log files, an FTP or SFTP server must be available and accessible to the storage system.	-
user=*?*	Name of a user for logging in to an FTP or SFTP server.	The value contains 1 to 64 characters without colons (:).
password=*?*	Password for logging in to an FTP or SFTP server.	The value contains 1 to 64 characters.

Parameter	Description	Value
path=*?*	Path and name of the exported log file.	The path must start with **/**. The file is a package. This parameter specifies the path and file name of the exported event or log on the FTP or SFTP server. For example: • **/test/** indicates that events or logs are saved in the **test** folder on the FTP/SFTP server. The file name is automatically generated. • **/test** indicates that events or logs are saved in the **test** file. • If you specify the file name, we recommend you add the file name extension **.tgz**. If you do not specify the file name extension, the CLI will add it automatically.

----End

Example

Export certain eService data to an FTP server, where the IP address of the FTP server is 192.168.8.211, the user name for logging in to the FTP server is **admin**, the password is **admin**, the exported eService data will be stored in the root directory of the FTP server, and the exported eService data will be saved with the default file name.

```
admin:/>export event event_type=call_home ip=192.168.8.211 user=admin password=***** path=/
protocol=FTP
WARNING: It will take several minutes to collect and export the information.
Have you read warning message carefully?(y/n)y
Are you sure you really want to perform the operation?(y/n)y
Controller ID: 0A
Package Path: /collector_chs_file_0A.tgz
Controller ID: 0B
Package Path: /collector_chs_file_0B.tgz
Command executed successfully.
```

5.6 Monitoring Storage System Performance

Performance monitoring data helps you understand system performance and use optimization configurations to improve system performance.

You can use the DeviceManager management software to monitor a storage system. You do not need to install DeviceManager. Instead, you can simply log in to it through a web browser. On DeviceManager, you can view real-time

performance monitoring data, alarms, and power consumption information about a storage system.

For details, see the *Performance Monitoring Guide*.

5.7 Managing Basic Information About a Storage System

You can modify the basic information such as the name and system time of a device based on service requirements.

5.7.1 Setting the Device Time

If the system time of the storage system is inaccurate, change the system time of the storage system. In this way, when alarms are generated, you can accurately determine the alarm generation time based on alarm logs. This operation allows you to synchronize the client time to the storage system and set NTP automatic synchronization or manually change the system time.

Prerequisites

- Complete the NTP server configuration before setting NTP automatic synchronization. For details about the operations, see related configuration documents of the NTP server.
- In an environment with the firewall function, when the NTP automatic synchronization function is enabled, you need to enable port 123.

Context

- Network time protocol (NTP) is a computer system time synchronization protocol, which can synchronize the computer system time to universal time coordinated (UTC). The server supporting and running the NTP is referred to as the NTP server.
- By synchronizing the client time, you can adjust the storage system time to be consistent with the client time.
- By configuring the NTP automatic synchronization, you can periodically and automatically synchronize a storage device with the NTP server which serves as an external time source.

Precautions

Changing the device time may cause the following impacts:

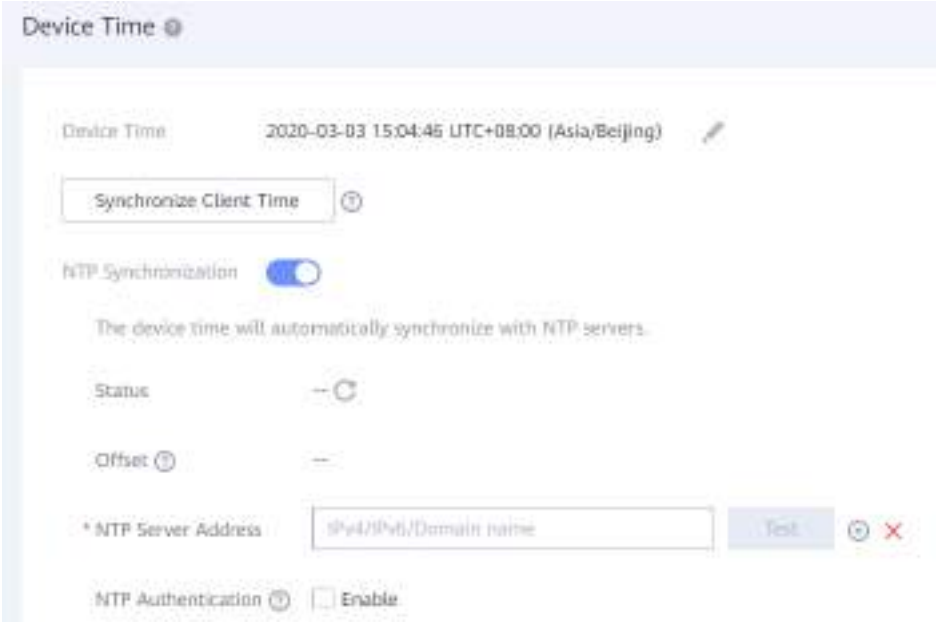
- If the device time is later than the license expiration date, the license may become invalid.
- If the device time is later than the certificate expiration date, the certificate will expire.
- If the device time is later than the user-defined password expiration date, the system may force users to change the login password.
- If the changed device time is later than the deadline for saving historical performance data, the system will no longer save historical performance data.

- Changing the device time affects BBU modules' lifespan and may trigger alarms indicating that a BBU module's life expires or is aged.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Basic Information** > **Device Time**.



Step 3 Configure the storage device time.

The storage device time can be configured in the following ways:

NOTE

Set the correct time zone and time; otherwise it may cause the time recorded in the alarms or logs to be inconsistent with the actual time which influences subsequent problem location.

- Manual

  a. Click on the right of **Device Time**.
  b. Click **Modify**.
  c. Change the storage device time.
     - In the time area, change the time of the device and click **OK**.
     - Select the time zone where the device is located from the **Time Zone** drop-down list box.
  d. Click .
     The security alert dialog box is displayed.
  e. Confirm the information in the dialog box, select **I have read and understand the consequences associated with performing this operation**, and click **OK**.

- Synchronize the client time.
  a. Click **Synchronize Client Time**.
  b. If the time zone ID cannot be obtained, **Client Time Zone** is displayed on DeviceManager. In the time zone list, select the time zone where the current client resides.
  c. Click .
     The security alert dialog box is displayed.
  d. Confirm the information in the dialog box, select **I have read and understand the consequences associated with performing this operation**, and click **OK**.
- Set NTP automatic synchronization.
  a. Select **NTP Synchronization**.
  b. Type the IPv4 address, IPv6 address or domain name of the NTP server in **NTP Server Address**.

     NOTE

     - A maximum of two NTP servers can be added. If the time of the one NTP server cannot be automatically synchronized to devices, the system synchronizes the time of another NTP server to devices.
     - Ensure that the time of two NTP servers is consistent.

  c. (Optional) Click **Test**.
  d. (Optional) In **NTP Authentication**, select **Enable**.

     NOTE

     - Only when NTPv4 or later is used, NTP authentication can be enabled to complete identity authentication for the NTP server and automatically synchronize the system clock to storage devices.
     - After NTP authentication is enabled, you need to import the CA certificate.

  e. Click **Save**.
  f. One minute after the configuration is saved, click on the right of **Status** to view the server status and the time difference between the NTP server and the storage device.

     NOTE

     - If the time difference is not 0, the time is being synchronized. If the time difference is 0, the time synchronization is complete.
     - The plus sign (+) before the time difference indicates that the device time is earlier than the NTP server time, and the subtraction sign (-) indicates that the device time is later than the NTP server time.

----End

5.7.2 Setting Device Information

This operation enables you to set device name and physical location of the device.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **Basic Information** > **Device Information**.

Step 3 Click **Modify** in the upper right corner of the **Basic Information** area.

Step 4 Modify device information:

1. Set the name and location of the device.

   NOTE

   - The device name contains 1 to 127 characters, including only letters, digits, periods (.), underscores (_), and hyphens (-). It cannot be left blank.
   - The device location contains 1 to 511 characters and cannot be left blank.

2. If the system has an effective capacity license but does not have SmartDedupe and SmartCompression licenses, set **Effective Capacity Alarm Threshold (%)** and **Effective Capacity Used Up Alarm Threshold (%)**.

   NOTE

   Effective Capacity Used Up Alarm Threshold (%) must be greater than **Effective Capacity Alarm Threshold (%)**.

3. Click **Save**.

----End

5.7.3 Set the Digital Warranty

Digital warranties for devices are provided so that you can enjoy better services in the Information Age. A digital warranty represents a digital record of committed warranty period. With the digital warranty function, you can check the start date of warranty service and committed warranty period.

Procedure

Step 1 Log in to the CLI as an administrator or super administrator.

Step 2 Set the service start date of a controller.

Run the **change controller starting_point_date controller_id**=*?* **date**=*?* command to set the service start date of a controller.

Table 5-35 Parameters

Parameter	Description	Value
controller_id=*?*	ID of a controller node.	[Value range] Run the **show controller general** command to obtain the value.

Parameter	Description	Value
date=?	Service start date.	[Value range] UTC format: YYYY-MM-DD. • YYYY: start year. The value starts from 1970. • MM: start month. • DD: start date.

The command output is as follows:

```
admin:/>change controller starting_point_date controller_id=0A date=2020-12-12
CAUTION: You are about to modify the service start time of the controller. This operation may result in extra alarms or error messages.
Suggestion: To prevent extra alarms or errors, ensure that the entered information is consistent with the contract information and that the entered parameters are valid.
Do you wish to continue?(y/n)y
Command executed successfully.
```

Step 3 Set the warranty period of a controller.

Run the **change controller service_session controller_id**=? **session**=? command to set the warranty period of a controller.

Table 5-36 Parameters

Parameter	Description	Value
controller_id=?	ID of a controller node.	[Value range] Run the **show controller general** command to obtain the value.
session=?	Warranty period.	[Value range] The value ranges from 0 to 600 (months).

The command output is as follows:

```
admin:/>change controller service_session controller_id=0A session=50
CAUTION: You are about to modify the service duration of the controller. The value ranges from 0 to 600, in months. This operation may cause extra alarms or errors.
Suggestion: To prevent extra alarms or errors, ensure that the entered information is consistent with the contract information and that the entered parameters are valid.
Do you wish to continue?(y/n)y
Command executed successfully.
```

Step 4 View the digital warranty of a device.

Run the **show controller general** command to view the digital warranty information.

The command output is as follows:

Table3 Parameters lists only the **Starting Point Date** and **Session** parameters. For details about other parameters in the **show controller general** command output, see the *Command Reference* of specific product model.

Table 5-37 Parameters

Parameter	Description
Starting Point Date	Service start date of a controller.
Session	Warranty period of a controller.

----End

5.8 Managing License Files

License files are authority credentials for value-added functions of the storage device. During routine maintenance, check that existing license files are available for their value-added functions.

For details about license-controlled functions, see Specifications Query (https://info.support.huawei.com/storage/spec/#/home).

This section describes how to browse and back up an activated license file. To import and activate a new license file, see the *Initialization Guide*.

5.8.1 Viewing an Activated License File

Before using value-added functions, check that their license files have been activated and effective.

Procedure

Step 1 Log in to DeviceManager.

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

Step 3 In the middle information pane, verify the information about active license files.

The licenses can be controlled using either of the following methods:

- By runtime: The **Expiry Date** of each license is displayed.

  NOTE

  If licenses are controlled by runtime, their **Used/Total Capacity** is **Unlimited** or **N/A**.

- By capacity: The **Used/Total Capacity** of each license is displayed.

  NOTE

  If licenses are controlled by capacity, their **Expiry Date** is **Permanent**.

  NOTE

  As the OceanStor UltraPath is not deployed on a storage system, you cannot check them on the license management page of the storage system. To view purchased features, you can obtain the product authorization certificate from your dealer, which shows the purchased features.

----End

5.8.2 Backing Up an Active License File

Back up license files so that you can re-import them if they are damaged after being activated.

Procedure

Step 1 Log in to DeviceManager.

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

Step 3 Back up active license files.

1. Click **Back Up License**.

   The **File Download** dialog box is displayed.

   NOTE

   Take Internet Explorer 8 for example.

2. Click **Save**.

   The **Save As** dialog is displayed.

3. Set a file name for and path to the exported license file.
4. Click **Save** and you have finished backing up the license file.

----End

5.9 Reclaiming Space of a Storage System

If all or some services of a storage system do not need to be running anymore, or some expanded space is unused, you can reclaim the space used by these services or the unused space and then use the space for new services, thereby enhancing storage space utilization.

5.9.1 Process for Reclaiming Space of a Storage System

Space reclamation can be classified into full reclamation and partial reclamation. This section describes the major processes of space reclamation.

Figure 5-28 and **Figure 5-29** illustrate the major processes of space reclamation.

NOTICE

Before a space reclamation, ensure that the space to be reclaimed does not need to be used anymore and data has been backed up, to avoid the data loss during space reclamation.

Figure 5-28 Process for full space reclamation

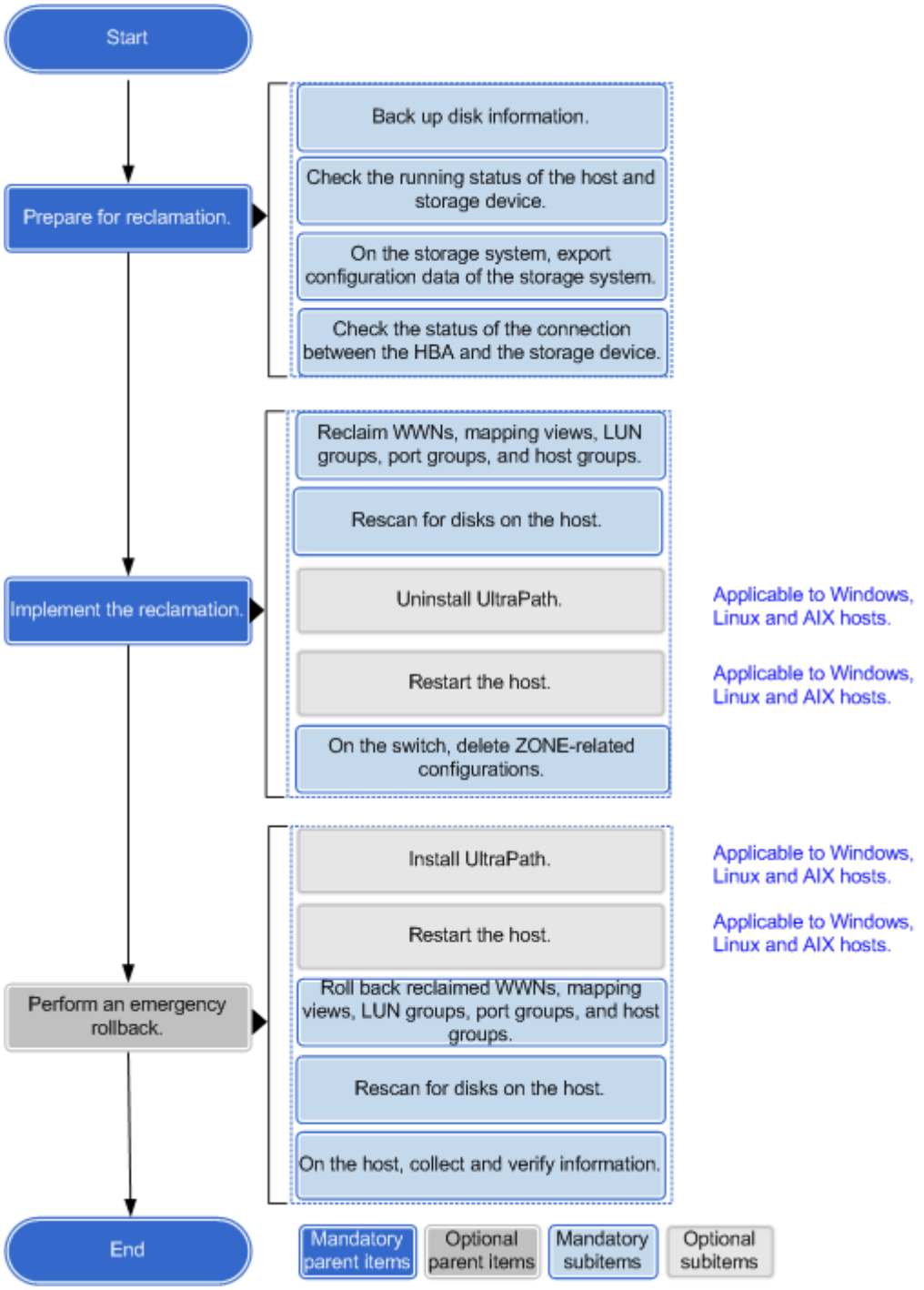
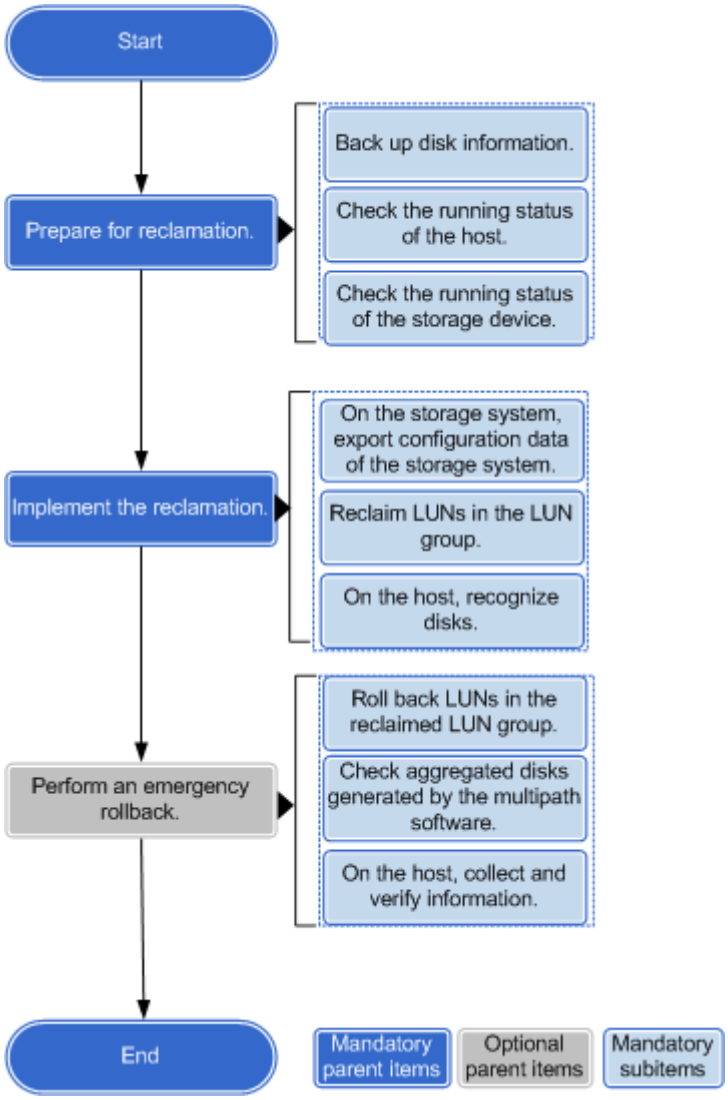


Figure 5-29 Process for partial space reclamation



5.9.2 Reclaiming Space of a Storage System (Windows)

This section describes how to reclaim space and then use it for new services if all or some services of a storage system are not required anymore, or some expanded space is unnecessary in a Windows operating system, thereby enhancing storage space utilization.

5.9.2.1 Preparing for Space Reclamation (Windows)

Before reclaiming space, you must finish preparatory work such as backing up disk information and checking the host and storage device's running status to ensure that the space reclamation can be successfully implemented.

Procedure

Step 1 Confirm the range of to-be-reclaimed storage space and back up disk information.

1. Confirm whether it is full reclamation or partial reclamation.
2. Back up disk information.
   a. Log in to the Windows Server 2008 application server as an administrator.
   b. Press **Windows+R** (if the operation is performed remotely, perform it in full screen mode) to open the **Run** dialog box.
   c. Type **diskmgmt.msc** and press **Enter**.
   d. On the **Disk Management** page that is displayed, view the host disk information.
3. Make sure that the to-be-reclaimed disk will not be used anymore.

Step 2 Check the host running status.

1. Check whether any error exists on the host.
   a. Press **Windows+R** (if the operation is performed remotely, perform it in full screen mode) to open the **Run** dialog box.
   b. Run **eventvwr.msc** and **devmgmt.msc** and press **Enter**.
   c. In the **Event Viewer** and **Device Manager** windows, check whether any error exists on the host. If there are, remove the errors and proceed to the next step.
2. Check the disk path status.
   a. Press **Windows+R** (if the operation is performed remotely, perform it in full screen mode) to open the **Run** dialog box and run **upadm** to log in to the CLI of UltraPath.
   b. Run **upadm show vlun** to query the status of all vLUNs. Confirm that the status of all vLUNs is **Normal**.
   c. Run **upadm show path** and make sure that the system path status is **Normal**. If a path whose status is **Degrade** exists, run **upadm set phypathnormal**. Specify the path whose status is **Degrade** using the **path_id** parameter.

Step 3 Check the storage system status. If there are alarms, clear them and then proceed to the next step.

Step 4 On the storage system, export the storage system configuration data.

1. Log in to the CLI of the storage system using PuTTY.

   NOTE

   The default super administrator name is **admin**.

2. Run **export running_data** to export and save the current configuration file.

Step 5 Check the status of the connection between the host HBA and the storage device.

1. As planned, check whether the two devices (the HBA and the storage device) are connected and whether the zoning on the switch is correct by using the WWN of the host HBA and the front-end port of the storage device.
2. Run **show port general** to check whether the planned front-end network is connected. Specify the front-end port using the **port_id** parameter.

   If the planned front-end network is connected, its **Type** is **Host Port** and its **Running** status is **Link up**.

3. Run **show initiator initiator_type=FC isfree=yes** to check whether the storage device can query the initiator on the host and filter out initiators that are not assigned to the host.

   In the command output, the planned HBA should exist and its running status should be **Online**.

```
admin:/>show initiator initiator_type=FC isfree=yes
WWN               Running Status       Free
-------------     -------------        -----
100000000000*     Online               Yes
Alias     Host ID        Multipath Type
-------   ----------     ------------------
--        --             Default
```

----End

5.9.2.2 Reclaiming Space (Windows)

This section describes how to reclaim storage space used by a Windows host in full reclamation or partial reclamation mode.

Full Reclamation

Step 1 Reclaim the World Wide Name (WWN).

1. Run **show mapping_view general** to query the ID of a host group in a mapping view to be reclaimed. Specify which mapping view to reclaim using the **mapping_view_id** parameter.
2. Obtain the information about hosts and initiators in the to-be-reclaimed host group.
   a. Run **show host_group host** to show the host that has been added to the to-be-reclaimed host group. Specify the ID of the to-be-reclaimed host group using the **mapping_view_id** parameter.
   b. Run **show initiator** to view the WWN about the host HBA that has been added to the to-be-reclaimed host group. Specify the ID of the host in the to-be-reclaimed host group using the **host_id** parameter.
3. Run **remove host initiator initiator_type=FC** to remove the WWN. Specify which WWN to reclaim using the **wwn** parameter.
4. Run **show initiator isfree=yes initiator_type=FC** to check whether the WWN is successfully deleted.

   If the deleted WWN exists in the command output, the deletion is successful.

```
admin:/>show initiator isfree=yes initiator_type=FC
WWN               Running Status       Free
-----------------   -------------------   -----
100000000000*     Online               Yes
Alias     Host ID        Multipath Type
-------   ----------     ----------------
--        --             Default
```

5. In DeviceManager, view the port information about the host.

Step 2 Run **upadm show path** to check the path status of the system. The reclaimed path should not exist in the command output.

NOTE

Wait at least 15 minutes and confirm that no errors exist on disks of other hosts. Then proceed to the next step.

Step 3 Delete the mapping view.

1. Run **show mapping_view general** to query and record the ID of a LUN group and host group in a mapping view to be reclaimed. Specify which mapping view to reclaim using the **mapping_view_id** parameter.
2. Run **remove mapping_view lun_group** to delete the LUN group mapped to the mapping view. Specify which mapping view and LUN group to reclaim using the **mapping_view_id** and **lun_group_id** parameters.
3. Run **remove mapping_view port_group** to delete the port group in the mapping view. Specify which mapping view and port group to reclaim using the **mapping_view_id** and **port_group_id** parameters.
4. Run **remove mapping_view host_group** to delete the host group in the mapping view. Specify which mapping view and host group to reclaim using the **mapping_view_id** and **host_group_id** parameters.
5. Run **delete mapping_view** to delete a mapping view. Specify which mapping view to reclaim using the **mapping_view_id** parameter.
6. Run **show mapping_view general** to check whether that mapping view has been deleted.

   The deleted mapping view should not exist in the command output.
7. In DeviceManager, view all mapping views. The deleted mapping view should not exist.

Step 4 Delete a LUN group.

1. Run **remove lun_group lun** to remove all LUNs in the LUN group. Specify which LUN group and LUNs to reclaim using the **lun_group_id** and **lun_id_list** parameters.
2. Run **delete lun_group** to delete a LUN group. Specify which LUN group to reclaim using the **lun_group_id** parameter.

Step 5 Delete a port group.

1. Run **remove port_group port** to remove all ports in the port group. Specify which port group and ports to reclaim using the **port_group_id** and **port_id_list** parameters.
2. Run **delete port_group** to delete a port group. Specify which port group to reclaim using the **port_group_id** parameter.

Step 6 Delete a host group.

1. Run **remove host_group host** to remove all hosts in the host group. Specify which host group and hosts to reclaim using the **host_group_id** and **host_id_list** parameters.
2. Run **delete host_group** to delete a host group. Specify which host group to reclaim using the **host_group_id** parameter.
3. Run **remove host initiator initiator_type=FC** to remove all initiators of the to-be-reclaimed host. Specify which initiators to reclaim using the **wwn** parameter.

4. Run **delete host** to delete a to-be-reclaimed host. Specify which host to reclaim using the **host_id** parameter.

Step 7 Scan for disks on the host.

1. Press **Windows+R** (if the operation is performed remotely, perform it in full screen mode) to open the **Run** dialog box.
2. Type **devmgmt.msc** and press **Enter**.
3. In the **Device Manager** window that is displayed, click **View** and select **Show hidden devices**.
4. Right-click **Disk Drives** and choose **Scan for hardware changes** to start scanning.
5. Check whether the number of newly generated **UltraPath_Disks** is the same as that of mapped LUNs. If they are different, check the LUN mapping and path connection status on the storage device.
6. Check whether the number of newly generated SCSI disks (**SCSI Disk Devices** on the Huawei storage device) doubles or quadruples that of **UltraPath_Disks** in **Step 7.5**. If not, check the LUN mapping and path connection status on the storage device.

Step 8 Uninstall UltraPath.

1. Press **Windows+R** (if the operation is performed remotely, perform it in full screen mode) to open the **Run** dialog box.
2. Type **appwiz.cpl** and press **Enter**.

   The **Programs and Features** page is displayed.
3. Right-click **UltraPath** and choose **Uninstall** from the shortcut menu.
4. Follow the wizard until UltraPath is uninstalled.

Step 9 Run **shutdown -r -t 0** to restart the host.

Step 10 On the switch, delete zone or VLAN configurations.

----End

Partial Reclamation

Step 1 Remove the to-be-reclaimed LUN from the owning LUN group.

1. Run **show mapping_view general** to obtain the details about the to-be-reclaimed mapping view. Specify the mapping view using the **mapping_view_id** parameter.
2. Run **remove lun_group lun** to remove the to-be-reclaimed LUN from the LUN group. Specify the LUN group and to-be-reclaimed LUN using the **lun_group_id** and **lun_id_list** parameters.
3. Run **show lun_group lun** to check whether the to-be-reclaimed LUN has been deleted from the LUN group successfully. Specify the LUN group using the **lun_group_id** parameter.

   The deleted LUN should not exist in the command output.

```
admin:/>show lun_group lun lun_group_id=LGID
ID    Name          Pool ID   Capacity
----  ------------  ----------  ---------
1     LUN1          0         1.000TB
```



```
Helth Status     Running Status     Type
---------------  ------------------ -----
Normal           Online             Thin
WWN
----------------------------
60022a11000*****************
```

Step 2 Scan for disks on the host.

1. Press **Windows+R** (if the operation is performed remotely, perform it in full screen mode) to open the **Run** dialog box.
2. Type **devmgmt.msc** and press **Enter**.
3. In the **Device Manager** window that is displayed, click **View** and select **Show hidden devices**.
4. Right-click **Disk Drives** and choose **Scan for hardware changes** to start scanning.
5. Check whether the number of newly generated **UltraPath_Disks** is the same as that of mapped LUNs. If they are different, check the LUN mapping and path connection status on the storage device.
6. Check whether the number of newly generated SCSI disks (**SCSI Disk Devices** on the Huawei storage device) doubles or quadruples that of **UltraPath_Disks** in **Step 2.5**. If not, check the LUN mapping and path connection status on the storage device.

----End

5.9.3 Reclaiming Space of a Storage System (Linux)

This section describes how to reclaim space and then use it for new services if all or some services of a storage system are not required anymore, or some expanded space is unnecessary in a Linux operating system, thereby enhancing storage space utilization.

5.9.3.1 Preparing for Space Reclamation (Linux)

Before reclaiming space, you must finish preparatory work such as backing up disk information and checking the host and storage device's running status to ensure that the space reclamation can be successfully implemented.

Procedure

Step 1 Confirm the range of to-be-reclaimed storage space and back up disk information.

1. Confirm whether it is full reclamation or partial reclamation.
2. Run **vgdisplay -v**, **pvdisplay**, and **fdisk -l** to view VG, PV, and disk information. Back up the information.
3. Make sure that the to-be-reclaimed disk will not be used anymore.
   a. Run **upadmin show vlun** to view the mappings between the to-be-reclaimed LUN and the disk on the host.
   b. Run **vgdisplay -v** and make sure that the to-be-reclaimed disk is not in a VG.

Step 2 Check the host running status.

1. Run **more /var/log/messages** to check whether there are any errors related to the storage system on the host. If there are, remove the errors and proceed to the next step.
2. Check the disk path status.
   a. Run **upadmin show vlun** to query the status of all vLUNs. Confirm that the status of all vLUNs is **Normal**.
   b. Run **upadmin show path** and make sure that the system path status is **Normal**. If a path whose status is **Degrade** exists, run **upadmin set phypathnormal**. Specify the path whose status is **Degrade** using the **path_id** parameter.
3. Run **upadmin set workingmode=0** to change the working mode of UltraPath.
4. Run **upadmin set loadbalancemode=round-robin** to change the I/O pathing mode of UltraPath.

Step 3 Check the storage system status. If there are alarms, clear them and then proceed to the next step.

Step 4 On the storage system, export the storage system configuration data.

1. Log in to the CLI of the storage system using PuTTY.

   NOTE

   The default super administrator name is **admin**.

2. Run **export running_data** to export and save the current configuration file.

Step 5 Check the status of the connection between the host HBA and the storage device.

1. As planned, check whether the two devices (the HBA and the storage device) are connected and whether the zoning on the switch is correct by using the WWN of the host HBA and the front-end port of the storage device.
2. Run **show port general** to check whether the planned front-end network is connected. Specify the front-end port using the **port_id** parameter.

   If the planned front-end network is connected, its **Type** is **Host Port** and its **Running** status is **Link up**.
3. Run **show initiator initiator_type=FC isfree=yes** to check whether the storage device can query the initiator on the host and filter out initiators that are not assigned to the host.

   In the command output, the planned HBA should exist and its running status should be **Online**.

```
admin:/>show initiator initiator_type=FC isfree=yes
WWN                Running Status       Free
------------------ -------------------- -----
100000000000*      Online               Yes
Alias     Host ID        Multipath Type
-------   ----------     ------------------
--        --             Default
```

----End

5.9.3.2 Reclaiming Space (Linux)

This section describes how to reclaim the space used by a Linux host using full reclamation or partial reclamation.

Full Reclamation

Step 1 Reclaim the WWN.

1. Run **show mapping_view general** to obtain the host group ID in the mapping view to be reclaimed. Specify the mapping view using the **mapping_view_id** parameter.
2. Obtain the information about hosts and initiators in the to-be-reclaimed host group.
   a. Run **show host_group host** to show the host that has been added to the to-be-reclaimed host group. Specify the ID of the to-be-reclaimed host group using the **mapping_view_id** parameter.
   b. Run **show initiator** to view the WWN about the host HBA that has been added to the to-be-reclaimed host group. Specify the ID of the host in the to-be-reclaimed host group using the **host_id** parameter.
3. Run **remove host initiator initiator_type=FC** to remove the WWN. Specify the to-be-reclaimed WWN using the **wwn** parameter.
4. Run **show initiator isfree=yes initiator_type=FC** to check whether the WWN is successfully deleted.

   If the deleted WWN exists in the command output, the deletion is successful.

   ```
   admin:/>show initiator isfree=yes initiator_type=FC
   WWN               Running Status       Free
   ----------------  -------------------  -----
   100000000000*     Online               Yes
   Alias     Host ID       Multipath Type
   -------   ----------    ------------------
   --        --            Default
   ```

5. In DeviceManager, view the port information about the host.

Step 2 Run **upadmin show path** to check the path status of the system. The reclaimed path should not exist in the command output.

NOTE

Wait at least 15 minutes and confirm that no errors exist on disks of other hosts. Then proceed to the next step.

Step 3 Delete a mapping view.

1. Run **show mapping_view general** to obtain the IDs of the LUN group and host group in the mapping view to be reclaimed. Specify the mapping view using the **mapping_view_id** parameter.
2. Run **remove mapping_view lun_group** to delete the LUN group mapped to the mapping view. Specify the to-be-reclaimed mapping view and the to-be-reclaimed LUN group using the **mapping_view_id** and **lun_group_id** parameters.
3. Run **remove mapping_view port_group** to delete the port group in the mapping view. Specify the to-be-reclaimed mapping view and the to-be-

reclaimed port group using the **mapping_view_id** and **port_group_id** parameters.

4. Run **remove mapping_view host_group** to delete the host group in the mapping view. Specify the to-be-reclaimed mapping view and the to-be-reclaimed host group using the **mapping_view_id** and **host_group_id** parameters.
5. Run **delete mapping_view** to delete a mapping view. Specify the to-be-reclaimed mapping view using the **mapping_view_id** parameter.
6. Run **show mapping_view general** to check whether that mapping view has been deleted.

   The deleted mapping view should not exist in the command output.
7. In DeviceManager, view all mapping views. The deleted mapping view should not exist.

Step 4 Delete a LUN Group

1. Run **remove lun_group lun** to remove all LUNs in the LUN group. Specify the to-be-reclaimed LUN group and the to-be-removed LUN using the **lun_group_id** and **lun_id_list** parameters.
2. Run **delete lun_group** to delete a LUN group. Specify the to-be-reclaimed LUN group using the **lun_group_id** parameter.

Step 5 Delete a port group.

1. Run **remove port_group port** to remove all ports in the port group. Specify the to-be-reclaimed port group and to-be-removed ports using the **port_group_id** and **port_id_list** parameters.
2. Run **delete port_group** to delete a port group. Specify the to-be-reclaimed port group using the **port_group_id** parameter.

Step 6 Delete a host group.

1. Run **remove host_group host** to remove all hosts in the host group. Specify the to-be-reclaimed host group and to-be-removed hosts using the **host_group_id** and **host_id_list** parameters.
2. Run **delete host_group** to delete a host group. Specify the to-be-reclaimed host group using the **host_group_id** parameter.
3. Run **remove host initiator initiator_type=FC** to remove all initiators of the to-be-reclaimed host. Specify the to-be-removed initiator using the **wwn** parameter.
4. Run **delete host** to delete a to-be-reclaimed host. Specify the to-be-reclaimed host using the **host_id** parameter.

Step 7 Scan for disks on the host.

1. Run **upRescan** to scan for disks.

```
#upRescan
  Begin to delete LUNs whose mappings do not exist
  Begin to delete LUNs whose mappings are changed
```

2. Run **upadmin show vlun** to check whether the number of disks managed by UltraPath is the same as planned.
3. Run **upadmin show path** to check whether the disk path status is normal. If the status of a path is **Degrade**, run **upadmin set phypathnormal** to set the path to **Normal**. In the command, set **path_id** to the ID of the **Degrade** path.

Step 8 Uninstall UltraPath.

1. Run **rpm -e UltraPath** to uninstall UltraPath.
2. Run **rpm -qa | grep UltraPath** to check whether the uninstallation is successful. If information about UltraPath does not exist in the command output, the uninstallation is successful.

Step 9 Run **shutdown -r now** to restart the host.

Step 10 Verify the storage environment on the host.

1. Run **fdisk -l** to check the host. In the command output, to-be-reclaimed disks should not exist.
2. Run **more /var/log/messages** to check whether there are any errors related to the storage system on the host. If there are, collect relevant information and remove the errors.

Step 11 On the switch, delete zone or VLAN configurations.

----End

Partial Reclamation

Step 1 Remove the to-be-reclaimed LUN from the owning LUN group.

1. Run **show mapping_view general** to obtain the details about the to-be-reclaimed mapping view. Specify the mapping view using the **mapping_view_id** parameter.
2. Run **remove lun_group lun** to remove the to-be-reclaimed LUN from the LUN group. Specify the LUN group and to-be-reclaimed LUN using the **lun_group_id** and **lun_id_list** parameters.
3. Run **show lun_group lun** to check whether the to-be-reclaimed LUN has been removed from the LUN group. Specify the LUN group where the to-be-reclaimed LUN resides using the **lun_group_id** parameter.

   The deleted LUN should not exist in the command output.

```
admin:/>show lun_group lun lun_group_id=LGID
ID     Name           Pool ID    Capacity
----   -------------  --------   --------
1      LUN1           0          1.000TB
Helth Status      Running Status      Type
---------------   ------------------- -------
Normal            Online              Thin
WWN
---------------------------------
60022a11000******************
```

Step 2 Scan for disks on the host.

1. Run **upRescan** to scan for disks.

```
#upRescan
  Begin to delete LUNs whose mappings do not exist
  Begin to delete LUNs whose mappings are changed
```

2. Run **upadmin show vlun** to check whether the number of disks managed by UltraPath is the same as planned.
3. Run **upadmin show path** to check whether the disk path status is normal. If the status of a path is **Degrade**, run **upadmin set phypathnormal** to set the path to **Normal**. In the command, set **path_id** to the ID of the **Degrade** path.

Step 3 Verify the storage environment on the host.

----End

5.9.4 Reclaiming Space of a Storage System (AIX)

This section describes how to reclaim space and then use it for new services if all or some services of a storage system are not required anymore, or some expanded space is unnecessary in an AIX operating system, thereby enhancing storage space utilization.

5.9.4.1 Preparing for Space Reclamation (AIX)

Before reclaiming space, you must finish preparatory work such as backing up disk information and checking the host and storage device's running status to ensure that the space reclamation can be successfully implemented.

Procedure

Step 1 Confirm the range of to-be-reclaimed storage space and back up disk information.

1. Confirm whether it is full reclamation or partial reclamation.
2. Run **lsvg**, **lspv** and **lsdev -Cc disk** to view volume group (VG), physical volume (PV), and disk information. Back up the information.
3. Confirm that the to-be-reclaimed disk will not be used anymore.
   a. Run **upadm show vlun** to view the mappings between the to-be-reclaimed LUN and the disk on the host.
   b. Run **lspv** and make sure that the to-be-reclaimed disk is not in a VG.

Step 2 Check the host running status.

1. Run **errpt** to check whether there are any errors on the host. Remove the errors before proceeding to the next step.
2. Check the disk path status.
   a. Run **upadm show vlun** to query the status of all vLUNs. Confirm that the status of all vLUNs is **Normal**.
   b. Run **upadm show path**. Check whether the system path status is **Normal**. If the status of a path is **Degrade**, run **upadm set phypathnormal**. Specify the path using the **path_id** parameter.

Step 3 Check the storage system status. If there are alarms, clear them and then proceed to the next step.

Step 4 On the storage system, export the storage system configuration data.

1. Log in to the CLI of the storage system using PuTTY.

   NOTE

   The default super administrator name is **admin**.

2. Run **export running_data** to export and save the current configuration file.

Step 5 Check the status of the connection between the host HBA and the storage device.

1. As planned, check whether the two devices (the HBA and the storage device) are connected and whether the zoning on the switch is correct by using the WWN of the host HBA and the front-end port of the storage device.
2. Run **show port general** to check whether the planned front-end network is connected. Specify the front-end port using the **port_id** parameter.

   If the planned front-end network is connected, its **Type** is **Host Port** and its **Running** status is **Link up**.
3. Run **show initiator initiator_type=FC isfree=yes** to check whether the storage device can query the initiator on the host and filter out initiators that are not assigned to the host.

   In the command output, the planned HBA should exist and its running status should be **Online**.

```
admin:/>show initiator initiator_type=FC isfree=yes
WWN                Running Status        Free
------------------ -------------------- -----
100000000000*      Online               Yes
Alias      Host ID        Multipath Type
-------    ----------     ------------------
--         --             Default
```

----End

5.9.4.2 Reclaiming Space (AIX)

This section describes how to reclaim the space used by an AIX host using full reclamation or partial reclamation.

Full Reclamation

Step 1 Delete a disk device.

1. Run **upadm show vlun** and **lsdev -Cc disk** to show all LUNs and disks on the host.
2. Run **rmdev -dl hdiskX** to delete the aggregation device composed of the disks to be reclaimed. **hdiskX** represents the aggregation device.
3. Run **upadm show path** and view the result in **Step 1.1** to check whether the aggregation device has been deleted.
4. Run **lsdev -Cc disk** and **lsdev -Cc disk | wc -l** and view the result in **Step 1.1** to check whether the device path file has been deleted.

Step 2 Reclaim the World Wide Name (WWN).

1. Run **show mapping_view general** to obtain the host group ID in the mapping view to be reclaimed. Specify the mapping view using the **mapping_view_id** parameter.
2. Obtain the information about hosts and initiators in the to-be-reclaimed host group.
   a. Run **show host_group host** to show the host that has been added to the to-be-reclaimed host group. Specify the ID of the to-be-reclaimed host group using the **mapping_view_id** parameter.
   b. Run **show initiator** to view the WWN about the host HBA that has been added to the to-be-reclaimed host group. Specify the ID of the host in the to-be-reclaimed host group using the **host_id** parameter.

3. Run **remove host initiator initiator_type=FC** to remove the WWN. Specify the to-be-reclaimed WWN using the **wwn** parameter.
4. Run **show initiator isfree=yes initiator_type=FC** to check whether the WWN is successfully deleted.

   If the deleted WWN exists in the command output, the deletion is successful.

   ```
   admin:/>show initiator isfree=yes initiator_type=FC
   WWN                 Running Status        Free
   ------------------  --------------------  -----
   100000000000*       Online                Yes
   Alias      Host ID         Multipath Type
   -------    ----------      ------------------
   --         --              Default
   ```

5. In DeviceManager, view the port information about the host.

Step 3 Run **upadm show path** to check whether only the paths of the to-be-reclaimed disks are **Failed**. If other paths are **Failed**, find out the cause and solve the problem.

NOTE

Wait at least 15 minutes and confirm that no errors exist on disks of other hosts. Then proceed to the next step.

Step 4 Delete a mapping view.

1. Run **show mapping_view general** to obtain the IDs of the LUN group and host group in the mapping view to be reclaimed. Specify the mapping view using the **mapping_view_id** parameter.
2. Run **remove mapping_view lun_group** to delete the LUN group mapped to the mapping view. Specify the to-be-reclaimed mapping view and the to-be-reclaimed LUN group using the **mapping_view_id** and **lun_group_id** parameters.
3. Run **remove mapping_view port_group** to delete the port group in the mapping view. Specify the to-be-reclaimed mapping view and the to-be-reclaimed port group using the **mapping_view_id** and **port_group_id** parameters.
4. Run **remove mapping_view host_group** to delete the host group in the mapping view. Specify the to-be-reclaimed mapping view and the to-be-reclaimed host group using the **mapping_view_id** and **host_group_id** parameters.
5. Run **delete mapping_view** to delete a mapping view. Specify the to-be-reclaimed mapping view using the **mapping_view_id** parameter.
6. Run **show mapping_view general** to check whether that mapping view has been deleted.

   The deleted mapping view should not exist in the command output.
7. In DeviceManager, view all mapping views. The deleted mapping view should not exist.

Step 5 Delete a LUN Group

1. Run **remove lun_group lun** to remove all LUNs in the LUN group. Specify the to-be-reclaimed LUN group and the to-be-removed LUN using the **lun_group_id** and **lun_id_list** parameters.

2. Run **delete lun_group** to delete a LUN group. Specify the to-be-reclaimed LUN group using the **lun_group_id** parameter.

Step 6 Delete a port group.

1. Run **remove port_group port** to remove all ports in the port group. Specify the to-be-reclaimed port group and to-be-removed ports using the **port_group_id** and **port_id_list** parameters.
2. Run **delete port_group** to delete a port group. Specify the to-be-reclaimed port group using the **port_group_id** parameter.

Step 7 Delete a host group.

1. Run **remove host_group host** to remove all hosts in the host group. Specify the to-be-reclaimed host group and to-be-removed hosts using the **host_group_id** and **host_id_list** parameters.
2. Run **delete host_group** to delete a host group. Specify the to-be-reclaimed host group using the **host_group_id** parameter.
3. Run **remove host initiator initiator_type=FC** to remove all initiators of the to-be-reclaimed host. Specify the to-be-removed initiator using the **wwn** parameter.
4. Run **delete host** to delete a to-be-reclaimed host. Specify the to-be-reclaimed host using the **host_id** parameter.

Step 8 Uninstall UltraPath.

1. Run **lslpp -L | grep -i UltraPath** to view the version of the installed UltraPath.
2. Run **installp -u program_name** to uninstall UltraPath, where **program_name** is the name of UltraPath shown in **Step 8.1**.
3. Run **lslpp -L | grep -i UltraPath**. If the command output does not contain the UltraPath shown in **Step 8.1**, the uninstallation is successful.

Step 9 Run **shutdown -Fr** to restart the host.

Step 10 On the switch, delete zone configurations.

----End

Partial Reclamation

Step 1 Delete a disk device.

1. Run **upadm show vlun** and **lsdev -Cc disk** to show all LUNs and disks on the host.
2. Run **rmdev -dl hdiskX** to delete the aggregation device composed of the disks to be reclaimed. **hdiskX** represents the aggregation device.
3. Run **upadm show path** and view the result in **Step 1.1** to check whether the aggregation device has been deleted.
4. Run **lsdev -Cc disk** and **lsdev -Cc disk | wc -l** and view the result in **Step 1.1** to check whether the device path file has been deleted.

Step 2 Remove the to-be-reclaimed LUN from the owning LUN group.

1. Run **show mapping_view general** to obtain the details about the to-be-reclaimed mapping view. Specify the mapping view using the **mapping_view_id** parameter.

2. Run **remove lun_group lun** to remove the to-be-reclaimed LUN from the LUN group. Specify the LUN group and to-be-reclaimed LUN using the **lun_group_id** and **lun_id_list** parameters.
3. Run **show lun_group lun** to check whether the to-be-reclaimed LUN has been removed from the LUN group. Specify the LUN group where the to-be-reclaimed LUN resides using the **lun_group_id** parameter.

   The deleted LUN should not exist in the command output.

```
admin:/>show lun_group lun lun_group_id=LGID
ID     Name          Pool ID    Capacity
----   -----------  ---------- -------------
1      LUN1          0          1.000TB
Helth Status      Running Status      Type
---------------   ------------------- -------
Normal            Online              Thin
WWN
---------------------------------
60022a11000******************
```

----End

5.9.5 Reclaiming Space of a Storage System (HP-UX)

Some or all of services in an HP-UX operating system may be not required anymore, or some expanded space may be unnecessary. In these cases, reclaim space and then use it for new services, thereby enhancing storage space utilization.

5.9.5.1 Preparing for Space Reclamation (HP-UX)

Before reclaiming space, you must finish preparatory work such as backing up disk information and checking the host and storage device's running status to ensure that the space reclamation can be successfully implemented.

Procedure

Step 1 Confirm the range of to-be-reclaimed storage space and back up disk information.

1. Confirm whether it is full reclamation or partial reclamation.
2. Run **ioscan -fnkC disk** and **vgdisplay -v** to view information about a disk in a volume group (VG) and back up the information.
3. Make sure that the to-be-reclaimed disk will not be used anymore.
   a. Run **ioscan -fnkC disk** to view the mappings between the to-be-reclaimed LUN and the disk on the host.
   b. Run **vgdisplay -v** and make sure that the to-be-reclaimed disk is not in a VG.

Step 2 Check the host running status.

1. Run **tail -200 /var/adm/syslog/syslog.log** to check the host status. If an error exists on storage device, remove it and proceed to the next step.
2. Check the disk path status.
   a. Run **scsimgr get_attr -a leg_mpath_enable** and make sure that Native Multi-Pathing (NMP) is enabled.

b. Run **scsimgr lun_map -D /dev/rdisk/diskX** to view disk path information, where **diskX** represents a disk on the host.

c. Run **scsimgr get_info -D /dev/rdisk/diskX** to view disk multipathing settings.

In the command output, make sure that the path status is **ACTIVE** and the load balancing mode is **round_robin**.

Step 3 Check the storage system status. If there are alarms, clear them and then proceed to the next step.

Step 4 On the storage system, export the storage system configuration data.

1. Log in to the command-line interface (CLI) of the storage system using PuTTY.

   NOTE

   The default super administrator name is **admin**.

2. Run **export running_data** to export and save the current configuration file.

Step 5 Check the status of the connection between the host HBA and the storage device.

1. As planned, check whether the two devices (the HBA and the storage device) are connected and whether the zoning on the switch is correct by using the WWN of the host HBA and the front-end port of the storage device.
2. Run **show port general** to check whether the planned front-end network is connected. Specify the front-end port using the **port_id** parameter.

   If the planned front-end network is connected, its **Type** is **Host Port** and its **Running** status is **Link up**.
3. Run **show initiator initiator_type=FC isfree=yes** to check whether the storage device can query the initiator on the host and filter out initiators that are not assigned to the host.

   In the command output, the planned HBA should exist and its running status should be **Online**.

```
admin:/>show initiator initiator_type=FC isfree=yes
WWN                Running Status       Free
------------------ -------------------- -----
100000000000*      Online               Yes
Alias     Host ID        Multipath Type
-------   ----------     ------------------
--        --             Default
```

----End

5.9.5.2 Reclaiming Space (HP-UX)

This section describes how to reclaim the space used by an HP-UX 11.31 host in full or partial reclamation mode.

Full Reclamation

Step 1 Reclaim the World Wide Name (WWN).

1. Run **show mapping_view general** to obtain the host group ID in the to-be-reclaimed mapping view. Specify the to-be-reclaimed mapping view using the **mapping_view_id** parameter.

2. Obtain the information about hosts and initiators in the to-be-reclaimed host group.
   a. Run **show host_group host** to show the host that has been added to the to-be-reclaimed host group. Specify the ID of the to-be-reclaimed host group using the **mapping_view_id** parameter.
   b. Run **show initiator** to view the WWN about the host HBA that has been added to the to-be-reclaimed host group. Specify the ID of the host in the to-be-reclaimed host group using the **host_id** parameter.
3. Run **remove host initiator initiator_type=FC** to remove the WWN. Specify the to-be-reclaimed WWN using the **wwn** parameter.
4. Run **show initiator isfree=yes initiator_type=FC** to check whether the WWN is successfully deleted.

   If the deleted WWN exists in the command output, the deletion is successful.

```
admin:/>show initiator isfree=yes initiator_type=FC
WWN                Running Status        Free
-----------------  --------------------  -----
100000000000*      Online                Yes
Alias      Host ID         Multipath Type
-------    ----------      ------------------
--         --              Default
```

5. In DeviceManager, view the port information about the host.

Step 2 Run **upadm show path** to check the path status of the system. The reclaimed path should not exist in the command output.

NOTE

Wait at least 15 minutes and confirm that no errors exist on disks of other hosts. Then proceed to the next step.

Step 3 Delete a mapping view.

1. Run **show mapping_view general** to obtain the IDs of the LUN group and host group in the mapping view to be reclaimed. Specify the mapping view using the **mapping_view_id** parameter.
2. Run **remove mapping_view lun_group** to delete the LUN group mapped to the mapping view. Specify the to-be-reclaimed mapping view and the to-be-reclaimed LUN group using the **mapping_view_id** and **lun_group_id** parameters.
3. Run **remove mapping_view port_group** to delete the port group in the mapping view. Specify the to-be-reclaimed mapping view and the to-be-reclaimed port group using the **mapping_view_id** and **port_group_id** parameters.
4. Run **remove mapping_view host_group** to delete the host group in the mapping view. Specify the to-be-reclaimed mapping view and the to-be-reclaimed host group using the **mapping_view_id** and **host_group_id** parameters.
5. Run **delete mapping_view** to delete a mapping view. Specify the to-be-reclaimed mapping view using the **mapping_view_id** parameter.
6. Run **show mapping_view general** to check whether that mapping view has been deleted.

   The deleted mapping view should not exist in the command output.

7. In DeviceManager, view all mapping views. The deleted mapping view should not exist.

Step 4 Delete a LUN Group

1. Run **remove lun_group lun** to remove all LUNs in the LUN group. Specify the to-be-reclaimed LUN group and the to-be-removed LUN using the **lun_group_id** and **lun_id_list** parameters.
2. Run **delete lun_group** to delete a LUN group. Specify the to-be-reclaimed LUN group using the **lun_group_id** parameter.

Step 5 Delete a port group.

1. Run **remove port_group port** to remove all ports in the port group. Specify the to-be-reclaimed port group and to-be-removed ports using the **port_group_id** and **port_id_list** parameters.
2. Run **delete port_group** to delete a port group. Specify the to-be-reclaimed port group using the **port_group_id** parameter.

Step 6 Delete a host group.

1. Run **remove host_group host** to remove all hosts in the host group. Specify the to-be-reclaimed host group and to-be-removed hosts using the **host_group_id** and **host_id_list** parameters.
2. Run **delete host_group** to delete a host group. Specify the to-be-reclaimed host group using the **host_group_id** parameter.
3. Run **remove host initiator initiator_type=FC** to remove all initiators of the to-be-reclaimed host. Specify the to-be-removed initiator using the **wwn** parameter.
4. Run **delete host** to delete a to-be-reclaimed host. Specify the to-be-reclaimed host using the **host_id** parameter.

Step 7 Delete a device file.

1. Run **ioscan -fNkC disk** and **ioscan -fNkC disk | grep -i HUAWEI | wc -l** to show all LUNs.
2. Delete a device path file.
   a. Run **ioscan -fNC disk** to scan for system disks.
   b. Run **ioscan -fNkC disk | grep -i NO_HW** to check whether there are disks whose status is **NO_HW**.
   c. Run **ioscan -fNkC disk | grep -i NO_HW | awk '{ print $3}' | xargs -n1 rmsf -C disk -H** to delete disks whose status is **NO_HW**.
   d. Run **ioscan -fNkC disk | grep -i NO_HW** to check whether there are disks whose status is **NO_HW**. If there are, delete them.
3. Run **ioscan -fNkC disk** and **ioscan -fNkC disk | grep -i HUAWEI | wc -l** again and view the result in **Step 7.1** to check whether the device path file has been deleted.

Step 8 Verify the storage environment on the host.

1. Run **ioscan -fNkC disk** to check the status of the disk device file on the host. Disks whose status is **NO_HW** should not exist.
2. Run **tail -200 /var/adm/syslog/syslog.log** to check whether there are any errors. If there are, collect relevant information and remove the errors.

Step 9 On the switch, delete zone configurations.

----End

Partial Reclamation

Step 1 Remove the to-be-reclaimed LUN from the owning LUN group.

1. Run **show mapping_view general** to obtain the details about the to-be-reclaimed mapping view. Specify the mapping view using the **mapping_view_id** parameter.
2. Run **remove lun_group lun** to remove the to-be-reclaimed LUN from the LUN group. Specify the LUN group and to-be-reclaimed LUN using the **lun_group_id** and **lun_id_list** parameters.
3. Run **show lun_group lun** to check whether the to-be-reclaimed LUN has been removed from the LUN group. Specify the LUN group where the to-be-reclaimed LUN resides using the **lun_group_id** parameter.

   The deleted LUN should not exist in the command output.

```
admin:/>show lun_group lun lun_group_id=LGID
ID     Name           Pool ID    Capacity
----   -------------  ---------- -------------
1      LUN1           0          1.000TB
Helth Status      Running Status      Type
---------------   ------------------- -------
Normal            Online              Thin
WWN
---------------------------------
60022a11000*****************
```

Step 2 Verify the storage environment on the host.

1. Run **ioscan -fNC disk** to scan the status of remaining disk paths.
2. Run **tail -200 /var/adm/syslog/syslog.log** to check whether there are any errors. If there are, collect relevant information and remove the errors.

----End

5.9.6 Emergency Rollback of Space Reclamation

This section describes how to perform an emergency rollback when you encounter an abnormality or fault during space reclamation.

Emergency rollback of space reclamation covers both the full reclamation and partial reclamation scenarios. **Figure 5-30** and **Figure 5-31** show the major procedures.

Figure 5-30 Emergency rollback procedure (full reclamation)

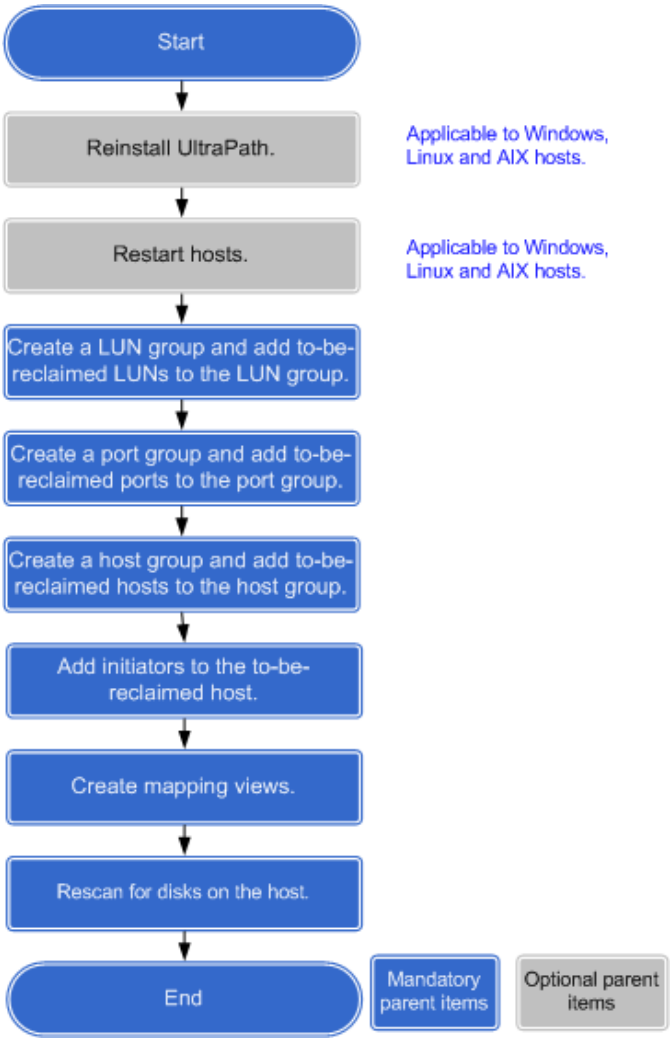
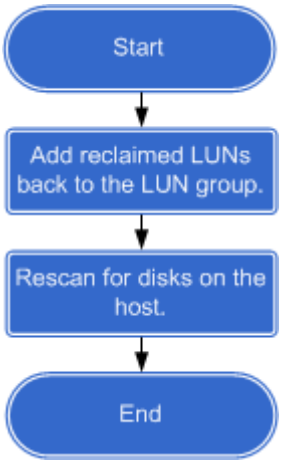


Figure 5-31 Emergency rollback procedure (partial reclamation)



5.10 Obtaining System Information

This section describes how to obtain system version information and ESN.

5.10.1 Obtaining Current System Version Information

You can use DeviceManager and the CLI to query and familiarize yourself with storage system version information so that you can quickly determine matching software versions based on the system version in maintenance.

Obtaining Current System Version Information Using DeviceManager

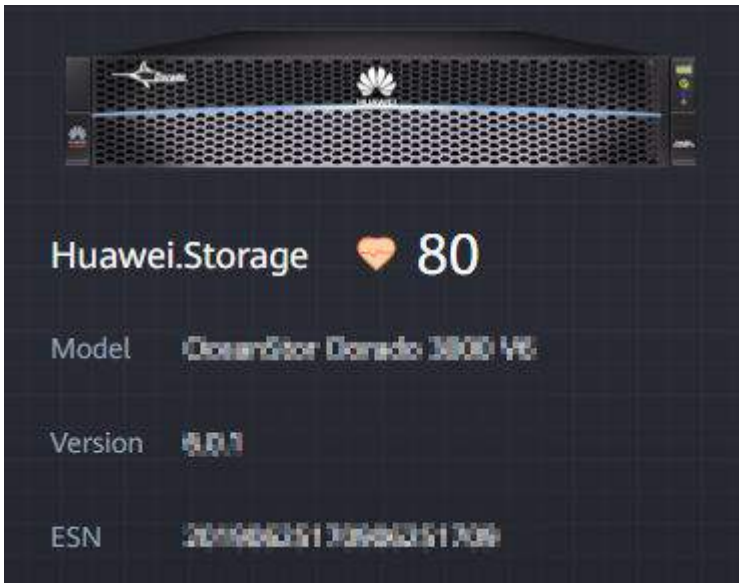
You can use DeviceManager to view the current storage system version.

Step 1 Log in to DeviceManager.

Step 2 In the navigation tree, click **Home**.

Step 3 In **Basic Information**, view **Version**, as shown in **Figure 5-32**.

Figure 5-32 Basic storage system information



You can then check the storage system version in the version mapping table to identify the UltraPath and SmartKit versions that match the storage system.

----End

Obtaining Current System Version Information Using the CLI

You can use the command-line interface (CLI) to query the storage system version to help you determine the software versions that match the storage system.

Step 1 Log in to the CLI as the super administrator.

Step 2 Run the **show system general** command to view the storage system version.

```
admin:/>show system general

System Name         : XXX.Storage
Health Status       : Normal
Running Status      : Normal
Total Capacity      : 3.186TB
SN                  : XXX
Location            :
Product Model       : XXX
Product Version     : VX00R00XCXX
High Water Level(%) : 80
Low Water Level(%)  : 20
WWN                 : XXX
Time                : 2015-07-07/15:34:05 UTC+08:00
Patch Version       : SPCXXX
```

In the command output, the value of **Product Version** is the version of the current storage system.

You can then check the storage system version in the version mapping table to identify the UltraPath and SmartKit versions that match the storage system.

----End

5.10.2 Obtaining System Historical Version Information

You can use the command-line interface (CLI) to query the historical versions of the storage system.

Prerequisites

You can successfully log in to the CLI on site.

Procedure

Step 1 Log in to the CLI as the super administrator.

Step 2 Run the **show upgrade package** command to view historical versions of the storage system.

```
admin:/>show upgrade package
Software Version

SN                   Name IP          Current Version History Version Type
-------------------- ---- ----------- --------------- --------------- ----------
XXXXXXXXXXXXXXXXXXXX 0A   10.94.80.72  VX00R00XCXX     --              Controller
XXXXXXXXXXXXXXXXXXXX 0B   10.94.80.73  VX00R00XCXX     --              Controller
HotPatch Version

SN                   Name IP          Current Version History Version Type
-------------------- ---- ----------- --------------- --------------- ----------
XXXXXXXXXXXXXXXXXXXX 0A   10.94.80.72  --              --              Controller
XXXXXXXXXXXXXXXXXXXX 0B   10.94.80.73  --              --              Controller
```

History Version indicates historical version information about the storage system, including the information about the software and hot patches.

----End

5.10.3 Obtaining the Storage Device ESN

The equipment serial number (ESN) is a character string that uniquely identifies a device. The ESN is required when you apply for licenses, report device repair, or configure eService.

Context

- You can query the ESN of a storage device on the information plate, on DeviceManager, or through the CLI.
- For a multi-controller storage system that contains two or more controller enclosures, the ESN of controller enclosure 0 is used as the ESN of the storage system. The ESN of the multi-controller storage system queried on DeviceManager or CLI through the management network port of any controller enclosure is always the ESN of controller enclosure 0. You are advised to use DeviceManager or CLI to query the ESN. If you want to query the ESN on the information plate, obtain the position of controller enclosure 0 on the system networking diagram used for controller expansion and then check the ESN on the information plate of controller enclosure 0.

Querying the ESN on the Information Plate

The information plate is located on the right side of the front panel of a controller enclosure, as shown in the following figures. Pull out the information plate from the controller enclosure to query the device information.

Figure 5-33 Information plate position of a 2 U controller enclosure

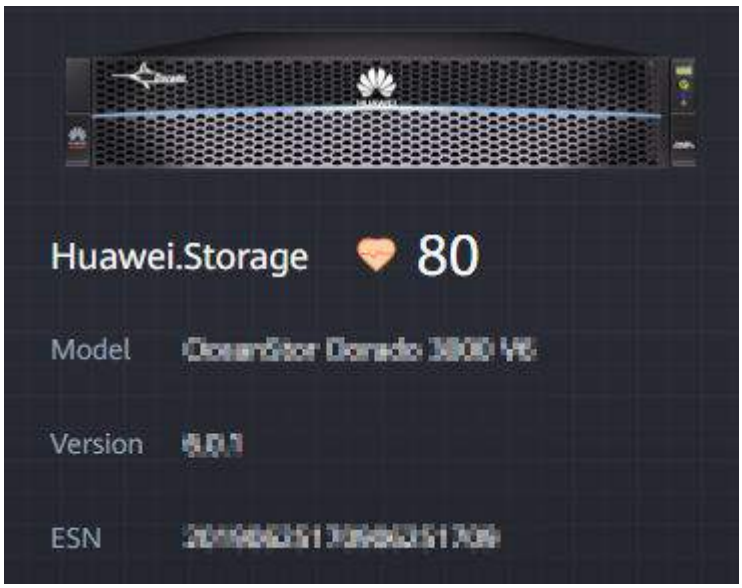
Figure 5-34 Information plate position of a 4 U controller enclosure

Querying the ESN on DeviceManager

Step 1 Log in to DeviceManager.

Step 2 In the navigation tree, click **Home**.

Step 3 In **Basic Information**, view **ESN**.



----End

Querying the ESN on the CLI

Step 1 Log in to the CLI.

Step 2 Run the **show system general** command to view the ESN, namely the **SN** field in the command output.

```
admin:/>showsystemgeneral
  System Name          : XXX.Storage
  Health Status        : Normal
  Running Status       : Normal
  Total Capacity       : 3.186TB
  SN                   : 2102XXXXXXXXXXXXXXXX
  Location             :
  Product Model        : XXXX
  Product Version      : VX00R00XCXX
  High Water Level(%) : 80
  Low Water Level(%)  : 30
  WWN                  : XXXX
  Time                 : 2018-07-07/15:34:05 UTC+08:00
  Patch Version        : SPCXXX SPHXXX
  Description          :
```

----End

5.11 Interconnecting Storage Devices with a Third-Party NMS

Huawei storage devices support SNMP and SMI-S interfaces that can be used for a third-party network management system (NMS) to manage Huawei storage devices.

Table 5-38 lists the protocol interfaces or plug-ins that can be used for a third-party NMS to interconnect with Huawei storage devices.

Table 5-38 Protocol interfaces or plug-ins used for interconnection

Name	Description	Reference
SMI-S	After installing the SMI-S provider on a third-party Windows/Linux server, users can use the SMI-S provider to manage Huawei storage systems.	*eSDK Storage SMI-S Provider Quick Start Guide*
SNMP	The SNMP protocol is used for a third-party NMS to view information about storage devices, including LUNs, ports, and storage pools.	• The **Configuring SNMP** section in the *Initialization Guide* specific to your product model. • The **Managing SNMP Community Strings** section in the *Administrator Guide* specific to your product model.
vCenter	OceanStor VMware vCenter Plug-in (vCenter plug-in for short) is a storage management plug-in developed based on vSphere Web Services Software Development Kit (SDK) and is used to manage Huawei storage devices through a vSphere client.	*eSDK Storage Quick Guide (vCenter, Plug-in)*
System Center	Storage Microsoft System Center Plug-in is a Huawei-developed plug-in for Microsoft System Center Operations Manager (SCOM) and is used to monitor Huawei storage devices.	*eSDK Storage Quick Guide (SCOM, Plug-in)*
REST	RESTful Applications Programming Interfaces (APIs) are open APIs provided by Huawei OceanStor DeviceManager based on Representational State Transfer (REST). Third-party developers can use RESTful APIs to access the open resources on OceanStor DeviceManager, such as alarms, performance data, and resource allocation information.	*REST Interface Reference*

NOTE

- Carrier users: log in to Huawei Carrier Product and Service Support (**https://support.huawei.com/carrierindex/en/hwe/index.html**). Search for and download the required document of the latest version.
- Enterprise users: log in to Huawei Enterprise Product and Service Support (**https://support.huawei.com/enterprise/en/index.html**). Search for and download the required document of the latest version.

5.12 Connection Change Between the Storage System and an Application Server

After the connection between the storage system and an application server changes, relevant configurations on the storage system and the application server must be changed. The purpose is to allow the application server to use storage space through the new connection channels. This chapter describes how to change configurations after replacing an HBA.

An HBA can be replaced in either online or offline mode. The main configuration procedures after an HBA replacement are shown in **Figure 5-35** and **Figure 5-36**.

Figure 5-35 Configuration procedure after an HBA offline replacement

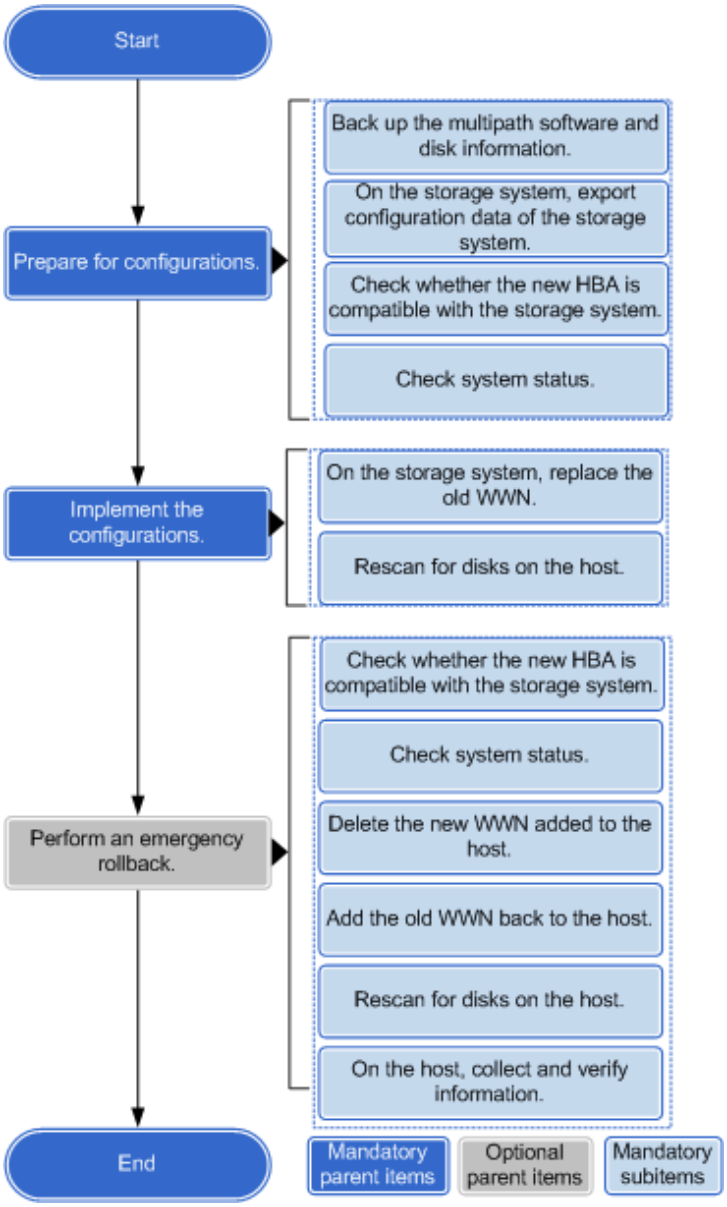
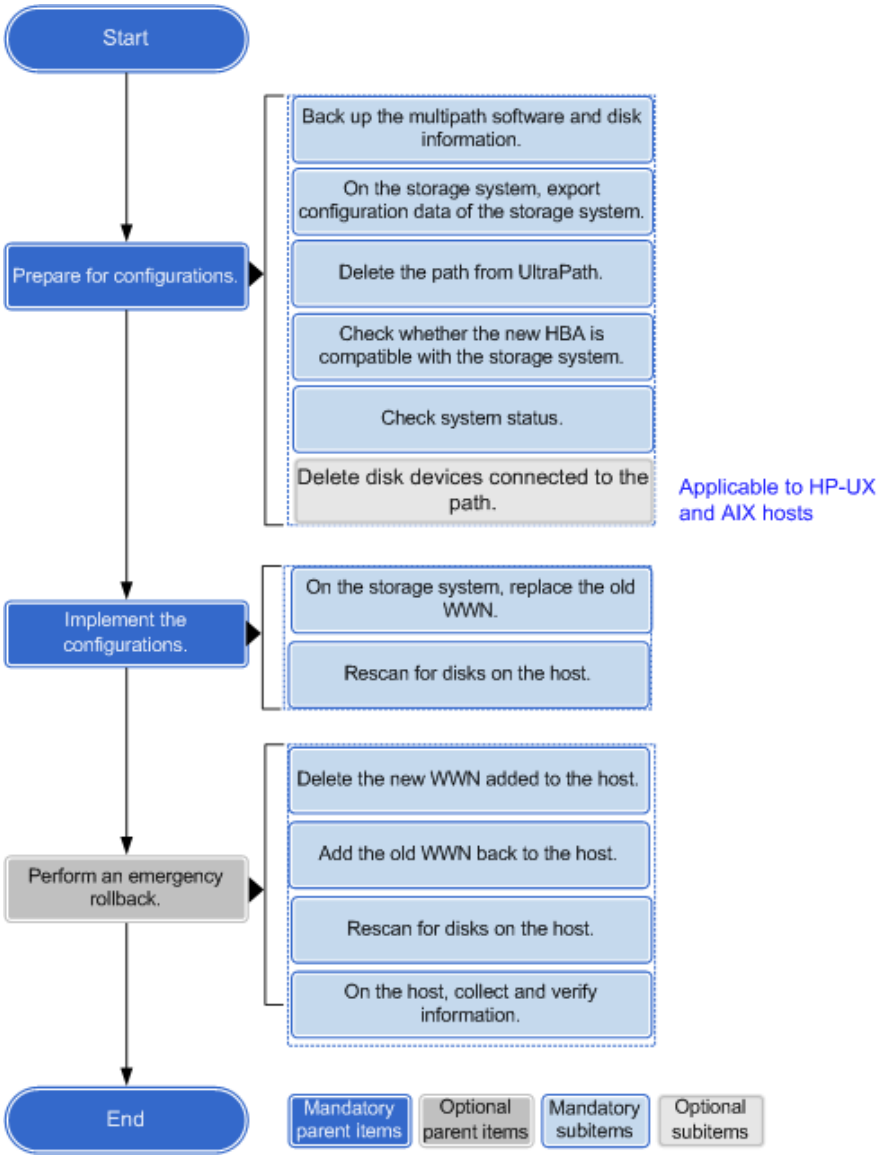


Figure 5-36 Configuration procedure after an HBA online replacement



5.12.1 Configurations and Operations After an HBA Replacement (in Windows)

This section describes after replacing the HBA of a Windows host, how to configure the HBA on the storage system and the host to make it work correctly.

5.12.1.1 Preparing for Configuration (in Windows)

Before configuring the new HBA, you must finish preparatory work such as backing up host multipath and disk information and checking the storage device's running status to ensure that the space configuration can be successfully implemented.

Prerequisites

- The UltraPath software has been installed on the host.
- The old HBA of the host has been replaced.

Procedure

Step 1 Back up UltraPath and disk information.

1. Run **upadm show vlun** and **upadm show path** to view and back up the UltraPath status information.
2. Back up disk information.
   a. Log in to the Windows Server 2008 application server as an administrator.
   b. Press **Windows+R** (if the operation is performed remotely, perform it in full screen mode) to open the **Run** dialog box.
   c. Type **diskmgmt.msc** and press **Enter**.
   d. On the **Disk Management** page that is displayed, view the host disk information.
3. Back up HBA information.

   If the **fcinfo** software is installed on the host, do the following:

   a. Press **Window+R** to open the **Run** dialog box.
   b. Type **cmd** and press **Enter**.
   c. In the command window that is displayed, run **fcinfo** to view the HBA information.

   If the **fcinfo** software is not installed on the host, do the following:

   a. Press **Window+R** to open the **Run** dialog box.
   b. Type **devmgmt.msc** and press **Enter** to open the **Device Manager** page.
   c. Select **Storage controllers** and double-click **Fibre Channel Adapter**. On the **Attribute** page, view the vendor and version information.

Step 2 Check the storage system status. If there are alarms, clear them and then proceed to the next step.

Step 3 On the storage system, export the storage system configuration data.

1. Log in to the command-line interface (CLI) of the storage system using PuTTY.

   NOTE

   The default super administrator name is **admin**.
2. Run **export running_data** to export and save the current configuration file.

Step 4 **Optional:** If online replacement is used, you need to delete path information.

- If the HBA is replaced due to a failure, do the following:
  a. Run **upadm show path** to check whether the path status of the faulty HBA is **Fault**. If the path status is **Fault**, run **upadm clear obsolete_path path_id=***?* to delete the faulty path. Specify the path whose status is **Fault** using its **path_id**.

b. Run **upadm show iostat array_id=***?* to monitor the load balancing of paths. Specify the storage device using the **array_id** parameter.

If I/Os are evenly distributed in the remaining paths and there are no errors after 30 seconds, press **Ctrl+C** to exit.

c. Run **upadm show path** to show UltraPath status information.

The information about the deleted paths should not appear in the execution result.

- If the HBA is replaced proactively, do the following:

a. Run **upadm show path** and **upadm show vlun** to show UltraPath status information.

b. Run **upadm set pathstate=disable** to disable all paths connected to the old HBA. Specify the path to be disabled using its **path_id**.

c. Run **upadm show iostat array_id=***?* to monitor the load balancing of paths. Specify the storage device using the **array_id** parameter.

If I/Os are evenly distributed in the remaining paths and there are no errors after 30 seconds, press **Ctrl+C** to exit.

d. Run **upadm show path** to show UltraPath status information.

In the execution result, the states of all paths connected to the old HBA are **Disable**.

Step 5 Check whether the new HBA is compatible with the storage system.

1. Press **Window+R** to open the **Run** dialog box.
2. Type **devmgmt.msc** and press **Enter** to open the **Device Manager** page.
3. Select **Storage controllers** and double-click **Fibre Channel Adapter**. On the **Attribute** page, view the vendor and version information.

Step 6 Check the host running status.

1. Check whether any error exists on the host.

a. Press **Windows+R** (if the operation is performed remotely, perform it in full screen mode) to open the **Run** dialog box.

b. Run **eventvwr.msc** and **devmgmt.msc** and press **Enter**.

c. In the **Event Viewer** and **Device Manager** windows, check whether any error exists on the host. If there are errors, remove them and then proceed to the next step.

2. Check disk path status.

a. Run **upadm show vlun** to query the status of all vLUNs. Confirm that the status of all vLUNs is **Normal**.

b. Run **upadm show path** to check whether the system path status is **Normal**. If the status of a path is **Degrade**, check the path connection status on the storage device.

Step 7 On the switch, check whether the zoning of the new HBA is complete.

----End

5.12.1.2 Configurations and Operations (in Windows)

Prerequisites

- The old HBA has been replaced and the new HBA has been correctly installed.
- The WWNs of the old and new HBAs have been obtained.
- UltraPath has been installed on the application server.

Procedure

Step 1 On the storage system, replace the old WWN.

1. Run **show initiator initiator_type=FC** to view the connection status between the HBA and the storage device and obtain the ID of the host to which the old HBA belongs.

   ```
   WWN              Running Status       Free      Alias     Host ID       Multipath Type
   ---------------- -------------------- -----     -------   ----------    ------------------
   100000000000*    Online               Yes       --        --            Default
   ```

2. Run **remove host initiator initiator_type=FC** to remove the WWN of the old HBA. Specify the WWN of the old HBA using the **wwn** parameter.
3. Run **add host initiator host_id=***?* **initiator_type=FC wwn=***?* to add the new WWN to the host. Specify the host and WWN of the new HBA using the **host_id** and **wwn** parameters.
4. Run **show initiator initiator_type=FC**. If in the command output, the WWN status of the new HBA is not **Free**, then the replacement is successful.

Step 2 Scan for disks on the host.

1. Press **Windows+R** (if the operation is performed remotely, perform it in full screen mode) to open the **Run** dialog box.
2. Type **devmgmt.msc** and press **Enter**.
3. In the **Device Manager** window that is displayed, click **View** and select **Show hidden devices**.
4. Right-click **Disk Drives** > **Scan for hardware changes**. The system will scan for disks automatically.
5. Check whether the number of newly generated UltraPath_Disks is the same as that of mapped LUNs. If they are not the same, check the LUN mapping and path connection status on the storage device.
6. Check whether the number of newly generated SCSI disks (SCSI Disk Devices on the Huawei storage device) is an integral multiple of the number of system paths. If not, check the LUN mapping and path connection status on the storage device.

   NOTE

   You can run **upadm show vlun** to query the number of system paths.

Step 3 Run **upadm show iostat array_id=***?* to monitor the load balancing of paths. Specify the storage device using the **array_id** parameter.

If I/Os are evenly distributed in all paths and there are no errors after 30 seconds, press **Ctrl+C** to exit.

----End

5.12.2 Configurations and Operations After an HBA Replacement (in Linux)

This section describes after replacing the HBA of a Linux host, how to configure the HBA on the storage system and the host to make it work correctly.

5.12.2.1 Preparing for Configuration (in Linux)

Before configuring the new HBA, you must finish preparatory work such as backing up host multipath and disk information and checking the storage device's running status to ensure that the space configuration can be successfully implemented.

Prerequisites

- The UltraPath software has been installed on the host.
- The old HBA of the host has been replaced.

Procedure

Step 1 Back up UltraPath and disk information.

1. Run **upadmin show vlun** and **upadmin show path** to view and back up the UltraPath status information.
2. Run **vgdisplay** and **vgs** to view and back up volume group (VG) information.
3. Run **pvs -a** to back up physical volume (PV) information.
4. Run **fdisk -l|grep "Disk "** and **systool -c fc_host -v** to back up disk and HBA information.

Step 2 Check the storage system status. If there are alarms, clear them and then proceed to the next step.

Step 3 On the storage system, export the storage system configuration data.

1. Log in to the command-line interface (CLI) of the storage system using PuTTY.

   NOTE

   The default super administrator name is **admin**.

2. Run **export running_data** to export and save the current configuration file.

Step 4 **Optional:** If online replacement is used, you need to delete path information.

- If the HBA is replaced due to a failure, do the following:
  a. Run **upadmin show path** to check whether the path status of the faulty HBA is **Fault**. If the path status is **Fault**, run **upadmin clear obsolete_path** to delete the faulty path. Specify the path whose status is **Fault** using its **path_id**.
  b. Run **upadmin show iostat array_id=***?* to monitor the load balancing of paths. Specify the storage device using the **array_id** parameter.

     If I/Os are evenly distributed in the remaining paths and there are no errors after 30 seconds, press **Ctrl+C** to exit.

c. Run **upadmin show path** to show UltraPath status information.

The information about the deleted paths should not appear in the execution result.

- If the HBA is replaced proactively, do the following:
  a. Run **upadmin show path** and **upadmin show vlun** to show UltraPath status information.
  b. Run **upadmin set pathstate=disable** to disable all paths connected to the old HBA. Specify the path to be disabled using its **path_id**.
  c. Run **upadmin show iostat array_id=***?* to monitor the load balancing of paths. Specify the storage device using the **array_id** parameter.

     If I/Os are evenly distributed in the remaining paths and there are no errors after 30 seconds, press **Ctrl+C** to exit.
  d. Run **upadmin show path** to show UltraPath status information.

     In the execution result, the states of all paths connected to the old HBA are **Disable**.

Step 5 Run **systool -c fc_host -v** to check whether the new HBA is compatible with the storage system. If it is not compatible with the storage system, replace it.

Step 6 Check the system status and check whether there are disks or tapes connected to the HBA.

1. Run **tail -200 /var/log/messages** to check the storage system status. If an error exists on the HBA or any disk, remove it and proceed to the next step.
2. Run **grep scsiY /proc/scsi/scsi** to check whether there are disks or tapes connected to the new HBA, where *scsiY* indicates the device file name of the new HBA.

   There should be no disk or tape under *scsiY*.
3. Run **systool -c fc_host -v** to obtain the WWN of the new HBA and record it, where *port_name* indicates the WWN of the new HBA.

Step 7 On the switch, check whether the zoning of the new HBA is complete.

----End

5.12.2.2 Configurations and Operations (in Linux)

Prerequisites

- The old HBA has been replaced and the new HBA has been correctly installed.
- The WWNs of the old and new HBAs have been obtained.
- UltraPath has been installed on the application server.

Procedure

Step 1 On the storage system, replace the old WWN.

1. Run **show initiator initiator_type=FC** to view the connection status between the HBA and the storage device and obtain the ID of the host to which the old HBA belongs.

WWN	Running Status	Free	Alias	Host ID	Multipath Type


```
-----------------  --------------------  -----  --------  -----------  ------------------
100000000000*      Online                Yes    --        --           Default
```

2. Run **remove host initiator initiator_type=FC** to remove the WWN of the old HBA. Specify the WWN of the old HBA using the **wwn** parameter.
3. Run **add host initiator host_id=***?* **initiator_type=FC wwn=***?* to add the new WWN to the host. Specify the host and WWN of the new HBA using the **host_id** and **wwn** parameters.
4. Run **show initiator initiator_type=FC**. If in the command output, the WWN status of the new HBA is not **Free**, then the replacement is successful.

Step 2 Scan for disks on the host.

1. Run **upRescan** to scan for disks.

```
#upRescan
  Begin to delete LUNs whose mappings do not exist
  Begin to delete LUNs whose mappings are changed
```

2. Run **upadmin show vlun** to check whether the number of disks managed by UltraPath is the same as planned.
3. Run **upadmin show path** to check whether the disk path status is normal. If you find a path whose status is **Degrade**, check the path connection status on the storage device.

Step 3 Run **upadmin show iostat array_id=***?* to monitor the load balancing of paths. Specify the storage device using the **array_id** parameter.

If I/Os are evenly distributed in all paths and there are no errors after 30 seconds, press **Ctrl+C** to exit.

----End

5.12.3 Configurations and Operations After an HBA Replacement (in AIX)

This section describes after replacing the HBA of an AIX host, how to configure the HBA on the storage system and the host to make it work correctly.

5.12.3.1 Preparing for Configuration (in AIX)

Before configuring the new HBA, you must finish preparatory work such as backing up host multipath and disk information and checking the storage device's running status to ensure that the space configuration can be successfully implemented.

Prerequisites

- The UltraPath software has been installed on the host.
- The old HBA of the host has been replaced.

Procedure

Step 1 Back up UltraPath and disk information.

1. Run **upadm show vlun** and **upadm show path** to view and back up the UltraPath status information.

2. Run **lsvg** and **lsvg vgname** to view and back up volume group (VG) information where **vgname** represents the name of the VG.
3. Run **pvdisplay** to view physical volume (PV) information.
4. Run **lsdev -Cc disk** and **lsdev -Cc adapter** respectively to back up disk and HBA information.

Step 2 Check the storage system status. If there are alarms, clear them and then proceed to the next step.

Step 3 On the storage system, export the storage system configuration data.

1. Log in to the command-line interface (CLI) of the storage system using PuTTY.

   NOTE

   The default super administrator name is **admin**.

2. Run **export running_data** to export and save the current configuration file.

Step 4 **Optional:** If online replacement is used, you need to delete path information.

- If the HBA is replaced due to a failure, do the following:
  a. Run **upadm show path** to show UltraPath status information.
  b. Run **rmpath -dl hdiskX -p fscsiY** to delete paths whose parent is fscsiY, where **hdiskX** and **fscsiY** indicate the device file name of a host disk and a to-be-replaced HBA respectively.
  c. Run **upadm show iostat array_id=***?* to monitor the load balancing of paths. Specify the storage device using the **array_id** parameter.

     If I/Os are evenly distributed in the remaining paths and there are no errors after 30 seconds, press **Ctrl+C** to exit.

     If I/Os are evenly distributed in the remaining paths and there are no errors after 30 seconds, press **Ctrl+C** to exit.
  d. Run **upadm show path** to show UltraPath status information.

     The information about the deleted paths should not appear in the execution result.
- If the HBA is replaced proactively, do the following:
  a. Run **upadm show path** and **upadm show vlun** to show UltraPath status information.
  b. Run **chpath -s disable -l hdiskX -p fscsiY** to disable paths whose parent is fscsiY, where **hdiskX** and **fscsiY** indicate the device file name of a host disk and a to-be-replaced HBA.
  c. Run **upadm show iostat array_id=***?* to monitor the load balancing of paths. Specify the storage device using the **array_id** parameter.

     If I/Os are evenly distributed in the remaining paths and there are no errors after 30 seconds, press **Ctrl+C** to exit.
  d. Run **rmpath -dl hdiskX -p fscsiY** to delete all disabled links.
  e. Run **upadm show path** to show UltraPath status information.

     The information about the deleted paths should not appear in the execution result.

Step 5 **Optional:** If the HBA is replaced online, you need to delete disk devices connected to the links.

1. Run **lsdev -Cc disk** and **lsdev -Cc disk | wc -l** to view system disk status.
2. Run **lsdev -p fscsiY** and **lsdev -p fscsiY -c disk -F name | xargs -n1 rmdev -dl** to delete disks connected to the path.
3. Rerun **lsdev -Cc disk** and **lsdev -Cc disk | wc -l** to view system disk information in which the deleted disks should not exist.

Step 6 Check whether the new HBA is compatible with the storage system.

1. Run **lscfg -vpl fcsY | grep Address** to check whether the WWN of the new HBA is as planned, where *fcsY* represents the new HBA.
2. Run **fcstat fcsY** to check whether the HBA model is compatible with the storage system.

NOTE

Systems earlier than AIX 5.3 TL03 do not support the **fcstat** command.

Step 7 Check the system status and check whether there are disks or tapes connected to the HBA.

1. Run **errpt** to check the storage system status. If an error exists on the HBA or any disk, remove it and proceed to the next step.
2. Run **lsdev -p fcsY** and **lsdev -p fscsiY** to check whether there are disks or tapes connected to the new HBA, where *fcsY* indicates the device file name of the new HBA and *fscsiY* indicates the subdevice of *fcsY*.

   There should be no disk or tape under *fscsiY*.
3. Modify the properties of the device *fscsiY*.
   a. Run the **lsattr -El fscsiY** command to check whether **fc_err_recov** is **fast_fail** and **dyntrk** is **yes**. If yes, go to **Step 7.4**. If no, go to **Step 7.3.b**.
   b. Run the **rmdev -l fscsiY -R** command to clear the configuration of device *fscsiY*.
   c. Run the **chdev -l fscsiY -a fc_err_recov=fast_fail** and **chdev -l fscsiY -a dyntrk=yes** commands to modify the properties of device *fscsiY*.
4. Run **cfgmgr -vl fcsY** to scan for the HBA and generate the *fscsiY* device.
5. Run **lsattr -El fcsY** and **lsattr -El fscsiY** to check whether device parameters are changed successfully.
6. Run **lscfg -vpl fcsY | grep Address** to view the WWN of the new HBA and record it.

Step 8 On the switch, check whether the zoning of the new HBA is complete.

----End

5.12.3.2 Configurations and Operations (in AIX)

Prerequisites

- The old HBA has been replaced and the new HBA has been correctly installed.
- The WWNs of the old and new HBAs have been obtained.

- UltraPath has been installed on the application server.

Procedure

Step 1 On the storage system, replace the old WWN.

1. Run **show initiator initiator_type=FC** to view the connection status between the HBA and the storage device and obtain the ID of the host to which the old HBA belongs.

```
WWN              Running Status       Free      Alias      Host ID        Multipath Type
-----------------  -------------------  -----  -------  ----------  ------------------
100000000000*      Online               Yes       --         --            Default
```

2. Run **remove host initiator initiator_type=FC** to remove the WWN of the old HBA. Specify the WWN of the old HBA using the **wwn** parameter.
3. Run **add host initiator host_id=***?* **initiator_type=FC wwn=***?* to add the new WWN to the host. Specify the host and WWN of the new HBA using the **host_id** and **wwn** parameters.

   NOTE

   If the system reports a failure in querying the WWN of a new HBA, run the **cfmgr** command and then the **add host initiator host_id=***?* command.
4. Run **show initiator initiator_type=FC**. If in the command output, the WWN status of the new HBA is not **Free**, then the replacement is successful.

Step 2 Scan for disks on the host.

1. Run **lsdev -Cc disk** and **lsdev -Cc disk | wc -l** to show disks on the host.
2. Run **cfgmgr -vl fcsY** to scan for the HBA and recognize the storage device.
3. Rerun **lsdev -Cc disk** and **lsdev -Cc disk | wc -l** and compare the result with that in **Step 2.1**. The number of newly generated device files should be the same as expected, and the vendors should all be **Huawei**.
4. Run **upadm show vlun** and compare the result with that in **Step 2.1** to check whether the number of disks managed by UltraPath is the same as planned.
5. Run **upadm show path** to check whether the disk path status is **Enable**. If you find a path whose status is **Degrade**, check the path connection status on the storage device.

Step 3 Run **upadm show iostat array_id=***?* to monitor the load balancing of paths. Specify the storage device using the **array_id** parameter.

If I/Os are evenly distributed in all paths and there are no errors after 30 seconds, press **Ctrl+C** to exit.

----End

5.12.4 Configurations and Operations After an HBA Replacement (in HP-UX)

This section describes after replacing the HBA of an HP-UX host, how to configure the HBA on the storage system and the host to make it work correctly.

5.12.4.1 Preparing for Configuration (in HP-UX)

Before configuring the new HBA, you must finish preparatory work such as backing up host multipath and disk information and checking the storage device's running status to ensure that the space configuration can be successfully implemented.

Prerequisites

The old HBA of the host has been replaced.

Procedure

Step 1 Back up the NMP multipath and disk information.

1. Run **scsimgr get_attr -a leg_mpath_enable** to view and back up the multipath status.
2. Run **vgdisplay -v** to view and back up volume group (VG) information.
3. Run **pvdisplay** to view physical volume (PV) information.
4. Run **ioscan -fkNC disk** and **ioscan -fnkC fc** to back up disk and HBA information.

Step 2 Check the storage system status. If there are alarms, clear them and then proceed to the next step.

Step 3 On the storage system, export the storage system configuration data.

1. Log in to the command-line interface (CLI) of the storage system using PuTTY.

   NOTE

   The default super administrator name is **admin**.

2. Run **export running_data** to export and save the current configuration file.

Step 4 **Optional:** If online replacement is used, you need to delete link information from the NMP multipath software.

- If the HBA is replaced due to a failure, do the following:
  a. Run **scsimgr lun_map -D /dev/rdisk/diskX** to view disk path information, where **diskX** represents a disk on the host.
  b. Run **ioscan -fnkC fc**, **ioscan -kfNC tgtpath**, **ioscan -P health -H hw_path**, and **rmsf -H hw_path** to delete links, where **hw_path** indicates the path of the HBA to be replaced.
  c. Run **sar -L 1 30** to monitor link I/Os.
  d. Run **scsimgr lun_map -D /dev/rdisk/diskX** to view disk path information, where **diskX** represents a disk on the host.

     The information about the deleted links should not appear in the command output.
- If the HBA is replaced proactively, do the following:
  a. Run **scsimgr lun_map -D /dev/rdisk/diskX** to view disk path information, where **diskX** represents a disk on the host.

b. Run **ioscan -fnkC fc**, **scsimgr -f disable -H hw_path** and **ioscan -P health -H hw_path** to disable links, where **hw_path** indicates the path of the HBA to be replaced.

c. Run **rmsf -H hw_path** to delete all disabled links.

d. Run **sar -L 1 30** to monitor link I/Os.

e. Run **scsimgr lun_map -D /dev/rdisk/diskX** to view disk path information. The information about the deleted links should not appear in the command output.

Step 5 **Optional:** If the HBA is replaced online, you need to delete disk devices connected to the links.

1. Run **ioscan -fnkC disk** and **ioscan -fnkC disk | grep -i HUAWEI | wc -l** to view system disk status.
2. Run **ioscan -fnkC fc** and **ioscan -fnk -C disk -H hw_path | grep -i HUAWEI | awk '{ print $3}' | xargs -n1 rmsf -C disk -H** to delete disk devices connected to the links, where **hw_path** indicates the path of the HBA to be replaced.
3. Run **ioscan -fnkC disk** and **ioscan -fnkC disk | grep -i HUAWEI | wc -l** again to check the system disk status, which should not contain the status of deleted disk devices.

Step 6 Check whether the new HBA is compatible with the storage system.

1. Run **fcmsutil /dev/fcdY** to check whether the WWN of the new HBA is as planned, where *fcdY* represents the new HBA.
2. Run **fcmsutil /dev/fcdY vpd** to check whether the HBA is compatible with the storage system.

Step 7 Check the system status and check whether there are disks or tapes connected to the HBA.

1. Run **tail -200 /var/adm/syslog/syslog.log** to check the storage system status. If an error exists on the HBA or any disk, remove it and proceed to the next step.
2. Run **ioscan -fnkC fc** and **ioscan -fnkH HW Path** to check whether there are disks or tapes connected to the new HBA, where *HW Path* indicates the path of the HBA to be replaced.

   There should be no disk or tape under *fcdY*.

Step 8 On the switch, check whether the zoning of the new HBA is complete.

----End

5.12.4.2 Configurations and Operations (in HP-UX)

Prerequisites

- The old HBA has been replaced and the new HBA has been correctly installed.
- The WWNs of the old and new HBAs have been obtained.

Procedure

Step 1 On the storage system, replace the old WWN.

1. Run **show initiator initiator_type=FC** to view the connection status between the HBA and the storage device and obtain the ID of the host to which the old HBA belongs.

```
WWN              Running Status      Free    Alias    Host ID      Multipath Type
---------------- ------------------- ------- -------- ---------- ------------------
100000000000*    Online              Yes     --       --         Default
```

2. Run **remove host initiator initiator_type=FC** to remove the WWN of the old HBA. Specify the WWN of the old HBA using the **wwn** parameter.
3. Run **create initiator fc wwn=***?* to create an FC initiator. **wwn** is the WWN of the new HBA.
4. Run **add host initiator host_id=***?* **initiator_type=FC wwn=***?* to add the new WWN to the host. Specify the host and WWN of the new HBA using the **host_id** and **wwn** parameters.
5. Run **show initiator initiator_type=FC**. If in the command output, the WWN status of the new HBA is not **Free**, then the replacement is successful.

Step 2 Scan for disks on the host.

1. Run **ioscan -fnNkC disk** and **vgdisplay -v** to show the disks and volume groups (VGs) on the host.
2. Run **ioscan -fnC disk** to scan for disks.
3. Rerun **ioscan -fnkC disk** and compare the result with that in **Step 2.1**. The number and the types of newly generated devices should be the same as planned.
4. Run **insf -eC disk** and confirm that the LUN device files are generated.
5. Rerun **ioscan -fnkC disk** and compare the result with that in **Step 2.1**. The number and the types of newly generated devices should be the same as planned.
6. If the NMP software is installed on the host, do the following:
   a. Run **scsimgr get_attr -a leg_mpath_enable** and confirm that the NMP is enabled.
   b. Run **ioscan -funC disk** to view the number of disk paths when NMP is not enabled.
   c. Rerun **ioscan -funNC disk** and confirm that the number of newly generated aggregated disks is the same as planned.
   d. Run **ioscan -m dsf** to view the mappings between persistent disks and legacy disks.
   e. Run **scsimgr lun_map -D /dev/rdisk/diskX** to view disk path information with NMP enabled, where **diskX** represents a disk on the host.

Step 3 Run **sar -L 1 30** to monitor path I/Os.

If I/Os are evenly distributed in all paths and there are no errors after 30 seconds, press **Ctrl+C** to exit.

----End

5.12.5 Emergency Rollback of Configurations and Operations After Replacing an HBA

After replacing an HBA, if you encounter an abnormality or fault during configurations and operations on the host or storage system, you can perform an emergency rollback as instructed in this section.

The main procedures for an emergency rollback are shown in **Figure 5-37** and **Figure 5-38**.

Figure 5-37 Emergency rollback procedure after an offline HBA replacement

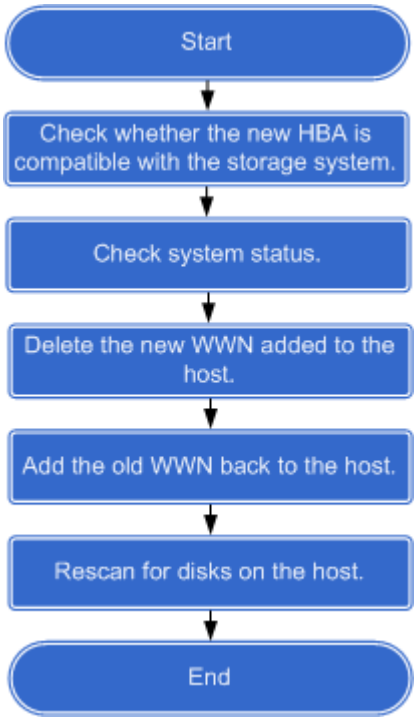


Figure 5-38 Emergency rollback procedure after an online HBA replacement

5.13 Changing IP Addresses of Management Network Ports

This section describes how to access a storage system through the IP addresses of the management network ports to configure and manage the storage system.

Prerequisites

Ensure that the temporary maintenance terminal used for initial configuration has been connected to the management ports of the storage device, and the IP address of the maintenance terminal and the default IP address of the management port are on the same network segment.

Context

- The default internal heartbeat IP addresses are **127.127.127.10** and **127.127.127.11** for a dual-controller storage system, and the subnet mask is **255.255.255.0**. The default internal heartbeat IP addresses are **127.127.127.10**, **127.127.127.11**, **127.127.127.12**, **and 127.127.127.13** for a four-controller storage system, and the subnet mask is **255.255.255.0**.
- The default IP addresses of maintenance network ports are **172.31.128.101** and **172.31.128.102**, and the subnet mask is **255.255.0.0**.

Precaution

- After the IP addresses of the management ports are modified, communication between the maintenance terminal and the storage device is down. Therefore, you are advised to first modify the IP addresses of controllers' management ports that are not directly connected to the maintenance terminal.
- The IP addresses of management network ports and internal heartbeat IP addresses must be on different network segments. Otherwise, route conflicts may occur. For a dual-controller system, you cannot use IP addresses that belong to the **127.127.127.XXX** network segment. For a four-controller storage system, you cannot set IP addresses that belong to the **127.127.127.XXX**, **172.16.126.XXX**, **172.16.127.XXX**, and **172.16.128.XXX** network segments.

  NOTE

  - 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.
  - Internal heartbeat links are established between controllers for these controllers to detect each other's working status. You do not need to separately connect cables. In addition, internal heartbeat IP addresses have been assigned before delivery, and you cannot change these IP addresses.
- The IP addresses of both management network ports and those of maintenance network ports must be on different network segments. You cannot use IP addresses that belong to the **172.31.XXX.XXX**. Otherwise, route conflicts may occur. You are advised to only connect the management network port to the network.

- By default, IP addresses of the management network ports and those of the service network ports are on different network segments. If they are in the same network segment, some functions of the storage system may be unavailable. It is strongly recommended that you do not set them on the same network segment.

Procedure

Step 1 Log in to DeviceManager.

Step 2 On the right navigation bar, choose **System > Hardware > Devices**.

Step 3 Click the controller enclosure where the management port resides.

Step 4 Click  to switch to the rear view.

Step 5 Click the management port whose information you want to view.

NOTICE

After the IP addresses of the management ports are modified, communication between the maintenance terminal and the storage device is down. Therefore, you are advised to first modify the IP addresses of controllers' management ports that are not directly connected to the maintenance terminal.

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

Step 6 Modify the IP address of management network port.

1. Click **Modify**.
2. In the **IPv4 Address** or **IPv6 Address** text box, enter an IP address for the management network port.
3. In the **Subnet Mask** or **Prefix** area, enter the subnet mask or prefix of the management network port.
4. In the **IPv4 Gateway** or **IPv6 Gateway** text box, enter a gateway of the IP address for the management network port.

Step 7 Confirm the IP address of management network port modification.

1. Click **Apply**.

   The security alert dialog box is displayed.
2. Confirm the information in the dialog box and select **I have read and understood the consequences associated with performing this operation**.
3. Click **OK**.

Step 8 Perform **Step 3** to **Step 7** again to modify other management port IP addresses.

----End

5.14 Connecting a Storage System to the DNS Server

After a storage system is connected to a DNS server, the storage can access other network devices through the DNS server. This operation enables you to configure a system management IP address for the active or standby DNS.

Prerequisites

- The DNS has been configured and is running properly.
- Port 53 of the TCP/UDP protocol between the storage system and the DNS server is enabled.

Context

- A DNS server is used to resolve host names in a domain.
- If you want to configure a standby DNS server, keep the domain names of the active and standby servers consistent.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Settings** > **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

   Configure the standby DNS IP address 1 first and then the standby DNS IP address 2.

Step 4 Click **Save**.

----End

5.15 Expanding Performance Layers, Storage Pools, and LUNs and Modifying File System Capacity

After adding storage components, perform necessary configurations on the storage system and application server to allocate the added storage space to system services.

NOTE

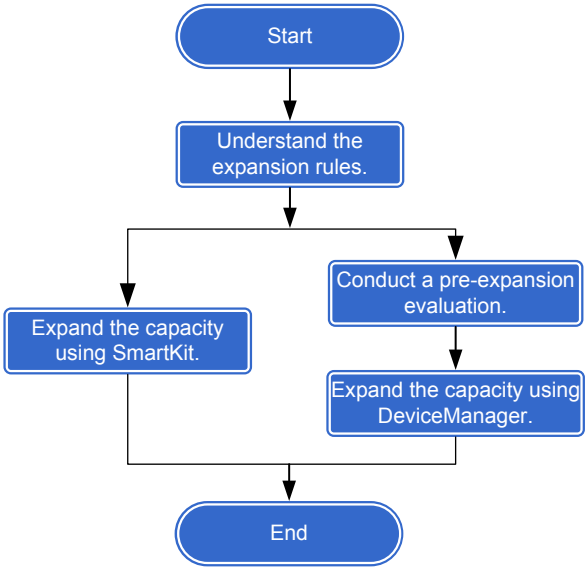
This section describes how to expand capacity of performance layers, storage pools, and LUNs, how to create LUNs, as well as modify capacity of file systems. For details about how to create storage pools, see "Creating a Storage Pool" in the *Basic Storage Service Configuration Guide* specific to your product model and version.

5.15.1 Expanding the Capacity of a Performance Layer or Storage Pool

To use the added storage space, you must first add the space to a performance layer or storage pool to expand its capacity.

The storage system supports storage pool expansion using SmartKit or DeviceManager. SmartKit is recommended.

Process for Expanding the Capacity of a Storage Pool



5.15.1.1 Rules for Expanding the Capacity of a Performance Layer or Storage Pool

This section describes the rules for expanding the capacity of a performance layer or storage pool.

Capacity Expansion Rules

- A storage pool or performance layer supports a maximum of two types of disks. The performance layer supports SSDs and SCM drives, and the storage pool supports SAS and NL-SAS disks.
- The type of disks that you want to add to a storage pool must be the same as that of disks in the storage pool.
- Disks from a maximum of two controller enclosures can be added to a storage pool.
- Disks from multiple controller enclosures can be added to a performance layer.
- HDDs cannot be added to all-flash storage pools that are using the data reduction functions.
- Self-encrypting and non-encrypting disks cannot coexist in a storage pool or performance layer.
- When expanding a storage pool that belongs to a single controller enclosure, if the used subscribed capacity of the storage pool has reached the maximum effective capacity of a controller enclosure, you are advised to use the disks that belong to the new controller to expand the storage pool.
- If member disks in a performance layer or storage pool are from only one controller enclosure, you can select disks that belong to other controller enclosures when expanding the performance layer or storage pool. Ensure that the number and capacity of disks that belong to the two controller enclosures in the storage pool are the same.
- A performance layer or storage pool supports disks of two different capacity specifications, but you can add disks of only one qualified specification at a time. The details are as follows:
  - When expanding the capacity of a storage pool or performance layer in a storage system with one controller enclosure, add disks of only one qualified specification at a time.
    - If the storage pool or performance layer contains disks of only one capacity specification, you can either add disks of the same type and capacity specification as the existing ones (recommended) or add disks of the same type but a larger capacity specification than the existing ones.

      For example, if a storage pool or performance layer contains only 960 GB disks, you can add either 960 GB disks (recommended) or disks greater than 960 GB.
    - If the storage pool or performance layer contains disks of two capacity specifications, you can only add disks of the greater capacity specification.

      For example, if a storage pool or performance layer contains both 960 GB and 1.92 TB disks, you can only add 1.92 TB disks for capacity expansion.
  - When expanding the capacity of a storage system with two or more controller enclosures, you must follow all the capacity expansion rules for a single controller enclosure storage system. In addition, if a storage pool or performance layer contains disks owned by two or more controller

enclosures, ensure that all controller enclosures are the same in terms of the slots for installing expansion modules, ports for connecting disk enclosures, number of disk enclosures, disk enclosure layout, as well as disk type and quantity.

- If the capacity specification of the disks to be added is greater than that of the disks in the storage pool or performance layer, you can use **eDesigner** to calculate the minimum number of disks to be added.
- For OceanStor 5310, 5510, and 5610, if four controllers in a cluster come from two controller enclosures, the member disks in the storage pool that is created in the initial configuration belong to different controller enclosures, and disks in a smart disk enclosure do not belong to the member disks. If you want to add disks in a smart disk enclosure when expanding the capacity of a storage pool, comply with the following rules:

  Assume that X (a number) disks are configured for each controller enclosure as member disks in a storage pool, and Y disks (newly added disks) are configured for each controller enclosure. Capacity expansion can be performed when X and Y comply with either of the following conditions. Otherwise, capacity expansion will fail.

  – X + Y >= 25
  – Y ≥ X - [MIN (1, number of disks to which the hot spare policy corresponds)]

  Example 1: If the hot spare policy of a storage pool is set to low (1 disk) and the number of member disks configured for each controller enclosure in the storage pool is 23 before capacity expansion, the number of new disks configured for each controller enclosure is at least 2.

  Example 2: If the hot spare policy of a storage pool is set to low (1 disk) and the number of member disks configured for each controller enclosure in the storage pool is 8 before capacity expansion, the number of new disks configured for each controller enclosure is at least 7.

NOTICE

For a storage system with two or more controller enclosures, the disk enclosures that have been powered on and identified by a controller enclosure cannot be connected to any other controller enclosure of the same storage system after removal. Otherwise, the storage system cannot be powered on.

5.15.1.2 Using SmartKit to Expand the Capacity of a Performance Layer or Storage Pool

This section describes how to expand the capacity of a performance layer or storage pool using SmartKit.

Procedure

Step 1 Log in to SmartKit.

Step 2 Add the storage device of which capacity you want to expand to SmartKit.

1. In the main window of SmartKit, click the **Devices** tab and select **Add**.

   The dialog box for adding a storage device is displayed.

2. In **Basic Information**, select **Specify IP Address (add a device by the IP address)** and enter the management IP address of the storage device. Then click **Next**.
3. In the **Login Information** area, enter the user name and password of the storage system administrator and click **Finish**.

   NOTE

   - When a device is added for the first time or a device certificate is not trusted, a message is displayed indicating that the connection is not trusted.
   - When an SSH server is added for the first time or the fingerprint of an SSH server changes, a message is displayed asking whether you want to continue to register the SSH server.

Step 3 In the main window of SmartKit, choose **Home** > **Capacity Expansion** > **Expand Disk Domain/Storage Pool/Performance Layer**.

The **Expand Disk Domain/Storage Pool/Performance Layer** page is displayed.

Step 4 Select the storage device.

1. Click **Device Selection**.

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

2. In the **Select Devices** dialog box, select the storage device for which you want to expand capacity and specify the **Results Save Folder**. Then click **OK**.

Step 5 Evaluate the expansion solution.

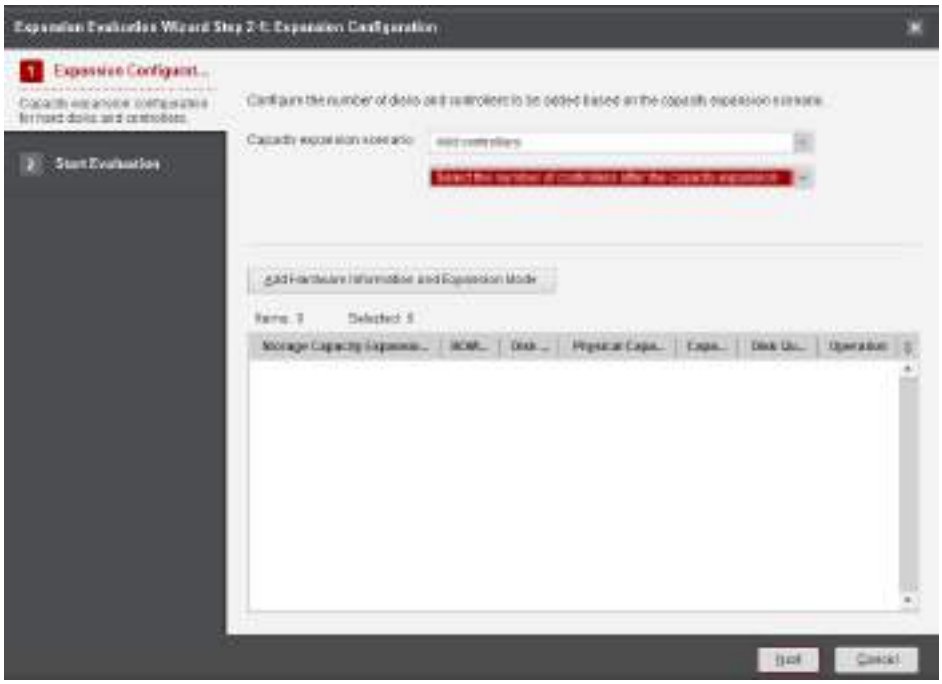
1. Click **Expansion Evaluation**.

   The **Expansion Configuration** page is displayed.

2. In **Capacity expansion scenario**, select **Expand disk domain/storage pool/performance layer**.
3. Click **Add Hardware Information and Expansion Mode**.

   NOTE

   You can add multiple configuration policies.



4. Specify the configuration parameters according to the capacity expansion plan. **Table 5-39** lists the parameters.

Table 5-39 Capacity evaluation parameters

Parameter	Description
Storage Capacity Expansion Mode	Method to add storage space. The value can be: – Create a storage pool: Use idle disks to create a new storage pool. – Expand storage pool (ID:*Y*) on CTE*X*: Add idle disks that belong to controller enclosure *X* to storage pool *Y* (*Y* indicates the ID of the storage pool).

Parameter	Description
BOM of Disk	BOM number of the new disk. **NOTE** – When you enter the BOM number, the tool displays the BOM number list of the disks. You can select the BOM number from the list or manually enter the complete BOM number. – If the entered BOM number is one in the list, the tool automatically fills in **Disk Type**, **Physical Capacity of a Single Disk**, and **Capacity Unit** based on the BOM number. – If the entered BOM number is not in the list, a dialog box is displayed. Confirm the entered BOM number and click **OK** to continue or click **Cancel** to enter the BOM number again. If the entered number is correct, click **OK** and manually enter **Disk Type**, **Physical Capacity of a Single Disk**, and **Capacity Unit**. – To add multiple disk types, click **Add Hardware Information and Expansion Mode** to add new configuration policies.
Disk Type	Type of the new disks. **NOTE** – Self-encrypting drives (SEDs) are supported.
Physical Capacity of a Single Disk	Capacity of the new disks.
Capacity Unit	Capacity unit of the new disks.
Disk Quantity	Number of new disks.
Operation	You can click **Delete** to delete the current configuration policy.

5. Click **Next**.

   The **Start Evaluation** page is displayed and the system starts to evaluate the expansion solution.

   NOTE

   – After completing the evaluation, click **Open the report** to go to the path for saving the evaluation report and obtain the report, that is, a **.zip** file named by the evaluation time.
   – You can also click **View the report** to open the report directly.

6. Click **Finish**.

NOTICE

Rectify the items (if any) that fail the evaluation according to the suggestions and evaluate the solution again. If the items fail the evaluation again, contact Huawei technical support. Otherwise, risks may arise during capacity expansion.

Step 6 Open the **Expand Storage Pool/Performance Layer Wizard**.

1. Click **Expansion**.

   The **Expansion** page is displayed.

2. Select **Expand Storage Pool/Performance Layer**.

   The **Expand Storage Pool/Performance Layer Wizard** is displayed.

Step 7 Follow the wizard to expand the capacity.

1. Confirm the precautions.

   Confirm the items and select **I have read the previous information and understood consequences of the operation**. Then click **Next**.

   The **Pre-expansion Check** dialog box is displayed.

2. The system automatically performs a pre-expansion check.

   If any check item fails, rectify the faults and perform the check again.

   After all check items are passed, click **Next**.

   The **Storage Pool/Performance Layer Expansion** dialog box is displayed.

3. The system automatically expands the capacity of the storage pool or performance layer. During the expansion, do not perform any operation on the storage system.

   NOTE

   - Determine whether to automatically allocate new capacity to associated storage pools based on the quota set before capacity expansion. If yes, click **OK**; if no, click **Cancel**.
   - The system expands the capacity according to the disk type and quantity specified during the expansion evaluation.
   - If the expansion fails, rectify the faults according to the suggestions provided by SmartKit and perform the expansion again.
   - If you want to modify the capacity quota of the performance layer, run the **change storage_pool general pool_id=? performance_layer_capacity=?** command to modify the value of the **performance_layer_capacity** field.

   After the expansion is complete, click **Next**.

   The **Completed** dialog box is displayed.

4. Click **Finish**.

Step 8 Inspect the storage device after expansion.

1. Click **Post-Expansion Inspection**.

   The inspection tool page is displayed.

2. Click **Select Check Items**.

   In the check item list, select the items you want to check.

3. Click **Next** to start the inspection.
   - **Open the result directory** is linked to the directory that stores the inspection report.
   - **View the report** is linked to the inspection results that are saved as **.html** files. These files are also compressed and stored in the result directory.
4. Click **Finish**.

   The inspection is complete.

----End

5.15.1.3 Using DeviceManager to Expand the Capacity of a Performance Layer or Storage Pool

This section describes how to expand the capacity of a performance layer or storage pool using DeviceManager.

5.15.1.3.1 Performing Pre-expansion Evaluation

Before expanding the capacity of a storage pool, use SmartKit to evaluate the expansion solution.

Procedure

Step 1 Log in to SmartKit.

Step 2 Add the storage device of which capacity you want to expand to SmartKit.

1. In the main window of SmartKit, click the **Devices** tab and select **Add**.

   The dialog box for adding a storage device is displayed.
2. In **Basic Information**, select **Specify IP Address (add a device by the IP address)** and enter the management IP address of the storage device. Then click **Next**.
3. In the **Login Information** area, enter the user name and password of the storage system administrator and click **Finish**.

NOTE

- When a device is added for the first time or a device certificate is not trusted, a message is displayed indicating that the connection is not trusted.
- When an SSH server is added for the first time or the fingerprint of an SSH server changes, a message is displayed asking whether you want to continue to register the SSH server.

Step 3 In the main window of SmartKit, choose **Home** > **Expansion** > **Expansion Evaluation**.

The **Expansion Evaluation** page is displayed.

Step 4 Select the storage device.

1. Click **Device Selection**.

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

2. Select the storage device and a path for saving task results. Click **OK**.

   NOTE

   After the expansion evaluation is complete, the storage system's configuration data is automatically backed up to the **\data\config** directory in the task result package. The data can be used to restore the storage system in the event of an expansion failure.

Step 5 Evaluate the expansion solution.

1. Click **Expansion Evaluation**.

   The **Expansion Configuration** page is displayed.

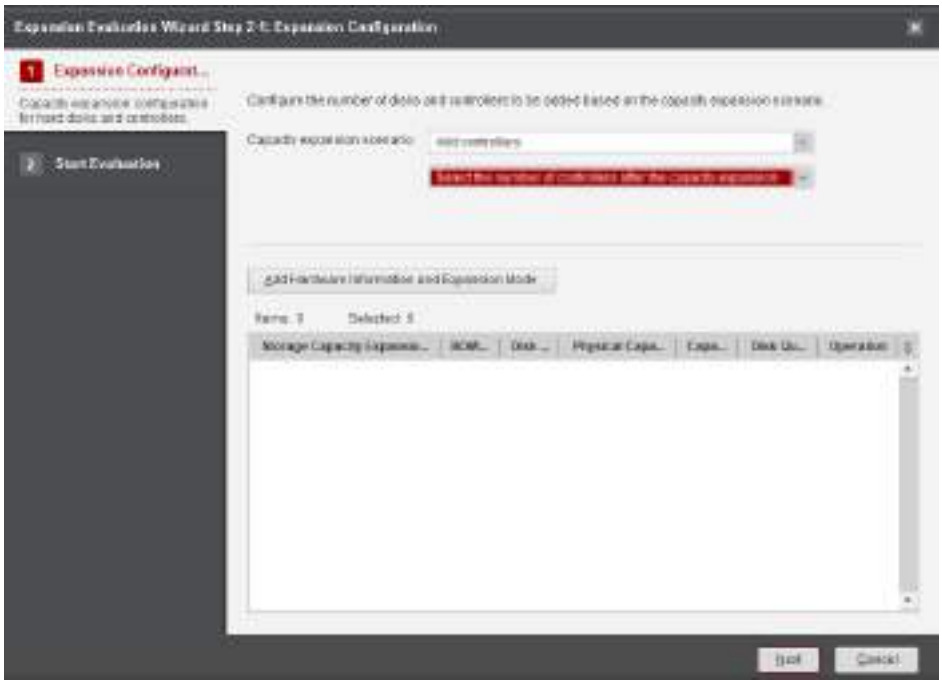
2. Select an expansion scenario.

   In **Capacity expansion scenario**, select **Expand storage pools**.

3. Click **Add Hardware Information and Expansion Mode**.

   NOTE

   You can add multiple configuration policies.



4. Specify the configuration parameters according to the capacity expansion plan. **Table 5-40** lists the parameters.

Table 5-40 Capacity evaluation parameters

Parameter	Description
Storage Capacity Expansion Mode	Method to add storage space. The value can be: – Create a storage pool: Use idle disks to create a new storage pool. – Expand storage pool (ID:*Y*) on CTE*X*: Add idle disks that belong to controller enclosure *X* to storage pool *Y* (*Y* indicates the ID of the storage pool). – Expand performance layer (ID:*Y*) on CTE*X*: Add idle disks that belong to controller enclosure *X* to performance layer *Y* (*Y* indicates the ID of the performance layer).
BOM of Disk	BOM number of the new disk. **NOTE** – When you enter the BOM number, the tool displays the BOM number list of the disks. You can select the BOM number from the list or manually enter the complete BOM number. – If the entered BOM number is one in the list, the tool automatically fills in **Disk Type**, **Physical Capacity of a Single Disk**, and **Capacity Unit** based on the BOM number. – If the entered BOM number is not in the list, a dialog box is displayed. Confirm the entered BOM number and click **OK** to continue or click **Cancel** to enter the BOM number again. If the entered number is correct, click **OK** and manually enter **Disk Type**, **Physical Capacity of a Single Disk**, and **Capacity Unit**. – To add multiple disk types, click **Add Hardware Information and Expansion Mode** to add new configuration policies.
Disk Type	Type of the new disks. **NOTE** – Self-encrypting drives (SEDs) are supported.
Physical Capacity of a Single Disk	Capacity of the new disks.
Capacity Unit	Capacity unit of the new disks.
Disk Quantity	Number of new disks.
Operation	You can click **Delete** to delete the current configuration policy.

5. Click **Next**.

   The **Start Evaluation** page is displayed and the system starts to evaluate the expansion solution.

NOTE

- After completing the evaluation, click **Open the report** to go to the path for saving the evaluation report and obtain the report, that is, a **.zip** file named by the evaluation time.
- You can also click **View the report** to open the report directly.

6. Click **Finish**.

NOTICE

Rectify the items (if any) that fail the evaluation according to the suggestions and evaluate the solution again. If the items fail the evaluation again, contact Huawei technical support. Otherwise, risks may arise during capacity expansion.

----End

5.15.1.3.2 Implementing Capacity Expansion for a Storage Pool

This section describes how to expand a storage pool to meet capacity requirements.

Prerequisites

The **Health Status** of the storage pool is **Normal**.

Procedure

Step 1 Choose **System** > **Storage Pools**.

Step 2 Click **More** on the right of the desired storage pool and choose **Expand**.

The **Expand Storage Pool** page is displayed on the right.

NOTE

Alternatively, click the name of the desired storage pool. In the upper right corner of the page that is displayed, select **Expand** from the **Operation** drop-down list.

Step 3 Expand the capacity layer and performance layer.

- Expanding the capacity layer

  Enter the number of disks in each controller enclosure to be added to the storage pool or click **Select** to manually select the disks.

NOTE

The entered number of disks is the total number of disks after capacity expansion.

- Expanding the performance layer

You are not allowed to manually select disks on DeviceManager. If free disks exist, the system adds all the free disks to the performance layer by default. If no free disk is available, capacity expansion is not performed for the performance layer.

NOTE

- You can click **View Selected Disks** to view the number of selected free disks.
- Select **Automatically allocate new capacity to associated storage pools based on the quota set before capacity expansion** if required.
- If you want to modify the capacity quota of the performance layer, run the **change storage_pool general pool_id=? performance_layer_capacity=?** command to modify the value of the **performance_layer_capacity** field.

Click **OK**.

Confirm your operation as prompted.

Step 4 Click **OK**.

Confirm your operation as prompted.

----End

5.15.1.3.3 Implementing Capacity Expansion for a Performance Layer

This section describes how to expand a performance layer to meet capacity requirements.

Procedure

Step 1 Choose **System** > **Storage Pools** > **Performance Layer**.

Step 2 Click **More** on the right of the desired performance layer and choose **Expand**.

The **Expansion** page is displayed.

NOTE

Alternatively, click the name of the desired performance layer. In the upper right corner of the page that is displayed, select **Expand** from the **Operation** drop-down list.

Step 3 Expand the performance layer.

You are not allowed to manually select disks on DeviceManager. The system adds all the free disks to the performance layer by default.

NOTE

- Select **Automatically allocate new capacity to associated storage pools based on the quota set before capacity expansion** if required.
- If you want to modify the capacity quota of the performance layer, run the **change storage_pool general pool_id=? performance_layer_capacity=?** command to modify the value of the **performance_layer_capacity** field.

Step 4 Click **OK**.

Confirm your operation as prompted.

----End

5.15.2 Expanding the Capacity of a LUN

When a service's storage space is insufficient, the storage space needs to be expanded in a timely manner. You can expand the capacity of LUNs to increase the service's storage space.

The following operations must be performed in sequence to expand the LUN capacity:

1. Expand the capacity of existing LUNs on the storage system. Huawei provides technical support for this operation.
2. Adjust the partition tables, volumes, clusters, databases, and applications on the host. The customer takes responsibility for this operation. The expansion operations on hosts in this document are for reference only.

WARNING

Expansion on a host involves non-Huawei software. Huawei does not have any information about such software and therefore cannot help the customer to assess potential risks. According to Huawei's project experience, it is risky to expand LUN capacity due to the complex operations. Instead, it is a good practice to expand capacity by adding LUNs.

Known potential risks in expanding the capacity of a LUN include but are not limited to:

- Expanding LUN capacity on a host (expanding the volume and file system capacity of the host) poses risks to service continuity and data integrity, and the risks exist for all storage vendors, not just for Huawei.
- Each operating system, file system, or volume management software has specific limits on LUN capacity. If the LUN capacity exceeds the limit after expansion, the LUN may fail to be identified by the host operating system or software. Moreover, the LUN cannot be downsized or restored after it is expanded. Consequently, the host may fail to access data, resulting in data loss.

NOTE

For details about the maximum LUN capacity supported by each operating system, see the official documents specific to your operating system.

- For partition tables, LUN capacity expansion may damage the partition tables or result in data loss.
- For the volume management software, LUN capacity expansion may cause the disk space to exceed the upper limit of the volume management software, resulting in an expansion failure.
- For databases, LUN capacity expansion may disorder metadata, leading to data inconsistency or loss.
- The impact of LUN capacity expansion cannot be determined when various applications are involved in complex scenarios.

5.15.2.1 Understanding the Expansion Process

Understanding the expansion procedure helps ensure a smooth expansion.

Figure 5-39 shows the process for expanding LUN capacity.

Figure 5-39 Expanding LUN capacity

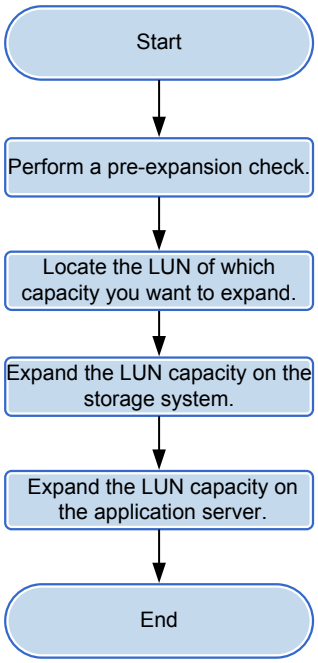


Table 5-41 describes each procedure in detail.

Table 5-41 Procedures for expanding LUN capacity

Procedure	Description
Perform a pre-expansion check.	Before expanding the LUN capacity, make sure that the storage system meets expansion requirements. Obtain and record necessary information including the IP address of the application server that uses the LUN, the WWN of the LUN, or the host LUN ID.
Locate the LUN of which capacity you want to expand.	Before expanding LUN capacity, confirm information about the LUN that carries service data to ensure a successful expansion.
Expand the LUN capacity on the storage system.	Expand the LUN capacity in online mode to the required capacity.
Expand the LUN capacity on the application server.	After completing the expansion, scan for disks on the application server to detect and use the expanded LUN.

5.15.2.2 Performing a Pre-Expansion Check

Storage space can be expanded in online mode. Before the expansion, check the storage system environment and service environment to ensure a smooth expansion.

Prerequisites

- You can log in to DeviceManager as the super administrator. Only a super administrator has the expansion permission.
- The storage system is running properly.
- You have obtained and recorded the WWN or IQN of the application server that uses the LUN and the WWN or ID of the LUN. The LUN has been mapped to the application server and the host configuration on the storage system is correct.

Procedure

Step 1 Log in to DeviceManager as the super administrator. Make sure that the storage environment meets the expansion requirement.

1. On the home page, check the device status and total capacity. Ensure that the storage system runs properly and has sufficient storage space.

   If the device status is **Fault**, contact Huawei technical support to locate and troubleshoot the fault. Start the expansion after the fault is rectified.

2. In the **Alarms** area, check current alarm information. Click **Show All**.

   The **Alarms and Events** page is displayed, listing all current alarms.

   If there are alarms related to the storage pool or LUN to be expanded, follow instructions in the **Suggestion** to handle the alarms. These alarms include **Storage Pool Is Degraded** and **LUN Is Faulty**.

Step 2 On DeviceManager, confirm and record the host corresponding to the application server, the LUN to be expanded, and the LUN's owning storage pool.

1. On the navigation bar of DeviceManager, choose **Services > Block Service > Host Groups > Hosts**.

   The **Hosts** page is displayed.

2. Based on the WWN or IQN of the application server you have recorded, find the host corresponding to the application server.
3. Select the host and check whether its status is normal.

   If any alarm is found, clear it according to the handling suggestion.

4. In the **Topology** area on the right of the page, click **Host LUN ID**, use the host LUN ID obtained from the server to determine the LUN to be expanded, and record the LUN name.
5. On the navigation bar, choose **Services > Block Service > LUN Groups > LUNs.**

   The **LUN** page is displayed.

6. Record the capacity and storage pool of the LUN to be expanded based on the LUN name.

----End

5.15.2.3 Locating the LUN of Which Capacity You Want to Expand

Before expanding LUN capacity, confirm information about the LUN that carries service data to ensure a successful expansion.

Prerequisites

- If a Fibre Channel network is used, the WWN of the Fibre Channel initiator has been obtained.
- If an iSCSI network is used, the IQN of the iSCSI initiator has been obtained.
- The UltraPath software has been installed on the host.

  NOTE

  This section uses UltraPath as an example. If you use third-party multipathing software, see the documents specific to your multipathing software.

Context

For an HP-UX operating system, run the **scsimgr -p get_attr all_lun -a device_file -a wwid** command to view the WWNs of disks on the host.

Procedure

Step 1 On the storage system, obtain the WWN of the LUN mapped to the host.

1. Log in to the CLI of the storage system as a super administrator.
2. Run the **show initiator initiator_type=? [wwn=? | iscsi_iqn_name=?]** command to query the host corresponding to the WWN or iSCSI IQN.

Parameter	Description	Value
initiator_type=*?*	Type of an initiator.	Possible values are: – **iSCSI**: iSCSI initiator. – **FC**: Fibre Channel initiator.
wwn=*?*	WWN of a Fibre Channel initiator. This parameter can be set only when **initiator_type=***?* is **FC**.	To obtain the value, run the **show initiator** command without parameters.
iscsi_iqn_name=*?*	IQN of an iSCSI initiator. This parameter can be set only when **initiator_type=***?* is **iSCSI**.	To obtain the value, run the **show initiator** command without parameters.

```
admin:/>show initiator initiator_type=FC wwn=21000024ff53b640

WWN              : 21000024ff53b640
Running Status   : Online
Free             : Yes
Alias            : suse2_01
Host ID          : 2
Multipath Type   : Default
```


Host ID is the ID of the host corresponding to the WWN.

3. Run the **show host lun host_id=***?* command to view all LUNs mapped to the host.

   host_id=*?* represents the ID of the host.

   ```
   admin:/>show host lun host_id=2

    LUN ID  LUN Name
    ------  ------------
    34      lun_0000
    35      lun_0001
    36      lun_0002
   ```

   LUN ID is the ID of each LUN mapped to the host from the storage system.

4. Run the **show lun general lun_id=***?* command to view the WWN of the LUN mapped to the host.

Step 2 On the host, view the WWN of the LUN.

1. Log in to the CLI of UltraPath on the host.
2. Run the **show vlun** command to query the WWNs of the disks on the host.

   NOTE

   For details about how to use the **show vlun** command, see the *UltraPath User Guide* specific to your operating system.

Step 3 Compare the WWNs obtained in step 1 and step 2. If they are the same, the LUN is the one to be expanded.

NOTE

For details about the preceding commands, see the *Command Reference* specific to your product model and version.

----End

5.15.2.4 Expanding the LUN Capacity on the Storage System

A user with the super administrator permission can use DeviceManager to expand LUN capacity and use the added storage space on the application server.

Prerequisites

- The storage system is working properly.
- You have determined the capacity you want to add to the LUN.
- A LUN on which SmartMigration is configured cannot be expanded.
- If third-party Veritas DMP is installed on your host and the capacity that is newly expanded for a LUN cannot be identified on the host, you are advised to expand capacity by adding LUNs.

Context

- For capacity expansion of HyperReplication LUNs, see "Expanding the Capacity of Remote Replication LUNs" in the *HyperReplication Feature Guide* specific to your product model and version.

- For capacity expansion of HyperMetro LUNs, see "Expanding the Capacity of HyperMetro LUNs" in the *HyperMetro Feature Guide* specific to your product model and version.
- For capacity expansion of 3DC LUNs, see "Expanding LUN Capacity for DR Star" in the *3DC Configuration* specific to your product model and version.

Procedure

Step 1 Log in to DeviceManager.

Step 2 On the navigation bar, choose **Services > Block Service > LUN Groups > LUNs**.

Step 3 Click **More** on the right of the LUN to be expanded and select **Expand** from the drop-down list.

The **Expand LUN** dialog box is displayed.

Step 4 Set **Added Capacity** to the amount of capacity that you want to add and select a unit.

Step 5 (Optional) Select or deselect **Only expand the local LUN**.

NOTE

- **Only expand the local LUN** are displayed only when the LUN belongs to a HyperMetro pair, remote replication pair, or DR Star trio.
- If you do not select **Only expand the local LUN**, the system will expand both the local and remote LUNs in the HyperMetro pair, remote replication pair, or DR Star trio. If you select **Only expand the local LUN**, the system will only expand the local LUN. In this case, manually expand the remote LUN to ensure the availability of HyperMetro, remote replication, or DR Star.
- Select **Only expand the local LUN** in the following scenarios:
  - The link to the remote device is disconnected.
  - The capacities of the local and remote LUNs are different.
  - The local device is a remote device in HyperMetro or asynchronous remote replication in a DR Star trio.
  - The remote LUN is in another protection relationship.

Step 6 Click **OK**.

Step 7 Verify and use the added capacity.

1. Click the LUN whose capacity has been expanded and view its current **Capacity**.

   If the **Capacity** value is the same as the actual capacity (the original capacity plus the added capacity), the capacity expansion is successful. Otherwise, rectify the fault based on the alarm information.
2. After the capacity expansion is successful, log in to the application server as the system administrator and scan for disks again. After the scanning is successful, the newly added storage capacity is available to the application server.

----End

5.15.2.5 Expanding the LUN Capacity on the Application Server

You can configure the application server so that it can identify and use the expanded storage space after the capacity on a LUN is expanded.

5.15.2.5.1 Expanding the LUN Capacity on a Windows Application Server

After expanding LUN capacity on the storage system, configure the corresponding application server to identify and use the expanded storage space. This section uses an application server running Windows Server 2008 as an example. For application servers running other versions of Windows operating systems, adjust the operations based on actual conditions.

Prerequisites

LUN capacity has been expanded on the storage system.

Context

In this example, the LUN is mapped as disk 3 on the application server. Its drive letter is **G:** and its capacity is expanded from 25 GB to 50 GB.

Procedure

Step 1 Log in to the Windows application server as an administrator.

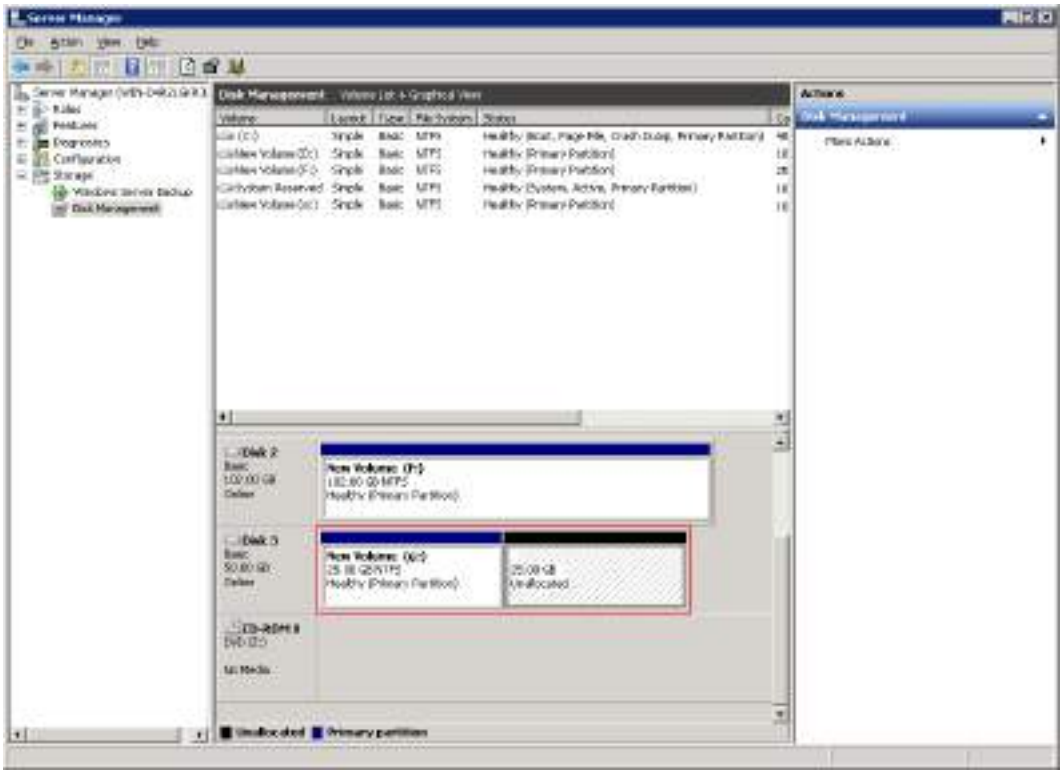
Step 2 On the desktop, click **Start** and choose **Administrative Tools** > **Server Manager**.

The **Server Manager** dialog box is displayed.

Step 3 In the navigation tree of the **Server Manager** dialog box, right-click **Disk Management** and choose **Rescan Disks** from the shortcut menu.

Figure 5-40 shows the scanning result. The unallocated space is displayed on the right side of disk G.

Figure 5-40 Disk scanning result



Step 4 Right-click disk G and choose **Extend Volume...** from the shortcut menu.

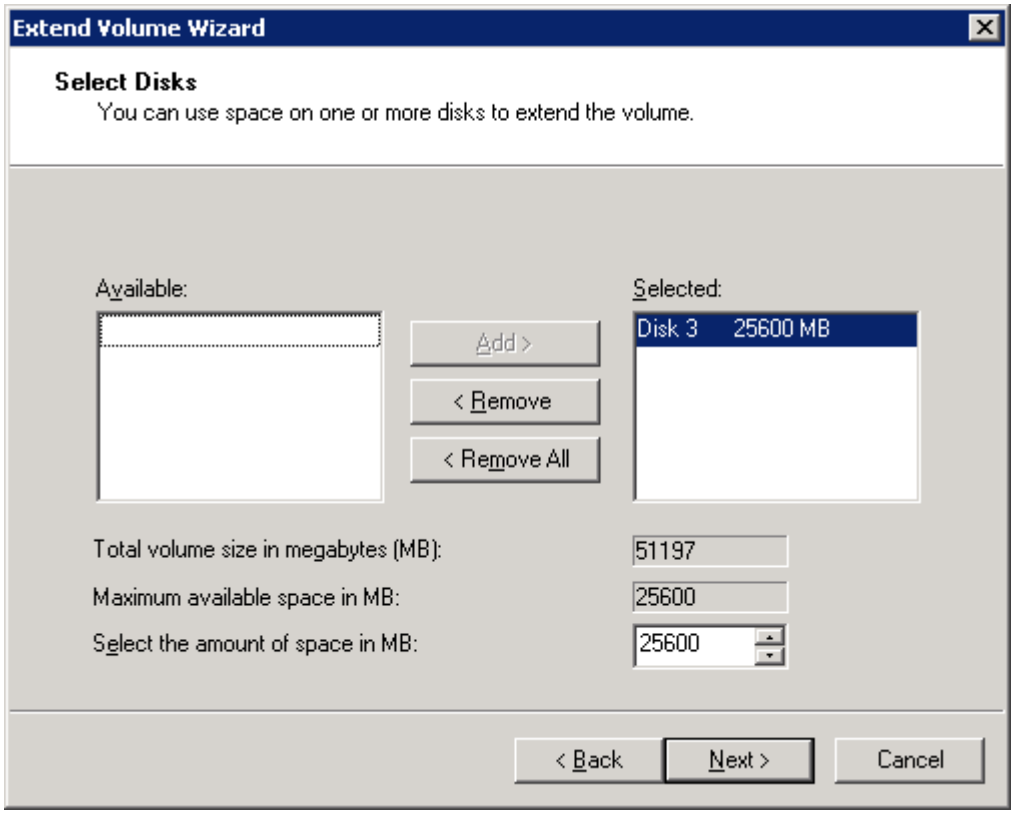
The **Extend Volume Wizard** dialog box is displayed, as shown in **Figure 5-41**.

Figure 5-41 Extend Volume Wizard

Step 5 Click **Next**.

The **Select Disks** page is displayed, as shown in **Figure 5-42**.

Figure 5-42 Select Disks



NOTE

- Disk 3 is the expanded LUN mapped to the application server.
- You can specify the required space in **Select the amount of space in MB**. The default value is the maximum available space.

Step 6 Click **Next**.

Step 7 Click **Finish**.

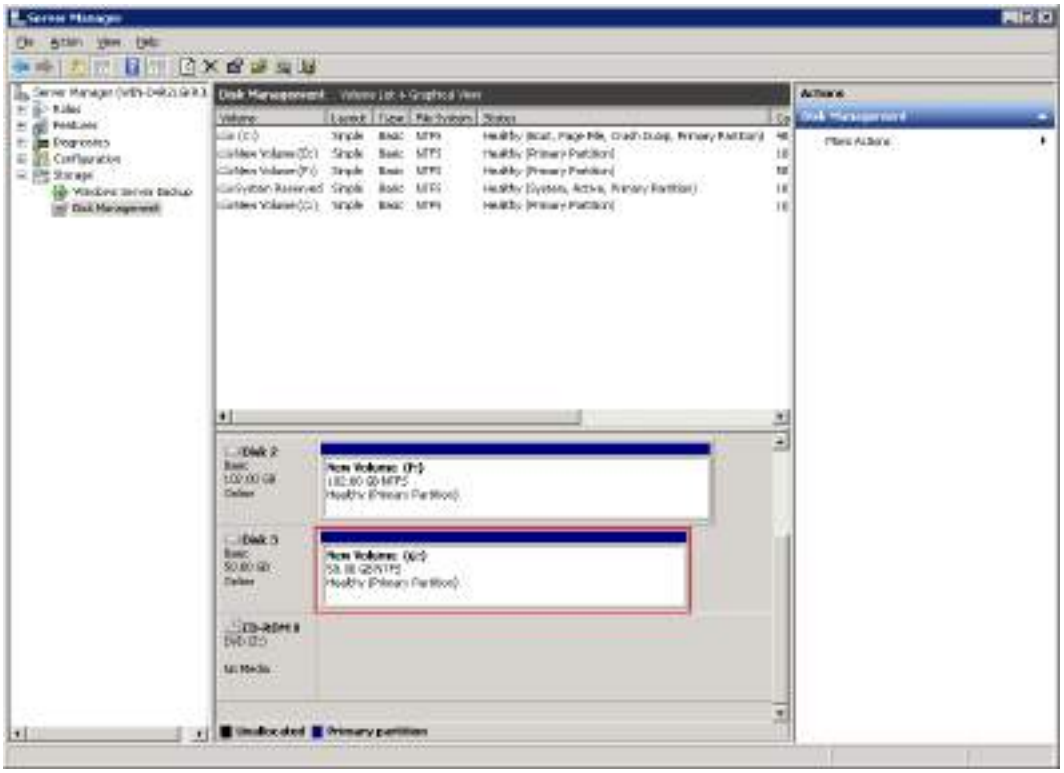
The **Server Manager** dialog box is displayed. Capacity expansion on the application server is complete.

----End

Result

In the **Server Manager** dialog box, check the capacity of disk G after expansion, as shown in **Figure 5-43**.

Figure 5-43 Operation result



5.15.2.5.2 Expanding the LUN Capacity on a SUSE Application Server

After expanding LUN capacity on the storage system, configure the corresponding application server to identify and use the expanded storage space. This section uses an application server running SUSE 11.0 as an example. For application servers running other versions of SUSE operating systems, adjust the operations based on actual conditions.

Prerequisites

LUN capacity has been expanded on the storage system.

Context

In this example, the LUN capacity is expanded from 25 GB to 50 GB. The drive letter of the mapped disk on the application server is **sdf**.

Procedure

Step 1 Scan for disks on the SUSE application server.

1. Scan for disks.
   - If UltraPath is installed, run the **hot_add** command.
   - If UltraPath is not installed, perform the following operations:
     i. Run the **lsscsi** command to obtain the ID of the host that uses the LUN. The following is an example.


```
SUSE:~ # lsscsi  [5:0:0:0]    disk    HUAWEI XXXX          2101  /dev/sdf
```

In the preceding command output, **5** in **[5:0:0:0]** indicates the host ID, **XXXX** indicates a specific product model or brand.

ii. Run the **echo '- - -' > /sys/class/scsi_host/host*N*/scan** command, where *N* indicates the host ID obtained in the preceding step.

After the scanning is complete, the disk capacity remains 25 GB.

2. Run the **echo 1 > /sys/block/sdf/device/rescan** command to rescan for disks.

After the scanning is complete, the disk capacity becomes 50 GB.

NOTE

sdf is the drive letter of the disk mapped from the LUN to the application server. The actual drive letter may be different.

Step 2 Run the **fdisk -l** command to query information about all disks on the application server.

```
SUSE:~ # fdisk -l
Disk /dev/sdb: 598.0 GB, 597998698496 bytes
255 heads, 63 sectors/track, 72702 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Disk identifier: 0xc433d0ae

 Device Boot      Start         End      Blocks Id  System
/dev/sdb1 *           1           9       72275+  83  Linux
/dev/sdb2            10         271     2104514+  83  Linux
/dev/sdb3           272       72703 581806279 83  Linux
/dev/sdb4             1           1           0+  ee  GPT

Partition table entries are not in disk order

Disk /dev/sdf: 53.7 GB, 53687091200 bytes
64 heads, 32 sectors/track, 51200 cylinders
Units = cylinders of 2048 * 512 = 1048576 bytes
Disk identifier: 0x00000000

Disk /dev/sdf doesn't contain a valid partition table
```

Step 3 Run the **resize2fs /dev/sdf** command to add the new storage space to the file system of the LUN.

- If the following command output is displayed, the file system is successfully expanded.

  ```
  SUSE:~ # resize2fs /dev/sdf
  resize2fs 1.41.9 (22-Aug-2009)
  Resizing the filesystem on /dev/sdf to 13107200 (4k) blocks.
  The filesystem on /dev/sdf is now 13107200 blocks long.
  ```

- If the following information is displayed, run the **e2fsck -f /dev/sdf** command and then the **resize2fs /dev/sdf** command.

  ```
  SUSE:~ # resize2fs /dev/sdf
  resize2fs 1.41.9 (22-Aug-2009)
  Please run 'e2fsck -f /dev/sdf' first.
  ```

----End

5.15.2.5.3 Expanding the LUN Capacity Using LVM on a SUSE Application Server

After expanding LUN capacity on the storage system, configure the corresponding application server to identify and use the expanded storage space. This section uses SUSE 11.0 as an example to describe how to non-disruptively expand the storage space on an application server using logical volume manager (LVM). For

application servers running other versions of SUSE operating systems, adjust the operations based on actual conditions.

Prerequisites

- LUN capacity has been expanded on the storage system.
- A physical volume to be expanded has been determined.

Context

In this example, **sdb5** is a physical volume under the drive letter of the disk mapped from the LUN to the application server. The capacity of **sdb5** is expanded from 104 MB to 120 MB.

Procedure

Step 1 On the application server, check the block device ID of the LUN in the operating system.

1. Run the **hot_add** command to scan for disks.
2. Run the **show vlun** command to query the LUN WWN.

```
UltraPath CLI #0 >show vlun
-------------------------------------------------------------------------------------------------------------------------------
-------------
 Vlun ID      Disk          Name                  Lun WWN              Status Capacity Ctrl(Own/Work)
Array Name  Dev Lun ID
    0         sda       WMQ_LUN_TEST_002  60022a11000beb2a0421c1cc000002d0  Normal
3.00GB               Array8.1       --
    1         sdb       WMQ_LUN_TEST_003  60022a11000beb2a0421c2a2000002d1  Normal
3.00GB               Array8.1       --
    2         sdc       WMQ_LUN_TEST_004  60022a11000beb2a0421c365000002d2  Normal
3.00GB               Array8.1       --
    3         sdd       WMQ_LUN_TEST_005  60022a11000beb2a0421c4bd000002d3  Normal
3.00GB               Array8.1       --
-------------------------------------------------------------------------------------------------------------------------------
-------------
```

The value of **Lun WWN** is the WWN of the LUN and **Disk** is the drive letter of the disk mapped from the LUN to the application server.

Step 2 Run the **echo 1 > /sys/block/sdb5/device/rescan** command to rescan for disks.

NOTE

sdb5 is a physical volume under the drive letter of the disk mapped from the LUN to the application server. Change it to the actual physical volume in your operation.

Step 3 Run the **pvresize /dev/sdb5** command to expand the physical volume.

Step 4 Run the **lvextend -L +16M /dev/testvg/testlv** command to expand the logical volume.

```
lvextend  -L +16M /dev/testvg/testlv
  Extending logical volume testlv to 120.00 MB
  Logical volume testlv successfully resized
```

In the command, **testlv** is the logical volume to be expanded.

Step 5 Run the **resize2fs /dev/testvg/testlv** command to expand the file system.

```
resize2fs /dev/testvg/testlv
  resize2fs 1.41.9 (22-Aug-2009)
```



```
Resizing the filesystem on /dev/testvg/testlv to 122800 (1k) blocks.
The filesystem on /dev/testvg/testlv is now 122800 blocks long.
```

----End

5.15.2.5.4 Expanding the LUN Capacity on a Red Hat Application Server

After expanding LUN capacity on the storage system, configure the corresponding application server to identify and use the expanded storage space. This section uses an application server running Red Hat 6.4 as an example. For application servers running other versions of Red Hat operating systems, adjust the operations based on actual conditions.

Prerequisites

LUN capacity has been expanded on the storage system.

Context

In this example, the LUN capacity is expanded from 25 GB to 50 GB. The drive letter of the mapped disk on the application server is **sdh**.

Procedure

Step 1 Scan for disks on the Red Hat application server.

1. Scan for disks.
   - If UltraPath is installed, run the **hot_add** command.
   - If UltraPath is not installed, perform the following operations:
     i. Run the **lsscsi** command to obtain the ID of the host that uses the LUN. The following is an example.
     ```
     [root@localhost ~]# lsscsi  [5:0:0:0]    disk    HUAWEI XXXX          2101  /dev/sdh
     ```
     In the preceding command output, **5** in **[5:0:0:0]** indicates the host ID, **XXXX** indicates a specific product model or brand.
     ii. Run the **echo '- - -' > /sys/class/scsi_host/host***N***/scan** command, where *N* indicates the host ID obtained in the preceding step.
     After the scanning is complete, the disk capacity remains 25 GB.
2. Run the **echo 1 > /sys/block/sdh/device/rescan** command to rescan for disks.

   NOTE

   sdh is the drive letter of the disk mapped from the LUN to the application server. The actual drive letter may be different.
3. If you use DM-multipath, run the **multipathd resize map** *mpathX* command to update *mpathX* capacity.
   After the scanning is complete, the disk capacity becomes 50 GB.

Step 2 Run the **fdisk -l** command to query information about all disks on the application server.

```
[root@localhost ~]# fdisk -l

Disk /dev/sdb: 16.1 GB, 16106127360 bytes
64 heads, 32 sectors/track, 15360 cylinders
Units = cylinders of 2048 * 512 = 1048576 bytes
```



```
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000


Disk /dev/sde: 107.4 GB, 107374182400 bytes
255 heads, 63 sectors/track, 13054 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000


Disk /dev/sdh: 53.7 GB, 53687091200 bytes
64 heads, 32 sectors/track, 51200 cylinders
Units = cylinders of 2048 * 512 = 1048576 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000
```

Step 3 Run the **resize2fs /dev/sdh** command to add the new storage space to the file system of the LUN.

NOTE

For Red Hat 6.X and 7.X, if an EXT4 file system is created, the following error may be reported:

```
resize2fs: Permission denied to resize filesystem
```

Unmount the device and run **e2fsck**.

```
umount /fs1
e2fsck -y /dev/sdh
```

```
[root@localhost ~]# resize2fs /dev/sdh
resize2fs 1.41.12 (17-May-2010)
Filesystem at /dev/sdh is mounted on /fs1; on-line resizing required
old desc_blocks = 2, new_desc_blocks = 4
Performing an on-line resize of /dev/sdh to 13107200 (4k) blocks.
The filesystem on /dev/sdh is now 13107200 blocks long.
```

----End

5.15.2.5.5 Expanding the LUN Capacity on a Solaris Application Server

After expanding LUN capacity on the storage system, configure the corresponding application server to identify and use the expanded storage space. This section uses an application server running Solaris 10 as an example. For application servers running other versions of Solaris operating systems, adjust the operations based on actual conditions.

Prerequisites

- LUN capacity has been expanded on the storage system.
- Services on the LUN to be expanded have been stopped.

Context

This section uses the default disk-based UNIX File System (UFS) on a Solaris application server as an example to describe how to expand a LUN and its file system on a raw disk. The LUN will be expanded from 50 GB to 60 GB.

Procedure

Step 1 Run the **cfgadm -al** command to scan for the LUNs mapped to the application server.

```
root@solaris:~# cfgadm -al
Ap_Id                          Type         Receptacle Occupant     Condition
c2                            scsi-sas     connected    configured unknown
c2::dsk/c2t6d0                CD-ROM       connected    configured unknown
c4                            scsi-sas     connected    configured unknown
c4::w5000cca0258a82e5,0       disk-path    connected    configured unknown
c5                            scsi-sas     connected    unconfigured unknown
c6                            scsi-sas     connected    configured unknown
c6::w5000cca02570b521,0       disk-path    connected    configured unknown
c7                            scsi-sas     connected    unconfigured unknown
c10                           fc-private   connected    configured unknown
c10::20080022a10bc14f         disk         connected    configured unknown
c11                           fc           connected    unconfigured unknown
usb0/1                        unknown      empty        unconfigured ok
usb0/2                        unknown      empty        unconfigured ok
usb0/3                        unknown      empty        unconfigured ok
usb1/1                        unknown      empty        unconfigured ok
usb1/2                        unknown      empty        unconfigured ok
usb2/1                        unknown      empty        unconfigured ok
usb2/2                        usb-hub      connected    configured ok
usb2/2.1                      unknown      empty        unconfigured ok
usb2/2.2                      unknown      empty        unconfigured ok
usb2/2.3                      usb-hub      connected    configured ok
usb2/2.3.1                    unknown      empty        unconfigured ok
usb2/2.3.2                    usb-storage  connected    configured ok
usb2/2.3.3                    usb-communi  connected    configured ok
usb2/2.4                      usb-device   connected    configured ok
usb2/3                        unknown      empty        unconfigured ok
usb2/4                        usb-hub      connected    configured ok
usb2/4.1                      unknown      empty        unconfigured ok
usb2/4.2                      unknown      empty        unconfigured ok
usb2/4.3                      unknown      empty        unconfigured ok
usb2/4.4                      unknown      empty        unconfigured ok
usb2/5                        unknown      empty        unconfigured ok
```

Step 2 Run the **umount /mnt/** command to unmount the disks corresponding to the LUN that you want to expand on the application server.

In the command, **/mnt/** indicates the mount directory of the disks corresponding to the LUN.

NOTE

If disks of the LUN that you want to expand are not mounted, skip this operation.

Step 3 Run the **format** command to query the information about all disks detected by the application server.

```
root@solaris:~# format
Searching for disks...done

AVAILABLE DISK SELECTIONS:
       0. c0t5000CCA0258A82E4d0 <SUN300G cyl 46873 alt 2 hd 20 sec 625>  solaris
          /scsi_vhci/disk@g5000cca0258a82e4
          /dev/chassis//SYS/HDD0/disk
       1. c0t5000CCA02570B520d0 <SUN300G cyl 46873 alt 2 hd 20 sec 625>  solaris
          /scsi_vhci/disk@g5000cca02570b520
          /dev/chassis//SYS/HDD4/disk
       2. c10t5d0 <drive type unknown>
          /pci@400/pci@2/pci@0/pci@a/SUNW,qlc@0/fp@0,0/ssd@w20080022a10bc14f,0
       3. c10t5d1 <HUAWEI-XXXXXX-2201 cyl 6398 alt 2 hd 64 sec 256>
          /pci@400/pci@2/pci@0/pci@a/SUNW,qlc@0/fp@0,0/ssd@w20080022a10bc14f,1
Specify disk (enter its number):
```


In the preceding command output, **c10t5d1** indicates the drive letter mapped by the LUN to the application server.

Step 4 Enter **3** after **Specify disk (enter its number)**, which is the ID of **c10t5d1**.

```
Specify disk (enter its number): 3
selecting c10t5d1
[disk formatted]
Note: detected additional allowable expansion storage space that can be
added to current SMI label's computed capacity.
Select <partition> <expand> to adjust the label capacity.

FORMAT MENU:
        disk       - select a disk
        type       - select (define) a disk type
        partition  - select (define) a partition table
        current    - describe the current disk
        format     - format and analyze the disk
        repair     - repair a defective sector
        label      - write label to the disk
        analyze    - surface analysis
        defect     - defect list management
        backup     - search for backup labels
        verify     - read and display labels
      save       - save new disk/partition definitions
        inquiry    - show disk ID
        volname    - set 8-character volume name
        !<cmd>     - execute <cmd>, then return
        quit
format>
```

Step 5 Run the **type** command to view the disk type.

```
format> type

AVAILABLE DRIVE TYPES:
        0. Auto configure
        1. Quantum ProDrive 80S
        2. Quantum ProDrive 105S
        3. CDC Wren IV 94171-344
        4. SUN0104
        5. SUN0207
        6. SUN0327
        7. SUN0340
        8. SUN0424
        9. SUN0535
        10. SUN0669
        11. SUN1.0G
        12. SUN1.05
        13. SUN1.3G
        14. SUN2.1G
        15. SUN2.9G
        16. Zip 100
        17. Zip 250
        18. Peerless 10GB
        19. SUN300G
        20. HUAWEI-XXXXXX-2201
        21. other
Specify disk type (enter its number)[20]:
```

Step 6 After **Specify disk type (enter its number)[20]:**, enter **0** to automatically update disks, re-define the disk type, and refresh the disk capacity.

```
Specify disk type (enter its number)[20]: 0
c10t5d1: configured with capacity of 59.98GB
<HUAWEI-XXXXXX-2201 cyl 7678 alt 2 hd 64 sec 256>
selecting c10t5d1
[disk formatted]
```

After the operations are complete, the disk capacity becomes 60 GB.

Step 7 Run the **partition** command and then run the **print** command to view disk partitions.

```
format> partition

PARTITION MENU:
        0      - change `0' partition
        1      - change `1' partition
        2      - change `2' partition
        3      - change `3' partition
        4      - change `4' partition
        5      - change `5' partition
        6      - change `6' partition
        7      - change `7' partition
        select - select a predefined table
        modify - modify a predefined partition table
        name - name the current table
        print  - display the current table
        label  - write partition map and label to the disk
        !<cmd> - execute <cmd>, then return
        quit
partition> print
Current partition table (default):
Total disk cylinders available: 7678 + 2 (reserved cylinders)

Part      Tag    Flag     Cylinders        Size            Blocks
  0       root    wm       0 - 15      128.00MB    (16/0/0)      262144
  1       swap    wu      16 - 31      128.00MB    (16/0/0)      262144
  2     backup    wu       0 - 7677       59.98GB    (7678/0/0) 125796352
  3 unassigned    wm       0              0         (0/0/0)           0
  4 unassigned    wm       0              0         (0/0/0)           0
  5 unassigned    wm       0              0         (0/0/0)           0
  6        usr    wm      32 - 7677       59.73GB    (7646/0/0) 125272064
  7 unassigned    wm       0              0         (0/0/0)           0
```

NOTE

Generally, if **Part** of a partition is numbered **2**, the partition indicates the entire disk that mapped to the application server.

Step 8 Run **l** and enter **y** to label the LUN that has been expanded.

```
partition> l
Ready to label disk, continue? y
```

Step 9 Run the **mount /dev/dsk/c10t5d1s6 /mnt/** command to mount the disk.

Step 10 Run the **growfs -M /mnt /dev/rdsk/c10t5d1s6** command to expand the file system of the LUN.

```
root@solaris:~# growfs -M /mnt /dev/rdsk/c10t5d1s6
/dev/rdsk/c10t5d1s6:    125272064 sectors in 20390 cylinders of 48 tracks, 128 sectors
        61168.0MB in 1275 cyl groups (16 c/g, 48.00MB/g, 5824 i/g)
super-block backups (for fsck -F ufs -o b=#) at:
 32, 98464, 196896, 295328, 393760, 492192, 590624, 689056, 787488, 885920,
Initializing cylinder groups:
.....................
super-block backups for last 10 cylinder groups at:
 124360864, 124459296, 124557728, 124656160, 124754592, 124853024, 124951456,
 125049888, 125148320, 125246752
```

Step 11 Run the **df -k** command to view the file system capacity.

```
root@solaris:~# df -k
Filesystem            1024-blocks        Used Available Capacity  Mounted on
rpool/ROOT/solaris     103219200     2269688  79378520     3%    /
/devices                       0           0         0     0%    /devices
/dev                           0           0         0     0%    /dev
ctfs                           0           0         0     0%    /system/contract
proc                           0           0         0     0%    /proc
mnttab                         0           0         0     0%    /etc/mnttab
```



```
swap                    30640088        2272    30637816     1%    /system/volatile
objfs                         0           0           0     0%    /system/object
sharefs                       0           0           0     0%    /etc/dfs/sharetab
fd                            0           0           0     0%    /dev/fd
rpool/ROOT/solaris/var
                         103219200      200868    79378520     1%    /var
swap                    30637816           0    30637816     0%    /tmp
rpool/VARSHARE          103219200          48    79378520     1%    /var/share
rpool/export            103219200          32    79378520     1%    /export
rpool/export/home       103219200          31    79378520     1%    /export/home
rpool                   103219200          73    79378520     1%    /rpool
/dev/dsk/c2t6d0s2          694700      694700           0 100%    /media/Oracle_Solaris-11_1-Text-SPARC
/dev/dsk/c10t5d1s6        61687396       61185    61120192     1%    /mnt
```

----End

5.15.2.5.6 Expanding the LUN Capacity on an AIX Application Server

After expanding LUN capacity on the storage system, configure the corresponding application server to identify and use the expanded storage space. This section uses an application server running AIX 6.1 as an example. For application servers running other versions of AIX operating systems, adjust the operations based on actual conditions.

Prerequisites

- LUN capacity has been expanded on the storage system.
- Services on the LUN to be expanded have been stopped.

Context

In the following example, the LUN to be expanded is LUN005 and its capacity is 25 GB. The capacity of the file system created on the LUN is 24 GB. The LUN and file system will be expanded to 50 GB and 48 GB respectively. The volume group name and logical volume name of the LUN to be expanded are **vg1** and **lv1** respectively. The mount directory of the file system that uses the LUN is **/mnt/lv1**.

Procedure

Step 1 Scan for disks on the AIX application server.

NOTICE

- If the LUN that you want to expand has been mapped to the application server and has mapping relationship with the application server during the expansion process, run **rmdev -dl diskName** to delete disk information before performing the following operations. In the command, **diskName** indicates the disk corresponding to the LUN before expansion.
- If the mapping between the LUN and application server is canceled before expansion and rebuilt after expansion, directly perform the following operations.

Run the **cfgmgr -v** command to scan for the LUN.

After the LUN is scanned, AIX automatically identifies the LUN that is mapped to the application server as a drive letter in hdisk format.

Step 2 Run the **lsdev -Cc disk** command to view the information about the disks that have been detected.

```
# lsdev -Cc disk
hdisk0  Available 01-08-00 SAS Disk Drive
hdisk1  Available 01-08-00 SAS Disk Drive
hdisk2  Available 04-00-02 MPIO Other FC SCSI Disk Drive
hdisk3  Available 04-00-02 MPIO Other FC SCSI Disk Drive
hdisk4  Available 03-01-02 Other FC SCSI Disk Drive
hdisk5  Available 04-01-02 HUAWEI XXXX FC Disk Drive
```

In the command output, **XXXX** indicates a specific product model or brand.

Step 3 Run the **upadm show lun** command to check the drive letter of the LUN that you want to expand.

```
# upadm show lun
Vendor of /dev/hdisk0 is not HUAWEI, XXXX, XXXX or XXXX
Vendor of /dev/hdisk1 is not HUAWEI, XXXX, XXXX or XXXX
Vendor of /dev/hdisk2 is not HUAWEI, XXXX, XXXX or XXXX
Vendor of /dev/hdisk3 is not HUAWEI, XXXX, XXXX or XXXX
-------------------------------------------------------------------------------------------
Device Name: Lun Name: Vendor ID:  Type:    Serial Number:  Device WWN:
-------------------------------------------------------------------------------------------
/dev/hdisk5 LUN005       HUAWEI     XXXX 1T50214955      60022a1100098e6703da136f0000000a
```

If there are multiple disks, the command output lists the drive letter of each disk. At the bottom of the command output, the drive letter of the newly created LUN is displayed. In this example, the LUN name is LUN005 and its drive letter is **hdisk5**. In the command output, **XXXX** indicates a specific product model or brand.

Step 4 Run the **umount /mnt/lv1** command to unmount the file system.

In the command, **/mnt/lv1** indicates the mount directory of the file system.

Step 5 Run the **varyoffvg vg1** command to deactivate volume group **vg1**.

In the command, **vg1** indicates the name of the volume group corresponding to the LUN that you want to expand.

Step 6 Run the **bootinfo -s hdiskX** command to check the LUN capacity after expansion. In the command, **X** indicates the number of the drive letter. In this example, **X** is **5**.

```
# bootinfo -s hdisk5
51200
```

In the preceding command output, the unit is MB, and the capacity is 51,200 MB (50 GB), which is the same as the expansion result displayed on the storage system.

Step 7 Run the **varyonvg vg1** command to activate volume group **vg1**.

Step 8 Refresh the capacity of the volume group corresponding to the LUN.

1. Run the **chvg -g vg1** command to refresh the volume group.

   ```
   # chvg -g vg1
   0516-1164 chvg: Volume group vg1 changed.  With given characteristics vg1
         can include up to 64 physical volumes with 2032 physical partitions each.
   ```

2. Run the **lsvg vg1** command and check the volume group parameters.

   ```
   # lsvg vg1
   VOLUME GROUP:       vg1                  VG IDENTIFIER:  00f6e07400004c00000000011660e3d1
   VG STATE:           active               PP SIZE:        32 megabyte(s)
   VG PERMISSION:      read/write           TOTAL PPs:      1599 (51168 megabytes)
   MAX LVs:            512                  FREE PPs:       62 (1984 megabytes)
   ```



```
LVs:            2          USED PPs:      1537 (49184 megabytes)
OPEN LVs:       0          QUORUM:        2 (Enabled)
TOTAL PVs:      1          VG DESCRIPTORS: 2
STALE PVs:      0          STALE PPs:     0
ACTIVE PVs:     1          AUTO ON:       yes
MAX PPs per VG: 130048
MAX PPs per PV: 2032       MAX PVs:       64
LTG size (Dynamic): 256 kilobyte(s)  AUTO SYNC:  no
HOT SPARE:      no         BB POLICY:     relocatable
```

In the command output, pay attention to the **PP SIZE** parameter, which is relevant to the logical volume size when you create or modify a logical volume. In this example, the value of **PP SIZE** is 32 MB.

Step 9 Modify the capacity of the logical volume to meet the needs of the file system.

1. Run the **lslv lv1** command and check the logical volume parameters.

```
# lslv lv1
LOGICAL VOLUME:     lv1                    VOLUME GROUP: vg1
LV IDENTIFIER:      00f6e07400004c00000000011660e3d1.1 PERMISSION:     read/write
VG STATE:           active/complete        LV STATE:       closed/syncd
TYPE:               jfs2                   WRITE VERIFY: off
MAX LPs:            768                    PP SIZE:        32 megabyte(s)
COPIES:             1                      SCHED POLICY: parallel
LPs:                768                    PPs:            768
STALE PPs:          0                      BB POLICY:      relocatable
INTER-POLICY:       minimum                RELOCATABLE:    yes
INTRA-POLICY:       middle                 UPPER BOUND:    128
MOUNT POINT:        /mnt/lv1               LABEL:          /mnt/lv1
MIRROR WRITE CONSISTENCY: on/ACTIVE
EACH LP COPY ON A SEPARATE PV ?: yes
Serialize IO ?:     NO
```

In the command output, **lv1** indicates the name of a logical volume in the volume group. Pay attention to the **MAX LPs**, **LPs**, and **PP SIZE** parameters in the command output, which indicate the maximum number of logical partitions, number of logical partitions, and size of the physical partition, respectively. The value of **MAX LPs** multiplied by **PP SIZE** is the size of the logical volume, and the value of **LPs** multiplied by **PP SIZE** is the capacity of the logical volume's file system. In this example, the values of **MAX LPs** and **LPs** are both 768, and the value of **PP SIZE** is 32 MB. Therefore, the capacities of the logical volume and the file system are both 24,576 MB (24 GB).

2. Run the **smit lv** command.

```
# smit lv
                          Logical Volumes

Move cursor to desired item and press Enter.

  List All Logical Volumes by Volume Group
  Add a Logical Volume
  Set Characteristic of a Logical Volume
  Show Characteristics of a Logical Volume
  Remove a Logical Volume
  Copy a Logical Volume


F1=Help           F2=Refresh        F3=Cancel         Esc+8=Image
Esc+9=Shell       Esc+0=Exit        Enter=Do
```

3. In the command output, select **Set Characteristic of a Logical Volume** and press **Enter**.

```
                  Set Characteristic of a Logical Volume

Move cursor to desired item and press Enter.

  Change a Logical Volume
  Rename a Logical Volume
```



```
Increase the Size of a Logical Volume
Add a Copy to a Logical Volume
Remove a Copy from a Logical Volume
```

4. In the command output, select **Change a Logical Volume** and press **Enter**.

```
                    Change a Logical Volume

Type or select a value for the entry field.
Press Enter AFTER making all desired changes.

                                        [Entry Fields]
* LOGICAL VOLUME name                      []                +
```

5. Press **Esc+4** to go to the logical volume name list. Select the logical volume you want to modify and press **Enter**.

```
                    Change a Logical Volume

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                        [Entry Fields]
* Logical volume NAME                      lv1
  Logical volume TYPE                     [jfs2]              +
  POSITION on physical volume               middle            +
  RANGE of physical volumes                 minimum           +
  MAXIMUM NUMBER of PHYSICAL VOLUMES      [128]               #
    to use for allocation
  Allocate each logical partition copy      yes               +
    on a SEPARATE physical volume?
  RELOCATE the logical volume during        yes               +
    reorganization?
  Logical volume LABEL                    [/mnt/lv1]
  MAXIMUM NUMBER of LOGICAL PARTITIONS    [1536]              #
  SCHEDULING POLICY for writing/reading     parallel          +
    logical partition copies
  PERMISSIONS                             read/write          +
  Enable BAD BLOCK relocation?              yes               +
  Enable WRITE VERIFY?                      no                +
  Mirror Write Consistency?                 active            +
  Serialize IO?                           no                  +
  Mirror Pool for First Copy                                  +
  Mirror Pool for Second Copy                                 +
  Mirror Pool for Third Copy                                  +
```

6. In the command output, select the **MAXIMUM NUMBER of LOGICAL PARTITIONS** parameter (that is, the **MAX LPs** parameter) and enter the maximum number of logical partitions for the logical volume.

   Because a file system is created on a logical volume, you must expand the capacity of the logical volume before the file system can be expanded. The capacity of the logical volume must not be smaller than that of the file system. Otherwise, the file system will fail to be expanded. In this example, the capacity of the file system will be expanded to 48 GB. First, you must adjust the maximum number of logical partitions to ensure that the capacity of the logical volume is greater than or equal to 48 GB (49,152 MB). To achieve this, the maximum number of logical partitions must not be smaller than 1536 (49,152 MB/32 MB).

7. After modifying the parameter, press **Enter**.

```
                    COMMAND STATUS

Command: OK            stdout: no            stderr: no

Before command completion, additional instructions may appear below.
```

8. Press **Esc+0** to exit the logical volume configuration interface.

Step 10 Expand the file system on the **lv1** logical volume.

1. Run the **chfs -a size=***48G* **/mnt/lv1** command to expand the file system.
   ```
   # chfs -a size=48G /mnt/lv1
   Filesystem size changed to 100663296
   ```
   As shown in the command output, the capacity of the file system has been expanded to 48 GB.
2. Run the **mount /mnt/lv1** command to mount the file system again.

----End

5.15.2.5.7 Expanding the LUN Capacity on an HP-UX Application Server

After expanding LUN capacity on the storage system, configure the corresponding application server to identify and use the expanded storage space. This section uses an application server running HP-UX 11i v3 as an example. For application servers running other versions of HP-UX operating systems, adjust the operations based on actual conditions.

Prerequisites

- LUN capacity has been expanded on the storage system.
- Services on the LUN to be expanded have been stopped.

Context

In this example, the LUN capacity is expanded from 25 GB to 50 GB and the mount directory for the LUN is **/test/**.

Procedure

Step 1 Scan for LUNs on the HP-UX application server.

1. Run the **ioscan** command to scan for hardware.
2. Run the **ioscan -funNC disk** command to query information about detected LUNs.

```
bash-3.2# ioscan -funNC disk
Class     I  H/W Path  Driver S/W State H/W Type     Description
==========================================================================
disk      2  64000/0xfa00/0x0 esdisk    CLAIMED      DEVICE       HP       DG146ABAB4
                    /dev/disk/disk2      /dev/disk/disk2_p1 /dev/rdisk/disk2     /dev/rdisk/disk2_p1
disk      3  64000/0xfa00/0x1 esdisk CLAIMED      DEVICE       HP       DG146ABAB4
                    /dev/disk/disk3      /dev/disk/disk3_p1 /dev/disk/disk3_p2 /dev/disk/disk3_p3 /dev/rdisk/
disk3     /dev/rdisk/disk3_p1  /dev/rdisk/disk3_p2  /dev/rdisk/disk3_p3
disk      5  64000/0xfa00/0x2 esdisk CLAIMED      DEVICE       TEAC     DV-28E-V
                    /dev/disk/disk5 /dev/rdisk/disk5
disk    399  64000/0xfa00/0x90  esdisk CLAIMED      DEVICE       HUAWEI XXXXXX
                    /dev/disk/disk399 /dev/rdisk/disk399
```

In this example, **/dev/disk/disk399** indicates the device file of the LUN mapped to the application server.

NOTE

If the operating system is HP-UX 11i v2 or HP-UX 11i v1, run the **ioscan -funC disk** command to query LUNs detected by the application server.

Step 2 Run the **umount /test/** command to unmount the file system of the LUN.

In the command, **/test/** indicates the mount directory of the file system.

Step 3 Run the **extendfs -F vxfs /dev/disk/disk399** command to expand the file system of the LUN.

In the command, **vxfs** indicates the file system type.

Step 4 Run the **mount /dev/disk/disk399 /test/** command to mount the file system of the LUN.

Step 5 Run the **bdf** command to check the file system capacity after expansion.

```
bash-3.2# bdf
Filesystem          kbytes    used avail %used Mounted on
/dev/vg00/lvol3    1048576  920416  127376 88% /
/dev/vg00/lvol1    1835008  368824 1454800 20% /stand
/dev/vg00/lvol8    8912896 2309816 6552824 26% /var
/dev/vg00/lvol7    6553600 3012368 3513640 46% /usr
/dev/vg00/lvol4     524288 23504  497008     5% /tmp
/dev/vg00/lvol6    7864320 4358216 3479048 56% /opt
/dev/vg00/lvol5     131072 64088 66464 49% /home
/dev/disk/disk399 52428800 79504 49077472     0% /test
```

The preceding command output shows that the capacity of the file system becomes 50 GB.

----End

5.15.2.5.8 Expanding the LUN Capacity on a VMware ESX Application Server

After expanding LUN capacity on the storage system, configure the corresponding application server to identify and use the expanded storage space. This section uses an application server running VMware ESXi 6.5.0 as an example. For application servers running other versions of VMware ESX operating systems, adjust the operations based on actual conditions.

Prerequisites

LUN capacity has been expanded on the storage system.

Context

In this example, the LUN capacity is expanded from 25 GB to 50 GB. The ID of the LUN to be expanded is **3**.

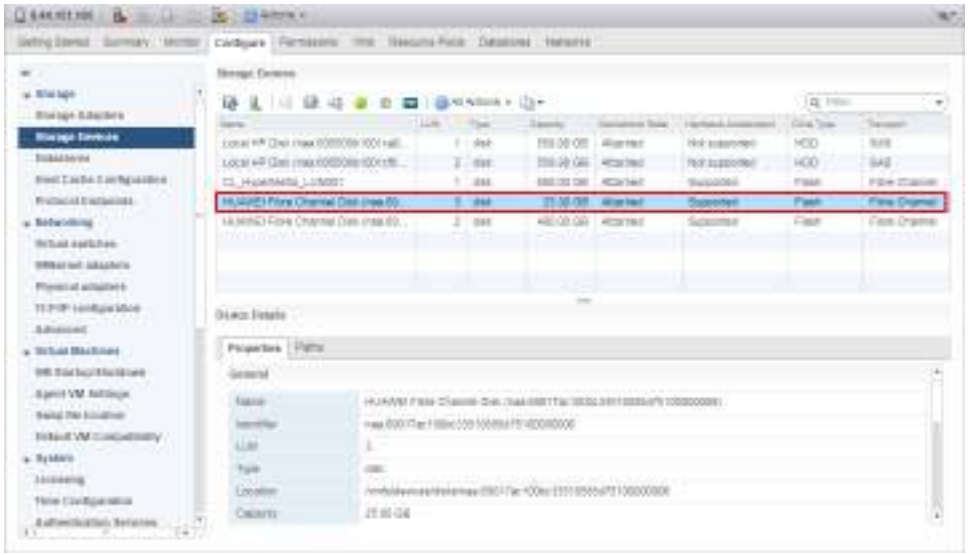
Procedure

Step 1 In vSphere Client, click the **Configure** tab.

Step 2 In the navigation tree on the left, choose **Storage** > **Storage Devices**.

Step 3 On the **Storage Devices** page, view the device mapped from the LUN to be expanded on the application server, as shown in **Figure 5-44**.

Figure 5-44 Device mapped from the LUN to be expanded on the application server



Step 4 On the **Devices** page, choose **All Actions** > **Rescan Storage**.

The **Rescan Storage** dialog box is displayed, as shown in **Figure 5-45**.

Figure 5-45 Rescan Storage dialog box

Step 5 Click **OK**.

It takes 2 to 4 minutes to scan for new storage devices and VMFS volumes. You can check the task status in the **Recent Tasks** area at the lower part of the main window.

- If the task status is **In Progress** as shown in **Figure 5-46**, the scanning is ongoing.

Figure 5-46 Scanning ongoing

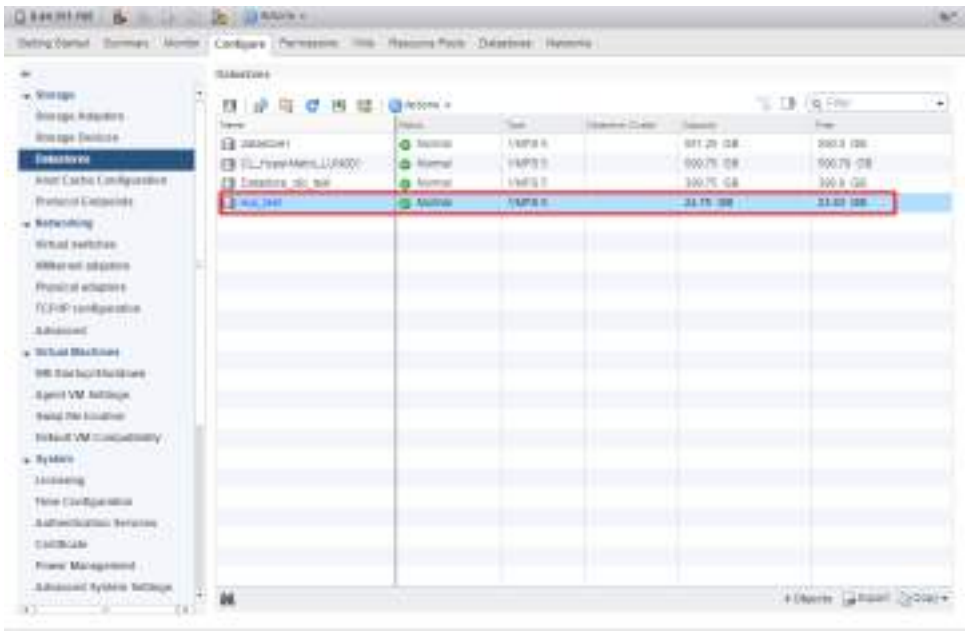
- If the task status is **Completed** as shown in **Figure 5-47**, the scanning is completed.

Figure 5-47 Scanning completed

Step 6 Click **Datastores**.

On the **Datastores** page, view the datastore mapped from the LUN to be expanded on the application server, as shown in **Figure 5-48**.

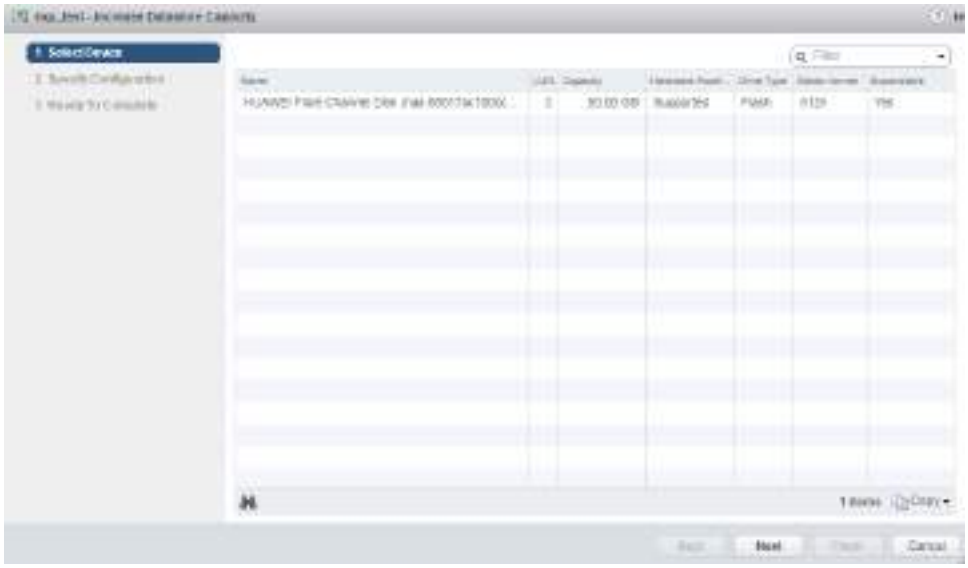
Figure 5-48 Datastore mapped from the LUN to be expanded on the application server



Step 7 Right-click the datastore corresponding to the LUN to be expanded, and choose **Increase Datastore Capacity** from the shortcut menu.

The **Increase Datastore Capacity** dialog box is displayed, as shown in **Figure 5-49**.

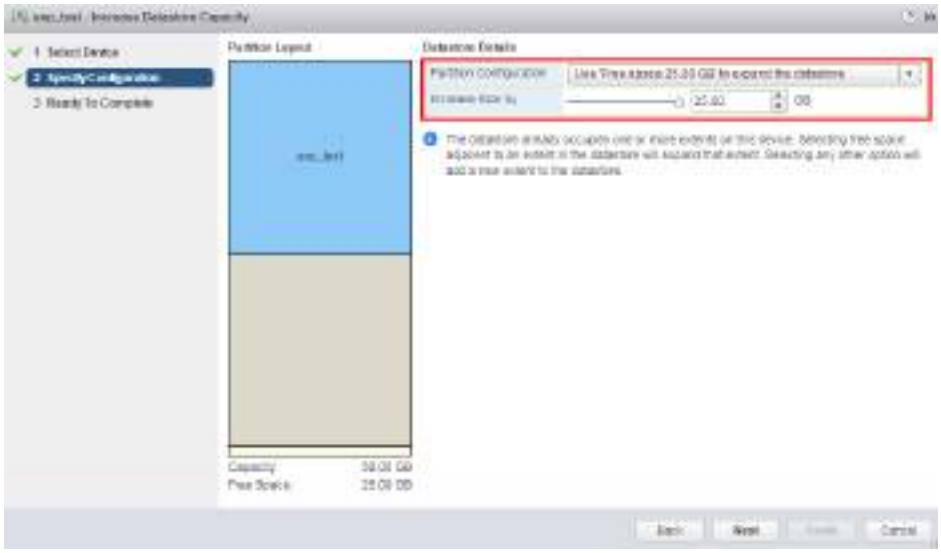
Figure 5-49 Increase Datastore Capacity dialog box



Step 8 Select the datastore corresponding to the LUN to be expanded and click **Next**.

Step 9 Set **Partition Configuration** and **Increase Size by**. The maximum storage space is recommended, as shown in **Figure 5-50**. Click **Next**.

Figure 5-50 Setting the datastore size



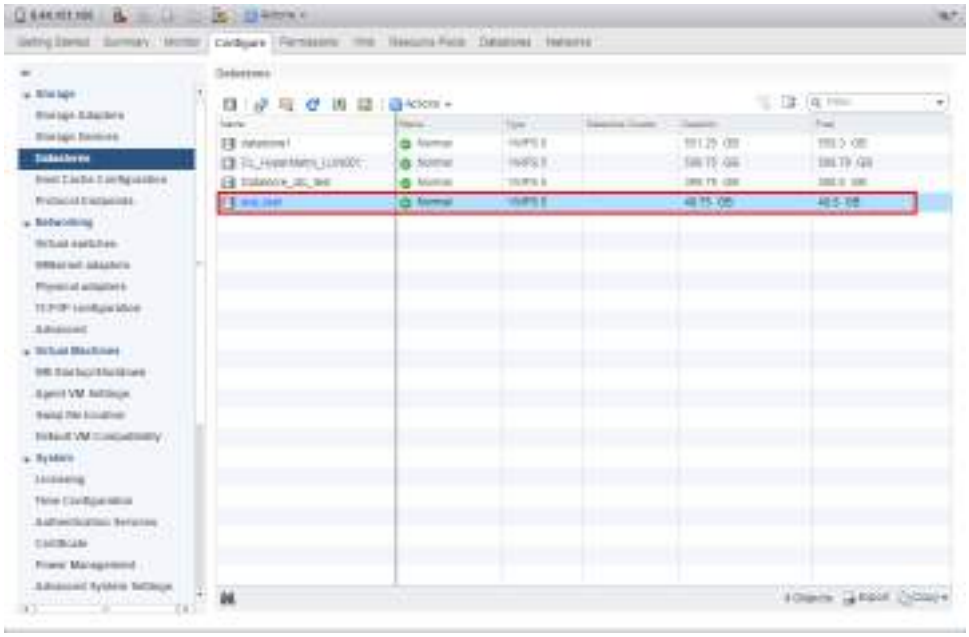
Step 10 Click **Finish**.

----End

Result

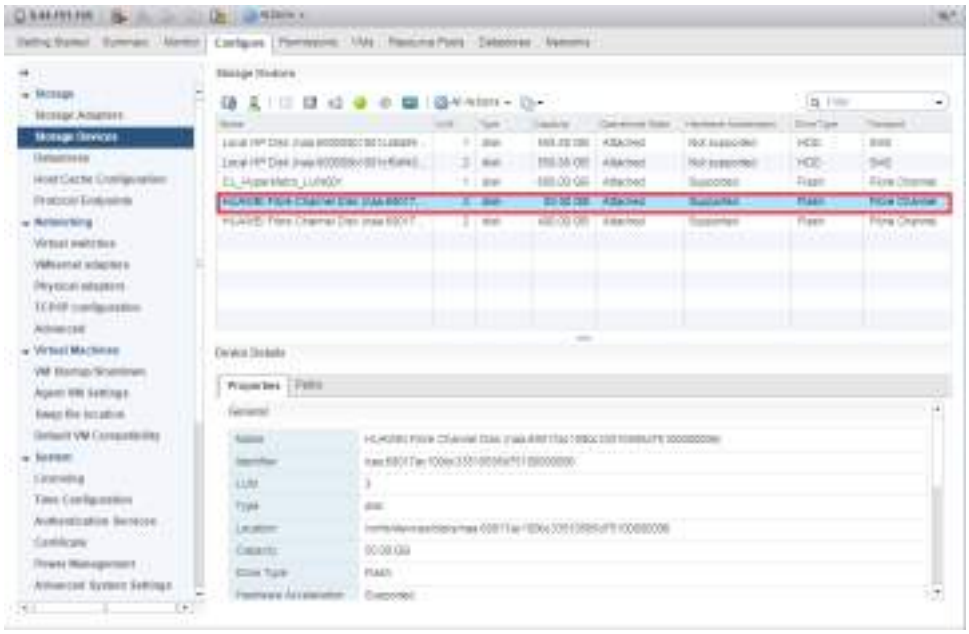
- On the **Datastores** page, view the expanded datastore, as shown in **Figure 5-51**.

Figure 5-51 Datastore mapped from the expanded LUN on the application server



- On the **Storage Devices** page, view the expanded device, as shown in **Figure 5-52**.

Figure 5-52 Device mapped from the expanded LUN on the application server



5.15.2.5.9 Expanding the LUN Capacity on a Hyper-V Application Server

After expanding LUN capacity on the storage system, configure the corresponding application server to identify and use the expanded storage space. This section uses a Windows Server 2016 Hyper-V cluster as an example. For Hyper-V clusters of other versions, adjust the operations based on actual conditions.

Prerequisites

LUN capacity has been expanded on the storage system.

Context

In this example, the Hyper-V cluster consists of two application servers: WIN2016_HOST1 and WIN2016_HOST2. The LUN to be expanded is mapped to disk 6 and disk 7 respectively on the two application servers. The LUN capacity is expanded from 25 GB to 58 GB.

Procedure

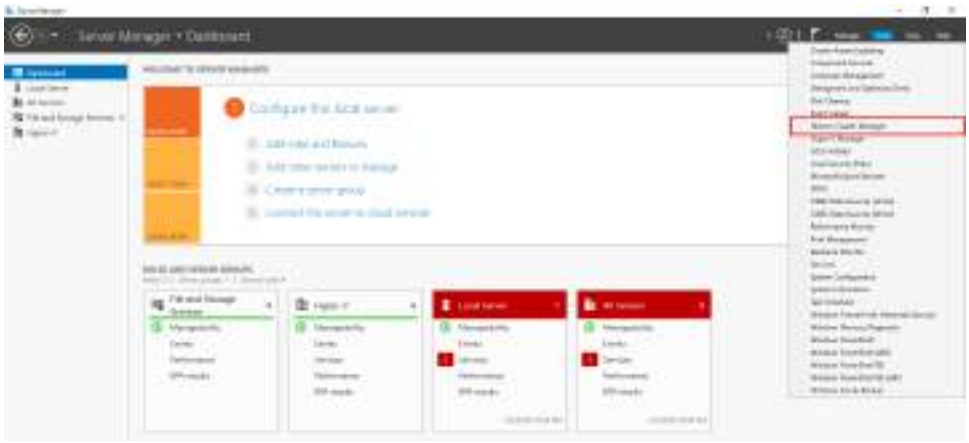
Step 1 Query the **Owner Node** of the shared volume of the cluster to be expanded.

1. Log in to either of the Windows application servers in the Hyper-V cluster as an administrator.
2. On the Windows desktop, click **Start** and choose **Server Manager**.

   The **Server Manager** dialog box is displayed.
3. Choose **Tools** > **Failover Cluster Manager**.

   The **Failover Cluster Manager** dialog box is displayed.

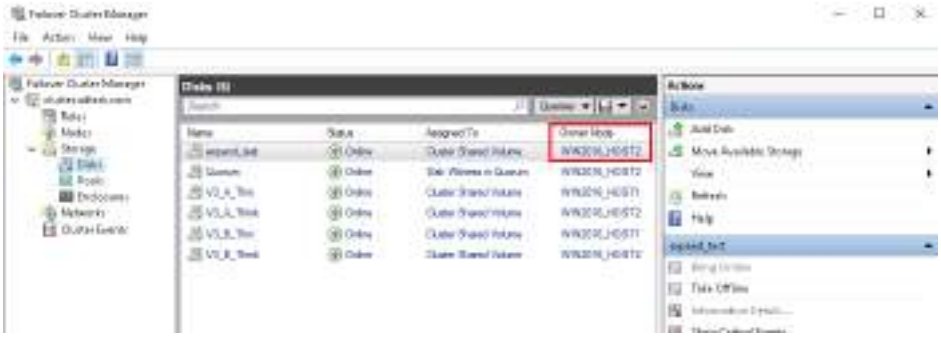
   Figure 5-53 Failover Cluster Manager

4. In the navigation tree on the left, choose **Storage** > **Disks** under the Hyper-V cluster to be expanded. In the **Disks** area, view the **Owner Node** of the shared volume of the cluster.

   In this example, the **Owner Node** of the shared volume of the cluster is WIN2016_HOST2.

Figure 5-54 Viewing the Owner Node of the shared volume

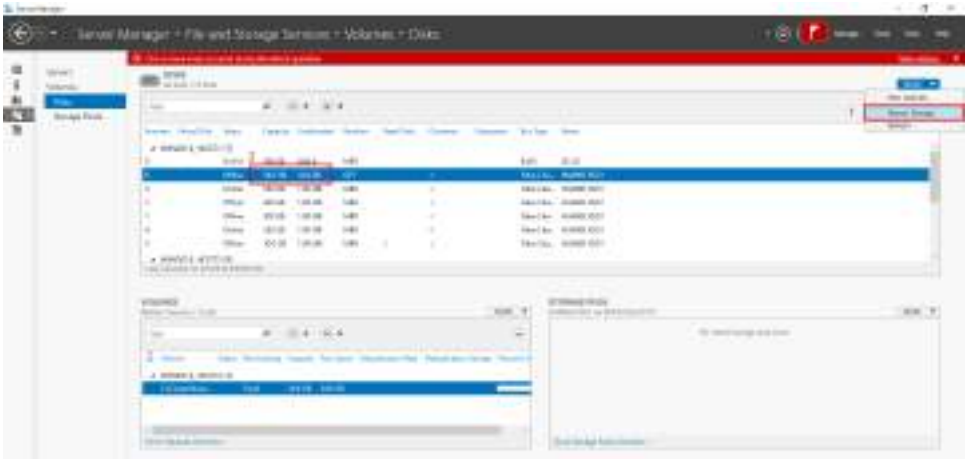


Step 2 Perform volume capacity expansion on the **Owner Node** of the shared volume of the cluster to be expanded. The following procedure takes the WIN2016_HOST2 application server as an example.

1. Log in to the WIN2016_HOST2 application server as an administrator.
2. Go to the **Server Manager** page. Choose **File and Storage Services** > **Volumes** > **Disks**.
3. Click **TASKS** > **Rescan Storage** to scan for disks on all application servers in the cluster.

   After the scanning is complete, check the capacity of the partitions to be expanded in the **DISKS** area. In this example, the total capacity of the partitions to be expanded is 58 GB, among which 33 GB is the unallocated capacity.

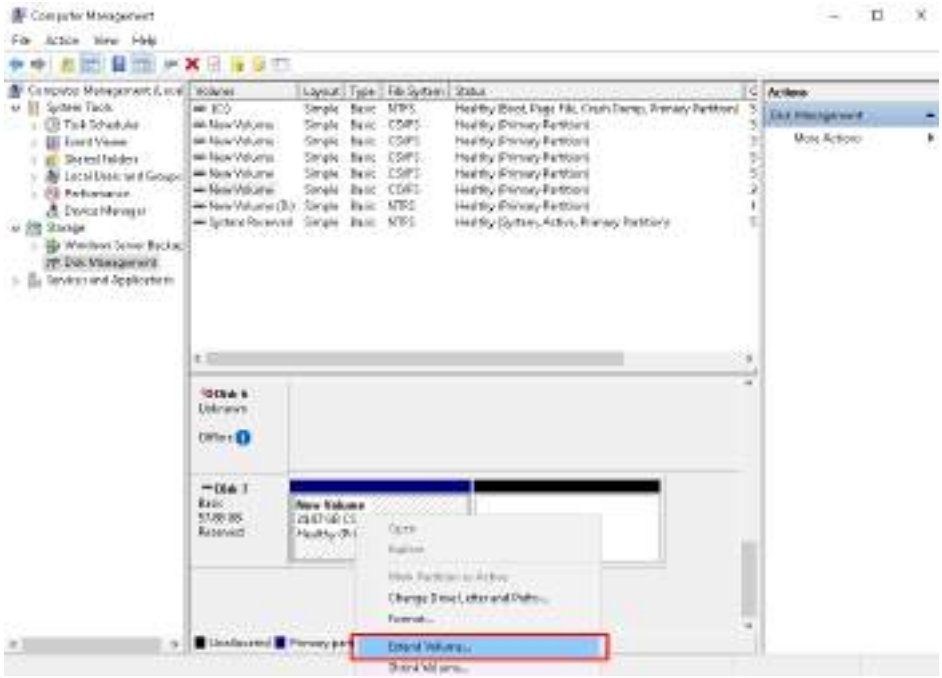
Figure 5-55 Scanning for disks



4. On the **Server Manager** page, choose **Tools** > **Computer Management**.

   The **Computer Management** dialog box is displayed.
5. Choose **Storage** > **Disk Management** in the navigation tree.

Figure 5-56 Disk management

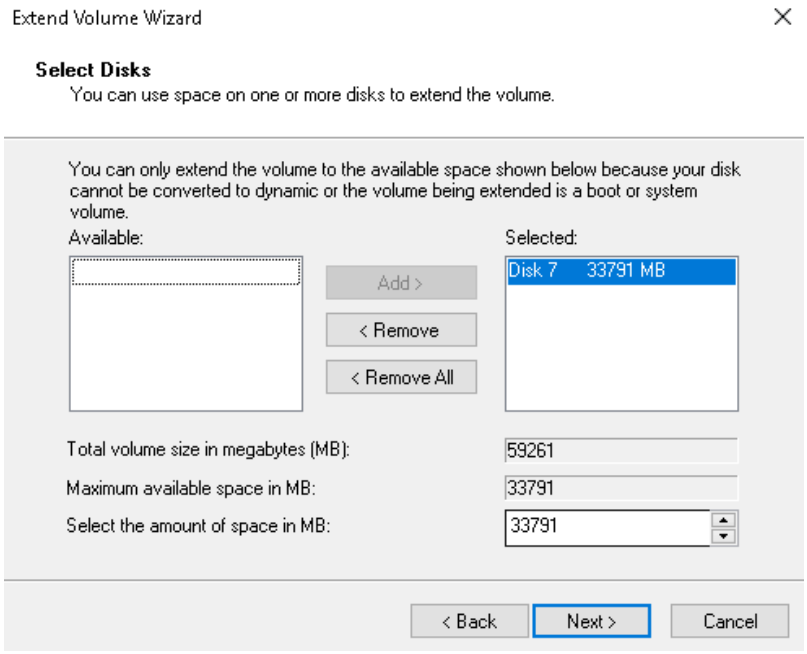


6. Right-click **Disk 7** and choose **Extend Volume...** from the shortcut menu.
   The **Extend Volume Wizard** dialog box is displayed.

Figure 5-57 Extend Volume Wizard

7. Click **Next**.
   The **Select Disks** page is displayed.

Figure 5-58 Select Disks



NOTE

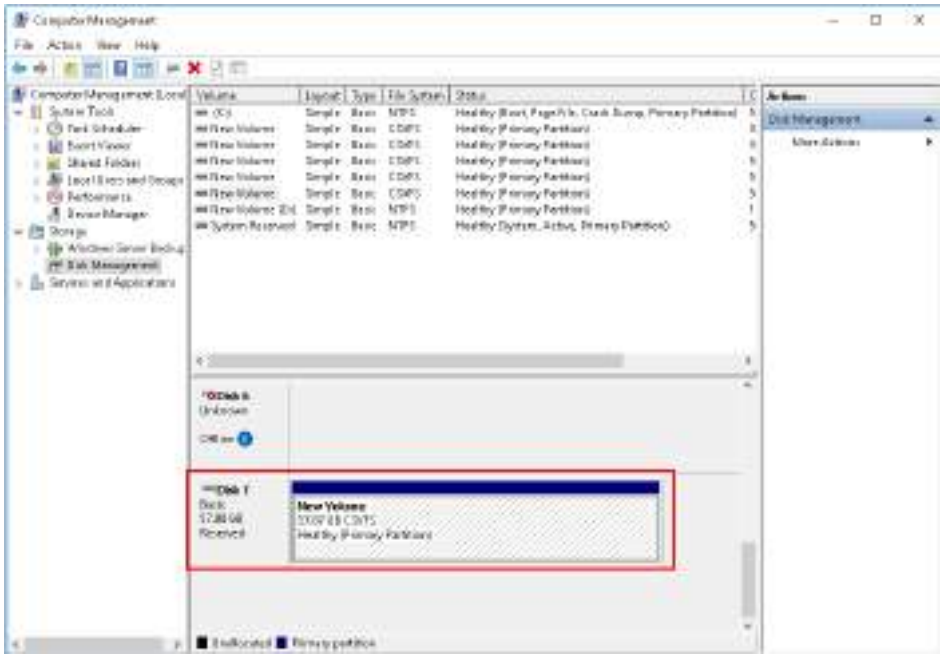
- Disk 7 is the disk mapped from the LUN to be expanded on the application server.
- You can specify the required space in **Select the amount of space in MB**. The default value is the maximum available space.

8. Click **Next**.
9. Click **Finish**. Partition expansion on the application server is complete.

NOTE

To expand the capacity of the shared volume of the cluster, you only need to perform partition expansion on the **Owner Node**. After this step is complete, perform **Step 3** to scan for disks. Other application servers in the cluster can identify the partitions after capacity expansion.

Figure 5-59 Partition expansion completed

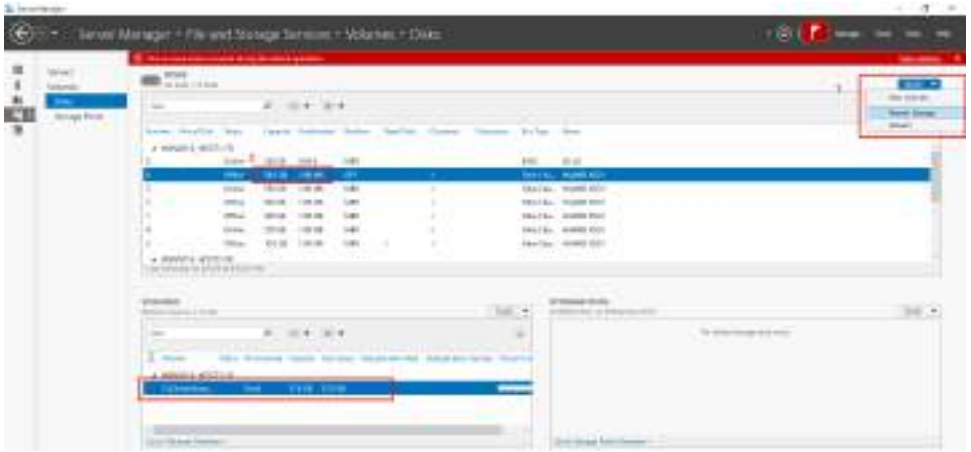


Step 3 Scan the shared volume and check the result of capacity expansion.

1. On the **Server Manager** page, choose **TASKS** > **Rescan Storage** to scan disks of all application servers in the cluster.

   After the scanning is complete, check the capacity after expansion in the **DISKS** area. In this example, the total capacity after disk scanning is 58 GB.

   Figure 5-60 Scan the shared volume



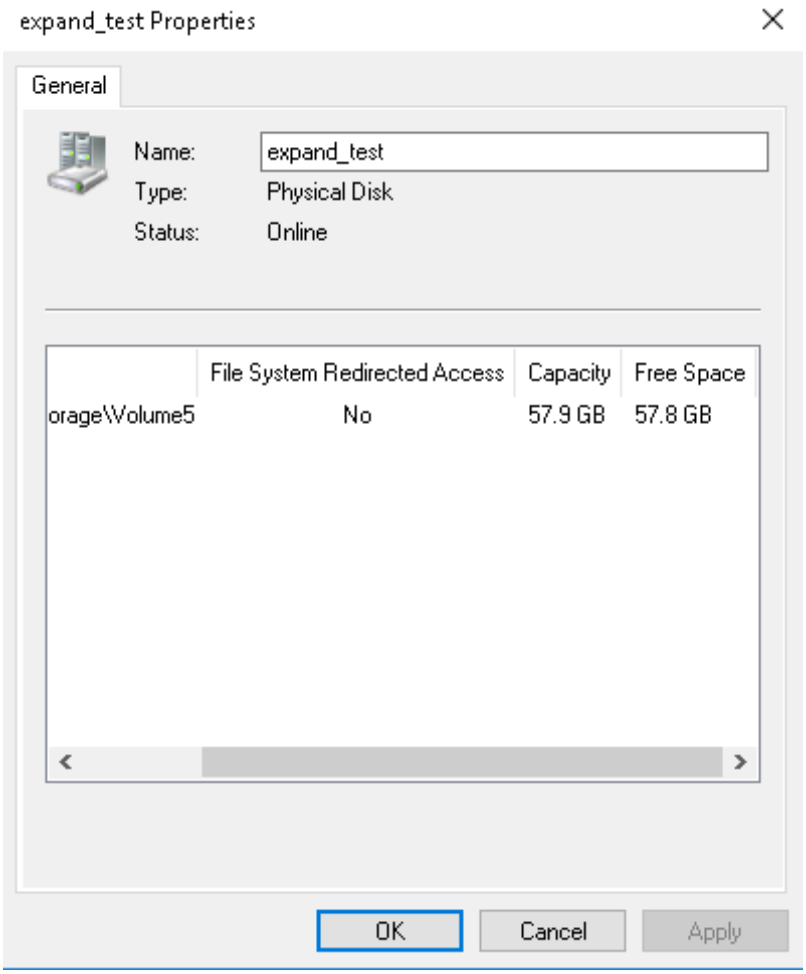
2. On the **Failover Cluster Manager** page, right-click the shared volume of the cluster and choose **Properties** from the shortcut menu.

   The **Properties** dialog box is displayed.

Figure 5-61 Properties

3. If the volume status is **Online** and the total volume capacity is the expected capacity after expansion, the volume is successfully expanded.

Figure 5-62 Volume status

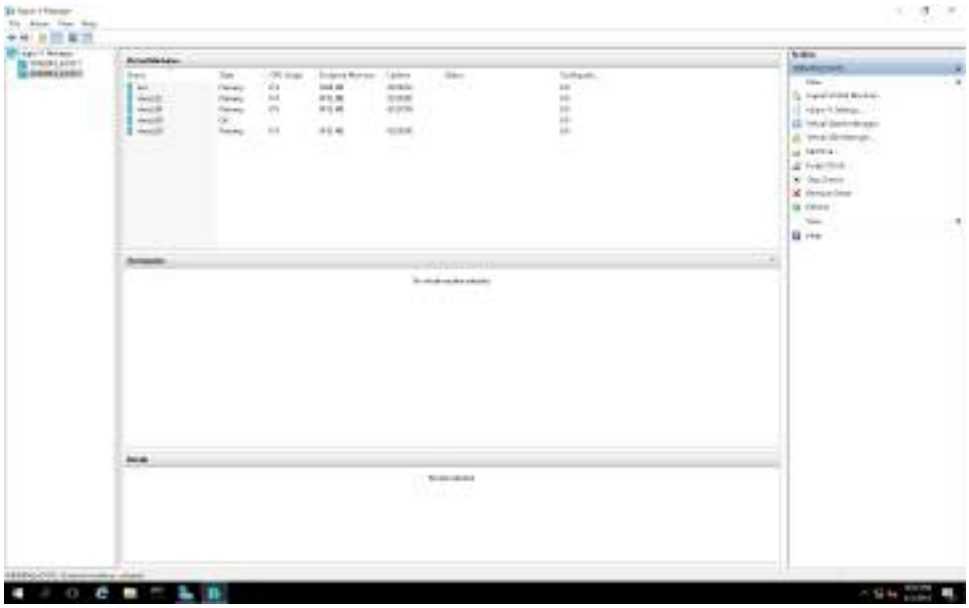


Step 4 Expand the disk capacity of a Hyper-V VM. This section describes how to expand the **test** VM on the **WIN2016_HOST2** application server.

1. On the **Server Manager** page, choose **Tools** > **Hyper-V Manager**.

   The **Hyper-V Manager** dialog box is displayed.

Figure 5-63 Hyper-V Manager



2. (Optional) Stop the VM. Right-click the VM to be expanded and choose **Turn Off** from the shortcut menu.

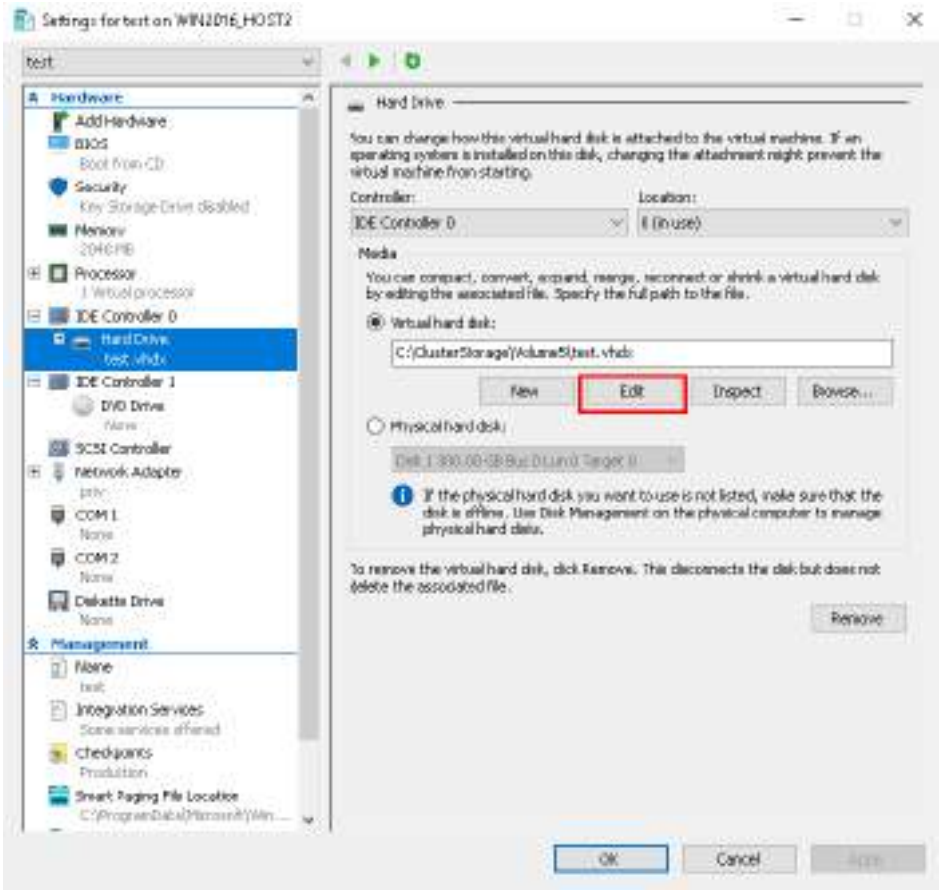
   NOTE

   - For a VM that uses the IDE disk controller, you must stop the VM before performing capacity expansion.
   - For Windows Server 2012 R2 to Windows Server 2019, if the VM uses the SCSI disk controller, skip this step.
   - For operating systems earlier than Windows Server 2012 R2, if the VM uses the SCSI disk controller, you must stop the VM before capacity expansion.

Figure 5-64 Stopping the VM

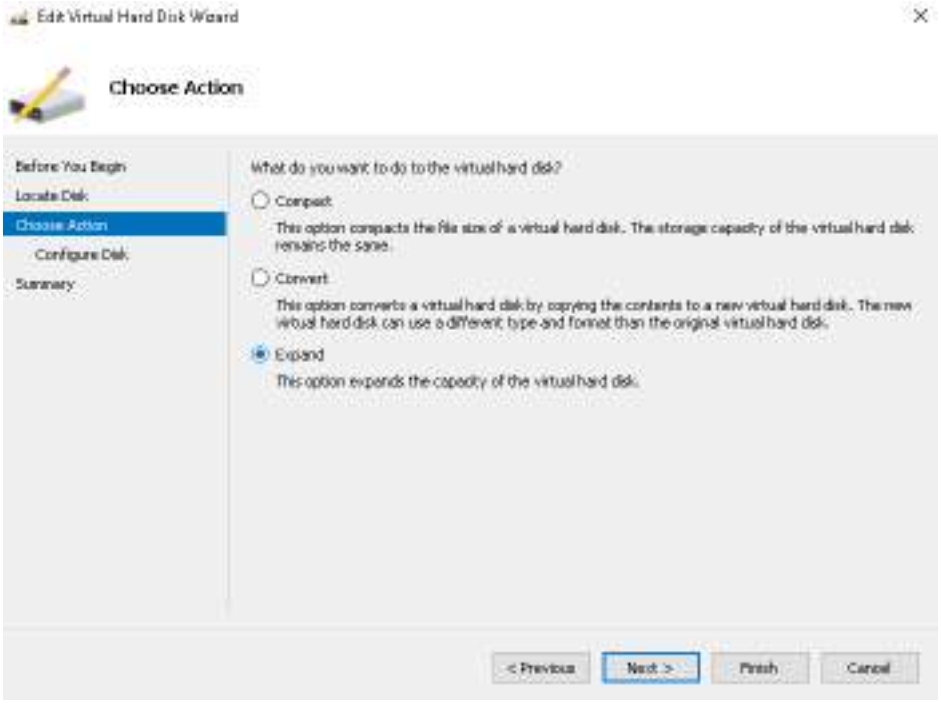
3. Right-click the VM name, and choose **Settings** from the shortcut menu.

Figure 5-65 Settings dialog box



4. In the navigation tree on the left, choose **Hard Drive** under the disk controller node to be expanded, and click **Edit**. The **Edit Virtual Hard Disk Wizard** dialog box is displayed.

Figure 5-66 Edit Virtual Hard Disk Wizard dialog box

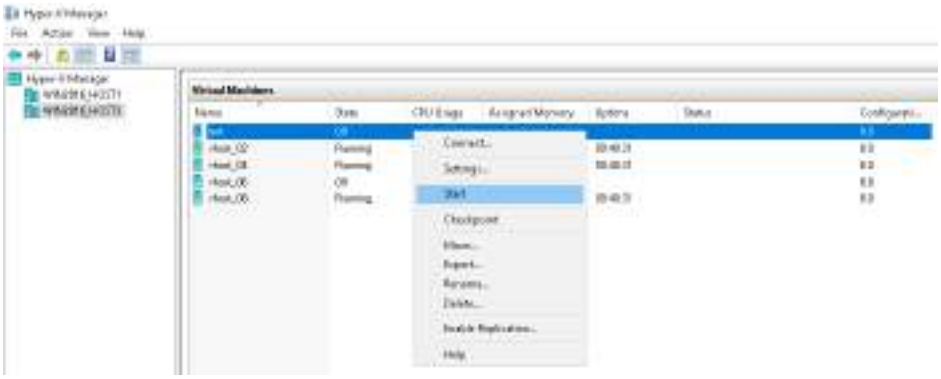


5. In the navigation tree on the left, click **Choose Action**, select **Expand**, and click **Next**.

   The **Configure Disk** page is displayed.

6. Enter the capacity after expansion in the **New size** text box and click **Finish**. The disk capacity expansion for the Hyper-V VM is completed.
7. If the VM is stopped, right-click the VM and choose **Start** from the shortcut menu to restart the VM.

Figure 5-67 Restarting the VM



----End

5.15.2.5.10 Expanding the LUN Capacity on a FusionCompute Application Server

After expanding LUN capacity on the storage system, configure the corresponding application server to identify and use the expanded storage space. This section uses FusionCompute 6.3.0 as an example. For FusionCompute application servers of other versions, adjust the operations based on actual conditions.

Prerequisites

- LUN capacity has been expanded on the storage system.
- No more than 64 capacity expansion operations have been performed on a datastore, and the total datastore capacity is not greater than 64 TB.
- The datastore type is virtualized SAN storage.

Procedure

Step 1 Scan for storage devices.

1. Log in to FusionCompute.
2. Click **Host and Cluster**.

   The **Host and Cluster** page is displayed.
3. In the navigation tree, choose **Site** > **Cluster** > **Host**.
4. In the middle function pane, choose **Resource** > **Storage Device**.

   The storage device list is displayed.

   Figure 5-68 Storage device list

   
5. Click **Scan**.

   The **Information** dialog box is displayed.
6. Click **OK**. The system starts to scan for storage devices.

   NOTE

   Click **click here** in the **Information** dialog box. On the **Task Center** page that is displayed, check the scan progress.

   After the scan is complete, you can view the capacity of IP SAN storage, which is the LUN mapped from the storage system to the application server.

Step 2 Expand the datastore capacity.

1. In the middle function pane, choose **Resource** > **Storage Device**.
2. Right-click the row of the datastore to be expanded and choose **Add Capacity** from the shortcut menu.

Figure 5-69 Expanding the datastore capacity

3. The storage devices that can be added are displayed in the list.
4. Select a storage device and click **OK**.

   The **Information** dialog box is displayed.
5. Click **OK**.

----End

5.15.3 Adding LUNs for Capacity Expansion

You can add LUNs to expand capacity for existing services, so that application servers can use the added storage space.

5.15.3.1 Adding LUNs on a Storage System

Create new LUNs on the storage system and map them to application servers' LUN groups.

Prerequisites

- Communication is normal between the storage system and the application server to which storage space is being expanded.
- You have determined the size of the new LUNs.
- The storage pool on the storage system has sufficient space for the new LUNs.
- If a Fibre Channel network is used, the WWN of the Fibre Channel initiator has been obtained.
- If an iSCSI network is used, the IQN of the iSCSI initiator has been obtained.

Procedure

Step 1 Locate the LUN group.

1. Log in to the CLI.
2. Run the **show initiator initiator_type=***?* **[wwn=***?***| iscsi_iqn_name=***?* **]** command to view the information about the corresponding host based on the initiator WWN or IQN.

Parameter	Description	Value
initiator_type=*?*	Initiator type.	Possible values are **FC** and **iSCSI**, where: – **iSCSI**: indicates an iSCSI initiator. – **FC**: indicates a Fibre Channel initiator.
wwn=*?*	WWN of a Fibre Channel initiator. This parameter is available only when **initiator_type=***?* is **FC**.	To obtain the value, run the **show initiator** command without parameters.
iscsi_iqn_name=*?*	IQN of an iSCSI initiator. This parameter is available only when **initiator_type=***?* is **iSCSI**.	To obtain the value, run the **show initiator** command without parameters.

```
admin:/>show initiator initiator_type=FC wwn=21000024ff53b640

WWN              : 21000024ff53b640
Running Status   : Online
Free             : Yes
Alias            : suse2_01
Host ID          : 2
Multipath Type   : Default
```

The value of **Host ID** is the ID of the host corresponding to the WWN.

3. Run the **show host host_group host_id=***?* command to query the information about the owning host group of the host.

```
admin:/>show host host_group host_id=2
Host Group ID Host Group Name
------------- ---------------
1             HostGroup000
```

4. Run the **show host_group mapping_view host_group_id=***?* command to query the information about the mapping view added to the host group.

```
admin:/>show host_group mapping_view host_group_id=1
Mapping View ID Mapping View Name
--------------- -----------------
0               testing
```

5. Run the **show mapping_view lun_group mapping_view_id=***?* command to query the information about the LUN group added to the mapping view.

```
admin:/>show mapping_view lun_group mapping_view_id=0
LUN Group ID    LUN Group Name
------------    --------------
1               lun_group_001
```

Step 2 Create LUNs.

1. On navigation bar of DeviceManager, choose **Services > Block Service > LUN Groups > LUNs**.
2. Click **Create**.

   The **Create LUN** page is displayed.
3. Set parameters as required. **Table 5-42** describes the parameters.

Table 5-42 Main parameters for creating a LUN

Parameter	Description
Capacity	Indicates the actual storage space assigned to the LUN.
Quantity	Indicates the quantity of LUNs to be created. The storage system allows you to create multiple LUNs at a time. Each LUN is allocated with the same capacity and automatically named.

4. Click **OK**.

   The LUN creation is complete.

Step 3 Add the new LUNs to the LUN group.

1. On navigation bar of DeviceManager, choose **Services > Block Service > LUN Groups.**
2. Select the LUN group and choose **More** > **Add LUN**.
3. In the **Available LUNs** area, select the new LUNs, and add them to the **Selected LUNs** area.
4. Click **OK**.

----End

5.15.3.2 Adding LUNs on an Application Server

5.15.3.2.1 Adding LUNs on a Windows Application Server

After creating LUNs and adding them to the LUN group on the storage system, configure the application server to identify and use the added storage space. This section uses an application server running Windows Server 2008 as an example. For application servers running other versions of Windows operating systems, adjust the operations based on actual conditions.

Prerequisites

LUNs have been created and added to a LUN group on the storage system.

Procedure

Step 1 Log in to the application server as an administrator.

Step 2 Right-click **Computer** and choose **Manage** from the shortcut menu.

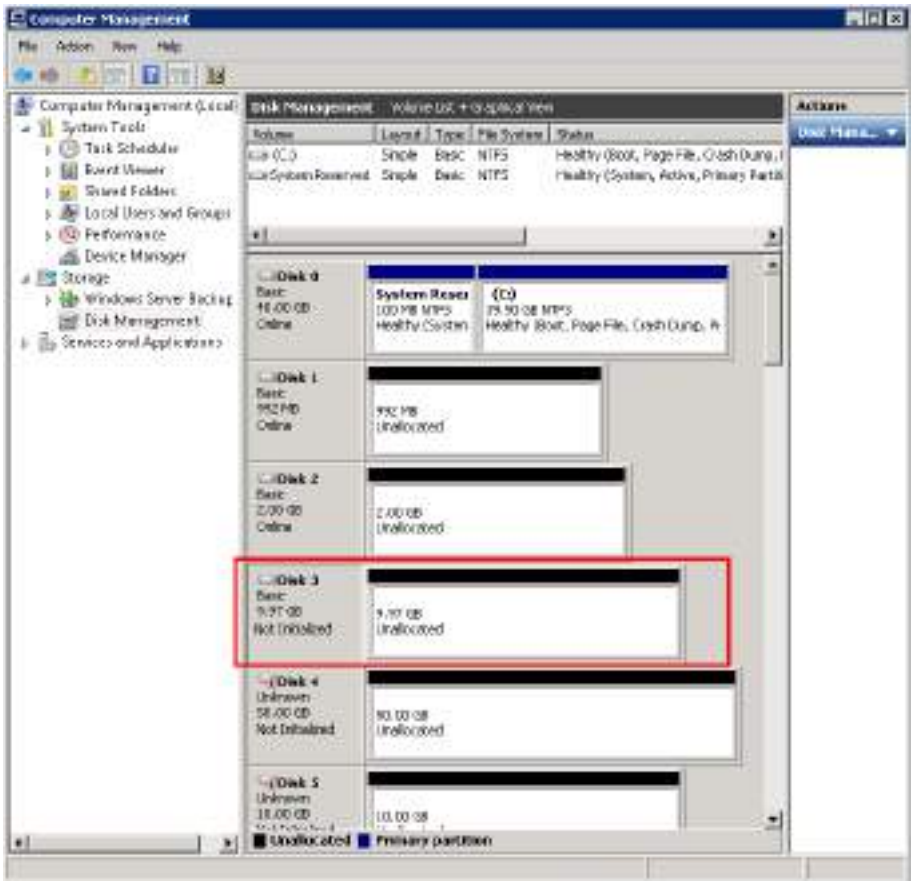
The **Server Manager** dialog box is displayed.

Step 3 Scan for new logical disks on the application server.

1. In the navigation tree of the **Server Manager** dialog box, choose **Storage** > **Disk Management**.
2. Right-click **Disk Management** and choose **Rescan Disks** from the shortcut menu.

After the scanning is complete, new logical disks are displayed on the right (using **Disk 3** as an example), as shown in **Figure 5-70**. (The display varies by disk size).

Figure 5-70 Viewing new logical disks



If no new logical disk is detected, perform the following operations:

a. Choose **Server Manager** > **Diagnostics** > **Device Manager** > **Disk Drives**.

b. Right-click **Disk Drives** and choose **Scan for hardware changes** from the shortcut menu.

c. Rescan for logical disks.

NOTE

If no new disk is detected, possible causes are:

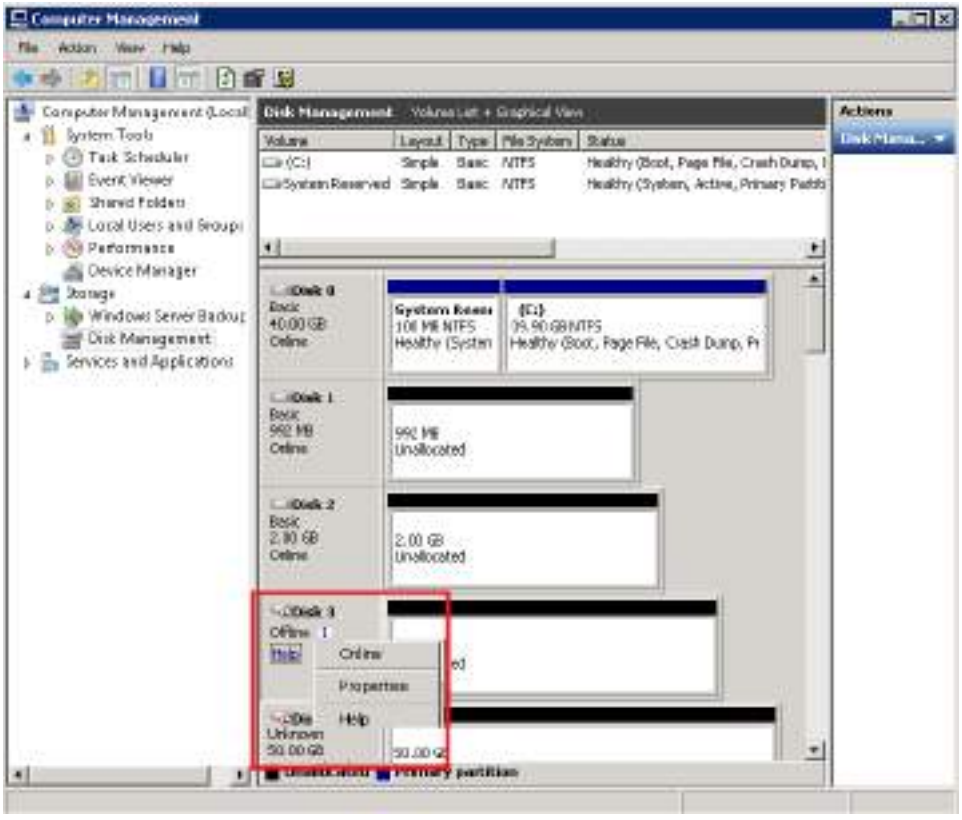
- The application server is incorrectly connected to the storage system after the network cable has been removed and reinserted.
- The link between the application server and storage system is down.
- The rate of the Fibre Channel front-end port is inconsistent with that of the Fibre Channel HBA on the application server.
- The HBA driver is not installed.
- A fault occurs in the storage pool.
- UltraPath has not been installed or an incorrect version has been installed.
- The device file on the application server is lost.

  For details, see Failure to Discover LUNs by an Application Server in *Troubleshooting Guide* specific to your product model and version.

Step 4 Initialize the new logical disks.

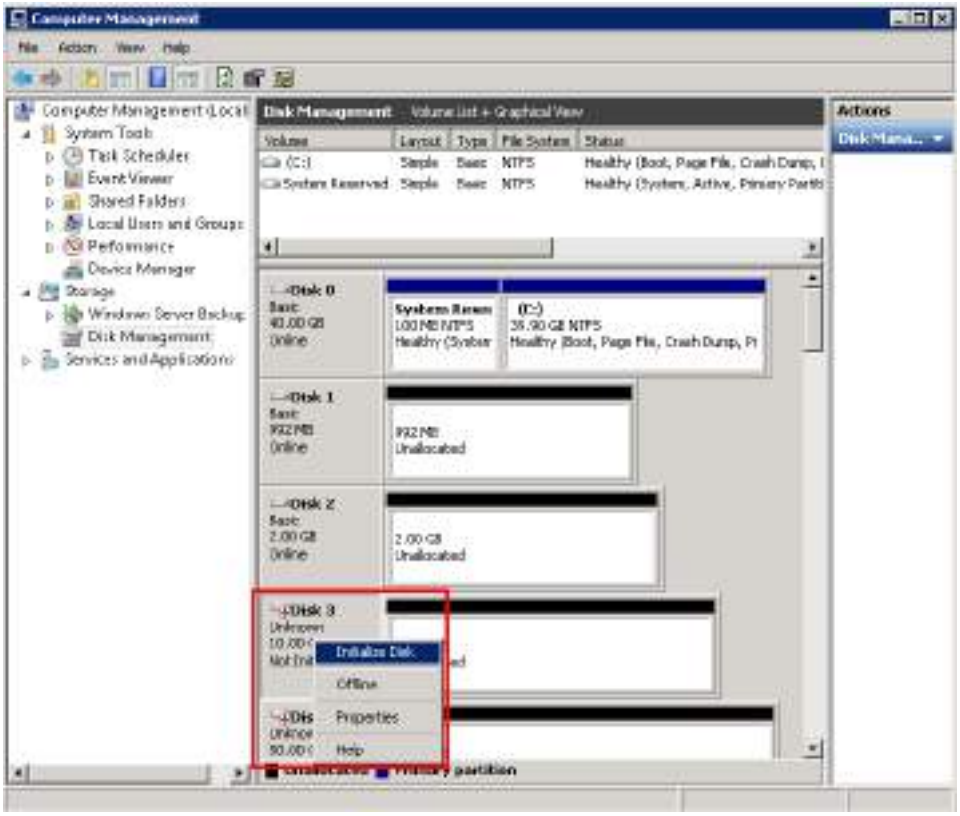
1. Right-click **Disk 3** and choose **Online** from the shortcut menu. The status of **Disk 3** changes to **Not Initialized**.

Figure 5-71 Online disk list



2. Right-click **Disk 3** and choose **Initialize Disk** from the shortcut menu.

Figure 5-72 Initializing disks



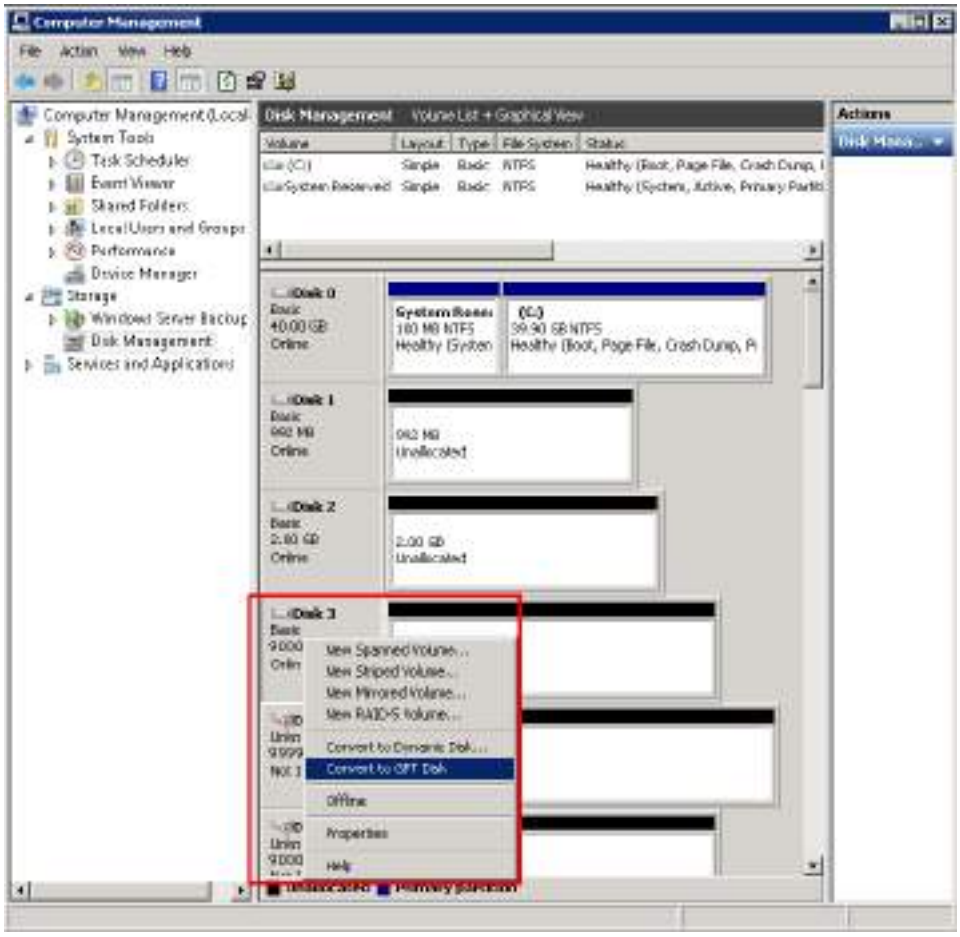
3. In the **Initialize Disk** dialog box that is displayed, select the logical disks that you want to initialize and click **OK**.

   Wait about one minute. When the status of **Disk 3** becomes **Online**, the initialization is successful.

Step 5 (Optional) If a new logical disk is larger than 2 TB, convert it into a GPT disk; otherwise, it is inaccessible.

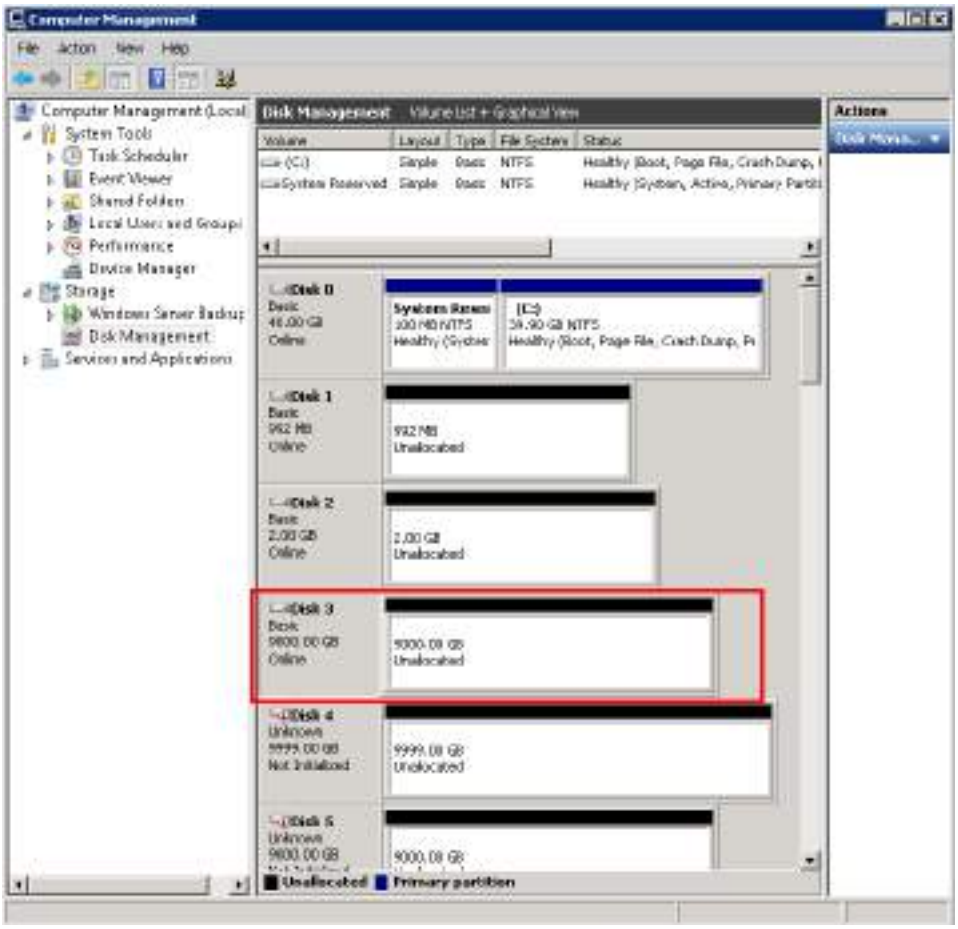
Right-click **Disk 3** and choose **Convert to GPT Disk** from the shortcut menu, as shown in **Figure 5-73**.

Figure 5-73 Converting a logical disk into a GPT disk



After a successful conversion, two partitions of the logical disk will combine, as shown in **Figure 5-74**.

Figure 5-74 Successful conversion of a logical disk into a GPT disk



Step 6 Partition and format the logical disks.

NOTE

When formatting a logical disk for the first time, do not read or write the logical disk until its status becomes **Healthy**; otherwise, the formatting may fail. If formatting fails, cancel the formatting operation and try again.

Step 7 Right-click the new logical disk and choose **Open** from the shortcut menu. You can read and write the logical disk.

----End

5.15.3.2.2 Adding LUNs on a SUSE Application Server

After creating LUNs and adding them to the LUN group on the storage system, configure the application server to identify and use the added storage space. This section uses an application server running SUSE 11.0 as an example. For application servers running other versions of SUSE operating systems, adjust the operations based on actual conditions.

Prerequisites

- LUNs have been created and added to a LUN group on the storage system.

- UltraPath has been installed on the application server.

Context

In this example, two LUNs have been mapped to the application server. The names of the two LUNs are **sdb** and **sdc**. A new thin LUN of 50 GB has been created and mapped to the application server using drive letter **sdd**. The name of the volume group is **thin**, the logical volume to be expanded is **lvthin**, and the file system's mount directory is **/dev/thin/lvthin**.

Procedure

Step 1 Scan for disks on the application server.

1. Run the **upadmin show vlun** command to query the existing LUNs. In this example, two LUNs are displayed.

```
# upadmin show vlun
Vlun ID     Disk        Name              Lun WWN              Status Capacity Ctrl(Own/Work)
Array Name
   0        sdb      SUSE11_LUN_01  6200bc71001faad3017fbf6b00000007  Normal
50.00GB              Huawei.Storage
   1        sdc      SUSE11_LUN_02  6200bc71001faad3017fc65b00000008  Normal
50.00GB              Huawei.Storage
```

2. Run the **hot_add** command to scan for disks.
3. Run the **upadmin show vlun** command again to query the current LUNs. Three LUNs are displayed.

```
# upadmin show vlun
Vlun ID     Disk        Name              Lun WWN              Status Capacity Ctrl(Own/Work)
Array Name
   0        sdb      SUSE11_LUN_01  6200bc71001faad3017fbf6b00000007  Normal
50.00GB              Huawei.Storage
   1        sdc      SUSE11_LUN_02  6200bc71001faad3017fc65b00000008  Normal
50.00GB              Huawei.Storage
   2        sdd      SUSE11_LUN_003  6200bc71001faad302429b1a0000000b Normal
50.00GB              Huawei.Storage
```

Step 2 Run the **pvcreate /dev/sdd** command to create a physical volume.

```
# pvcreate /dev/sdd
  Physical volume "/dev/sdd" successfully created
```

Step 3 Run the **vgextend thin /dev/sdd** command to expand the volume group.

```
# vgextend thin /dev/sdd
  Volume group "thin" successfully extended
```

Step 4 Run the **lvextend -L +49G /dev/thin/lvthin** command to expand the logical volume.

```
# lvextend  -L +49G /dev/thin/lvthin
  Extending logical volume lvthin to 148.00 GiB
  Logical volume lvthin successfully resized
```

Step 5 Run the **resize2fs /dev/thin/lvthin** command to expand the file system.

```
# resize2fs /dev/thin/lvthin
resize2fs 1.41.9 (22-Aug-2009)
Filesystem at /dev/thin/lvthin is mounted on /thin; on-line resizing required
old desc_blocks = 7, new_desc_blocks = 10
Performing an on-line resize of /dev/thin/lvthin to 38797312 (4k) blocks.
The filesystem on /dev/thin/lvthin is now 38797312 blocks long.
```

----End

5.15.3.2.3 Adding LUNs on an AIX Application Server

After creating LUNs and adding them to the LUN group on the storage system, configure the application server to identify and use the added storage space. This section uses an application server running AIX 6.1 as an example. For application servers running other versions of AIX operating systems, adjust the operations based on actual conditions.

Prerequisites

- LUNs have been created and added to a LUN group on the storage system.
- UltraPath has been installed on the application server.

Context

In this example, two LUNs have been mapped to the application server, which are named **hdisk2** and **hdisk3**. A new thin LUN of 50 GB has been created and mapped to the application server using drive letter **hdisk4**. The names of the volume group and the file system's mount directory are **thinvg** and **/thin**, respectively.

Procedure

Step 1 Run the **lsdev -Cc disk** command to view the information about identified disks.

```
# lsdev -Cc disk
hdisk0 Available 00-08-00 SAS Disk Drive
hdisk1 Available 00-08-00 SAS Disk Drive
hdisk2 Available 05-00-01 Huawei XXXX FC Disk Drive
hdisk3 Available 05-00-01 Huawei XXXX FC Disk Drive
```

In the command output, **XXXX** indicates the product model or brand.

Step 2 Run the **lsvg thinvg** command to check the capacity of the volume group to be expanded (which is **thinvg** in this example).

Step 3 Run the **lsdev -Cc adapter | grep fcs** and **cfgmgr -vl fcsX** commands to scan for disks.

```
# lsdev -Cc adapter | grep fcs
fcs0    Available 05-00 4GB FC PCI Express Adapter (df10000fe)
# cfgmgr -vl fcsX ;X=0,1,2,...
```

Step 4 Run the **lsdev -Cc disk** command again to view the information about identified disks.

```
# lsdev -Cc disk
hdisk0 Available 00-08-00 SAS Disk Drive
hdisk1 Available 00-08-00 SAS Disk Drive
hdisk2 Available 05-00-01 Huawei XXXX FC Disk Drive
hdisk3 Available 05-00-01 Huawei XXXX FC Disk Drive
hdisk4 Available 05-00-01 Huawei XXXX FC Disk Drive
```

Step 5 In the multipathing mode, run the **upadm show vlun** command to view LUN information.

```
# upadm show vlun
Vlun ID    Host Lun ID  Disk Name      Vlun Name              Vlun WWN               Status      In Use
Capacity  Controller(Own/Work)    Array Name          Array SN
    2         1        hdisk2     aix7_LUN_001    6200BC71001FAAD300E9891C0000000D    Available
Yes       50GB                        Huawei.Storage 210235G7FC10D8000001
    3         2        hdisk3     aix7_LUN_002    6200BC71001FAAD300E990520000000E    Available
Yes       50GB                        Huawei.Storage 210235G7FC10D8000001
```



```
   4        3        hdisk4     aix7_LUN_003     6200bc71001faad301045cae0000000f     Available      Yes
50GB                          Huawei.Storage 210235G7FC10D8000001
```

Step 6 Run the **extendvg thinvg hdisk4** command to expand the volume group.

Step 7 Run the **chfs -a size=+49G /thin** command to expand the file system.

----End

5.15.4 Modifying the Capacity of a File System

This operation enables you to modify the capacity of a file system to meet service requirements.

Context

For HyperMetro file systems, you can only modify the capacity of the local file system. After the modification, the capacity of the remote file system is automatically synchronized.

Procedure

Step 1 Choose **Services** > **File Service** > **File Systems**.

Step 2 Select the vStore to which the desired file system belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Click **More** on the right of the desired file system and select **Modify Capacity**.

The **Modify File System Capacity** page is displayed on the right.

NOTE

You can also click the name of the desired file system. In the upper right corner of the page that is displayed, click **Modify Capacity** from the **Operation** drop-down list.

Step 4 Set the file system capacity.

1. In **Capacity**, set the file system capacity.

   NOTE

   The file system capacity cannot exceed the system specifications.

2. Select a capacity unit from the right drop-down list.

   Possible options are **Block**, **MB**, **GB**, **TB**, and **PB**.

Step 5 Determine whether to change the capacity of a remote file system.

NOTE

- Changing the capacity of a remote file system is supported only when the local file system is configured with remote replication.
- If you do not select a remote file system, only the capacity of the local file system will be changed. To ensure availability of the remote replication pair, change the capacity of the local file system manually.
- Remote file systems with abnormal remote devices or invalid remote replication pairs cannot be selected.

Step 6 Click **OK**.

----End

5.15.5 Performing an Emergency Rollback

5.15.5.1 Performing an Emergency Rollback (for Windows)

This section describes how to roll back the storage system to the pre-expansion state if any exception occurs during expansion. The rollback procedure includes reclaiming the new LUNs, WWNs, and ports, and then scanning for disks on the application server.

Prerequisites

UltraPath has been installed on the application server.

Context

- The method to reclaim new LUNs described in this section is for the rollback of expansion by adding LUNs.
- This section uses Windows Server 2008 as an example.

Procedure

Step 1 (Optional) Reclaim new LUNs from the existing LUN group.

1. Log in to the CLI of the storage system.
2. Run the **remove lun_group lun** command to remove new LUNs from the LUN group. Specify the LUN group and the LUN to be removed using the **lun_group_id** and **lun_id_list** commands respectively.
3. Run the **show lun_group lun** command to view LUNs contained in the LUN group. Specify the LUN group using the **lun_group_id** command.

   The LUN group does not contain the new LUNs.

Step 2 (Optional) Reclaim new WWNs from the existing host group.

1. Log in to the CLI of the storage system.
2. Run the **remove host initiator initiator_type=FC** command to remove new initiators from the host group. Specify the WWN of the initiator to be removed using **wwn**.
3. Run the **show initiator** command to view the current initiator information about the host. Specify the host using the **host_id** command.

   The information does not contain the new initiators.

Step 3 (Optional) Reclaim new ports from the existing port group.

1. Log in to the CLI of the storage system.
2. Run the **remove port_group port** command to remove new ports from the port group. Specify the port group, the type of the port, and the port to be removed using the **port_group_id**, **port_type**, and **port_id_list** commands respectively.

3. Run the **show port_group port** command to view the information about the ports in the port group. Specify the port group using the **port_group_id** command.

   The port group does not contain the new ports.

Step 4 Scan for disks on the application server.

1. Log in to the Windows Server 2008 application server as an administrator.
2. On the desktop, click **Start** and choose **Administrative Tools** > **Server Manager**.

   The **Server Manager** dialog box is displayed.
3. In the navigation tree of the **Server Manager** dialog box, right-click **Disk Management** and choose **Rescan Disks** from the shortcut menu.
4. In UltraPath's CLI on the application server, run the **upadm show vlun** and **upadm show path** commands to view the device information of UltraPath.

   The command outputs do not contain information about the added disks.

Step 5 Check the application server's running status after the rollback.

1. From the **Server Manager** dialog box, go to the **Event Viewer** and **Device Manager** pages respectively to check for any errors.

   If there are errors, resolve them before proceeding with the next step.
2. Run the **upadm show path** command to check the disk path status.

----End

5.15.5.2 Performing an Emergency Rollback (for Linux)

This section describes how to roll back the storage system to the pre-expansion state if any exception occurs during expansion. The rollback procedure includes reclaiming the new LUNs, WWNs, and ports, and then scanning for disks on the application server.

Prerequisites

UltraPath has been installed on the application server.

Context

The method to reclaim new LUNs described in this section is for the rollback of expansion by adding LUNs.

Procedure

Step 1 (Optional) Reclaim new LUNs from the existing LUN group.

1. Log in to the CLI of the storage system.
2. Run the **remove lun_group lun** command to remove new LUNs from the LUN group. Specify the LUN group and the LUN to be removed using the **lun_group_id** and **lun_id_list** commands respectively.
3. Run the **show lun_group lun** command to view LUNs contained in the LUN group. Specify the LUN group using the **lun_group_id** command.

The LUN group does not contain the new LUNs.

Step 2 (Optional) Reclaim new WWNs from the existing host group.

1. Log in to the CLI of the storage system.
2. Run the **remove host initiator initiator_type=FC** command to remove new initiators from the host group. Specify the WWN of the initiator to be removed using the **wwn** command.
3. Run the **show initiator** command to view the current initiator information about the host. Specify the host using the **host_id** command.

   The information does not contain the new initiators.

Step 3 (Optional) Reclaim new ports from the existing port group.

1. Log in to the CLI of the storage system.
2. Run the **remove port_group port** command to remove new ports from the port group. Specify the port group, the type of the port, and the port to be removed using the **port_group_id**, **port_type**, and **port_id_list** commands respectively.
3. Run the **show port_group port** command to view the information about the ports in the port group. Specify the port group using the **port_group_id** command.

   The port group does not contain the new ports.

Step 4 Scan for disks on the application server.

1. Run the **upRescan** command to rescan for disks.
2. Run the **upadmin show vlun** and **upadmin show path** commands to view the device information of UltraPath.
3. Run the **fdisk -l** command to view the disk information on the host.

The command outputs in **Step 4.2** and **Step 4.3** do not contain information about the new disks.

Step 5 Check the host's running status after the rollback.

1. Run the **tail -200 /var/log/messages** command to check for any errors.

   If there are errors, resolve them before proceeding with the next step.
2. Run the **upadmin show path** command to check the disk path status.

----End

5.15.5.3 Performing an Emergency Rollback (for AIX)

This section describes how to roll back the storage system to the pre-expansion state if any exception occurs during expansion. The rollback procedure includes reclaiming the new LUNs, WWNs, and ports, and then scanning for disks on the application server.

Prerequisites

UltraPath has been installed on the application server.

Context

The method to reclaim new LUNs described in this section is for the rollback of expansion by adding LUNs.

Procedure

Step 1 Delete device files corresponding to the new LUNs.

1. Run the **upadm show vlun** command to view the information about all LUNs.
2. Run the **rmdev -dl** command to delete the new virtual disks identified by UltraPath.

   hdisk*X* indicates a new virtual disk generated after disk re-allocation during expansion.
3. Run the **upadm show vlun** command to view the information about all LUNs.

   Compare the command output with the result of **Step 1.1** to check whether new virtual disks identified by UltraPath have been deleted.

Step 2 (Optional) Reclaim new LUNs from the existing LUN group.

1. Log in to the CLI of the storage system.
2. Run the **remove lun_group lun** command to remove new LUNs from the LUN group. Specify the LUN group and the LUN to be removed using the **lun_group_id** and **lun_id_list** commands respectively.
3. Run the **show lun_group lun** command to view LUNs contained in the LUN group. Specify the LUN group using the **lun_group_id** command.

   The LUN group does not contain the new LUNs.

Step 3 (Optional) Reclaim new WWNs from the existing host group.

1. Log in to the CLI of the storage system.
2. Run the **remove host initiator initiator_type=FC** command to remove new initiators from the host group. Specify the WWN of the initiator to be removed using **wwn**.
3. Run the **show initiator** command to view the current initiator information about the host. Specify the host using the **host_id** command.

   The information does not contain the new initiators.

Step 4 (Optional) Reclaim new ports from the existing port group.

1. Log in to the CLI of the storage system.
2. Run the **remove port_group port** command to remove new ports from the port group. Specify the port group, the type of the port, and the port to be removed using the **port_group_id**, **port_type**, and **port_id_list** commands respectively.
3. Run the **show port_group port** command to view the information about the ports in the port group. Specify the port group using the **port_group_id** command.

   The port group does not contain the new ports.

Step 5 Scan for disks on the application server.

1. Run the **upRescan** command to rescan for disks.

2. Run the **upadm show vlun** and **upadm show path** commands to view the device information of UltraPath.
3. Run the **fdisk -l** command to view the disk information on the host.

The command outputs in **Step 5.2** and **Step 5.3** do not contain information about the new disks.

Step 6 Check the host's running status after the rollback.

1. Run the **errpt** command to check for any errors.

   If there are errors, resolve them before proceeding with the next step.
2. Run the **upadm show path** command to check the disk path status.

----End

5.15.5.4 Performing an Emergency Rollback (for HP-UX)

This section describes how to roll back the storage system to the pre-expansion state if any exception occurs during expansion. The rollback procedure includes reclaiming the new LUNs, WWNs, and ports, and then scanning for disks on the application server.

Context

The method to reclaim new LUNs described in this section is for the rollback of expansion by adding LUNs.

Procedure

Step 1 (Optional) Reclaim new LUNs from the existing LUN group.

1. Log in to the CLI of the storage system.
2. Run the **remove lun_group lun** command to remove new LUNs from the LUN group. Specify the LUN group and the LUN to be removed using the **lun_group_id** and **lun_id_list** commands respectively.
3. Run the **show lun_group lun** command to view LUNs contained in the LUN group. Specify the LUN group using the **lun_group_id** command.

   The LUN group does not contain the new LUNs.

Step 2 (Optional) Reclaim new WWNs from the existing host group.

1. Log in to the CLI of the storage system.
2. Run the **remove host initiator initiator_type=FC** command to remove new initiators from the host group. Specify the WWN of the initiator to be removed using the **wwn** command.
3. Run the **show initiator** command to view the current initiator information about the host. Specify the host using the **host_id** command.

   The information does not contain the new initiators.

Step 3 (Optional) Reclaim new ports from the existing port group.

1. Log in to the CLI of the storage system.
2. Run the **remove port_group port** command to remove new ports from the port group. Specify the port group, the type of the port, and the port to be

removed using the **port_group_id**, **port_type**, and **port_id_list** commands respectively.

3. Run the **show port_group port** command to view the information about the ports in the port group. Specify the port group using the **port_group_id** command.

   The port group does not contain the new ports.

Step 4 Delete device files.

1. Run the **ioscan -fnkC disk** and **ioscan -fnkC disk | grep -i HUAWEI | wc -l** commands to view the information about all LUNs.
2. Delete path device files.
   a. Run the **ioscan -fnC disk** command to scan for system disks.
   b. Run the **ioscan -fnkC disk | grep -i NO_HW** command to check for disks whose status is **NO_HW**.
   c. Run the **ioscan -fnkC disk | grep -i NO_HW | awk '{ print $3}' | xargs -n1 rmsf -C disk -H** command to delete disks whose status is **NO_HW**.
   d. Run the **ioscan -fnkC disk | grep -i NO_HW** command again to check for disks whose status is **NO_HW**.
3. Run the **ioscan -fnkC disk** and **ioscan -fnkC disk | grep -i HUAWEI | wc -l** commands again to view the information about all LUNs.

   Compare the command outputs with the results in **Step 4.1** to check whether path device files have been deleted.

Step 5 Check the host's running status after the rollback.

1. Run the **tail -200 /var/adm/syslog/syslog.log** command to check for any errors.

   Handle the errors before proceeding with the next step.
2. Run the **ioscan -fnkC disk** command to check the disk path status.

----End

5.16 Erasing Data from Disks (SmartErase)

You need to erase data from disks if their life cycles end, or if they are faulty and need to be returned for repair, or if the security level of the area where the storage system resides decreases.

5.16.1 Function Characteristics and Application Scenarios

The data erasure feature (SmartErase) of OceanStor storage systems overwrites the original data on disks. In this way, data on disks is permanently erased and cannot be restored.

Function Characteristics

- The erased data cannot be restored, ensuring information security.
- Three data erasure mechanisms are provided.
  - **block_erase:** It is a block-level data erasure mechanism that erases both user data and mapping.

  - **cryptographic_erase**: Oriented to self-encrypting disks (SEDs), this mechanism erases both user data and mapping by erasing security keys.
  - **overwrite**: This mechanism overwrites user data by repeatedly writing specific hexadecimal numbers. Currently, the supported overwrite standards are **DoD 5220.22-M (E)**, **DoD 5220.22-M (ECE)**, **VSITR**, and **Custom**.
    - DoD 5220.22-M (E): DoD 5220.22-M standard that enables a storage system to write 0x55, 0xAA, and a pseudo random number in sequence.
    - DoD 5220.22-M (ECE): DoD 5220.22-M (ECE) standard that enables a storage system to write 0x55, 0xAA, a pseudo random number, a pseudo random number, 0x55, 0xAA, and a pseudo random number in sequence.
    - VSITR: VSITR standard that enables a storage system to write 0x00, 0xFF, 0x00, 0xFF, 0x00, 0xFF, and a pseudo random number in sequence.
    - Custom: User-defined standard. You can customize the hexadecimal numbers to be written and the number of write times.

  NOTE

  - The SmartErase license is not displayed on the **License Management** page in DeviceManager.
  - The data erasure function can be implemented based on DoD 5220.22-M (E), DoD 5220.22-M (ECE), VSITR, and Custom standards. However, the function is not certified by a third-party professional data erasure organization. If you need third-party professional certification, purchase a third-party professional data erasure service.
  - Do not erase disk data within 15 minutes after the storage system is upgraded or a patch is installed.
- Data erasure results can be verified.

Application Scenarios

- Erase data from selected disks. In this scenario, you can erase data in either of the following ways:
  - User data erasure: Erase user data but retain disk authentication information.
  - Full erasure: Erase both user data and disk authentication information.

  NOTE

  - Disk authentication information is used by Huawei storage systems to identify and authenticate disks. Storage systems cannot identify disks whose authentication information is erased.
  - The disks whose authentication information is retained can be used again, but the disks whose authentication information is erased can no longer be used.
  - Data erasure operations performed on DeviceManager and in the CLI user view only erase user data but retain disk authentication information.
  - Full erasure can be performed only in the CLI engineer view.
- Erase data from all disks in a storage pool to be deleted. For details, see **Deleting a Storage Pool** in the *Basic Storage Service Configuration Guide*.

NOTE

This operation will not erase data from the faulty disks in a storage pool.

5.16.2 Erasing Data from a Single Disk

This section describes how to erase data from a single disk. Erased data cannot be restored, thereby ensuring data security.

Prerequisites

- The storage system is running properly.
- To ensure user data security, data on member disks in a storage pool cannot be erased.
- To erase data from a faulty disk in a storage pool, perform the following operations:
  - If there are vacant slots in the storage system, you are advised to replace the faulty disk first. Do not erase data on a newly inserted disk in the slot of the replaced disk. Insert the faulty disk into a vacant slot, and then erase data as instructed in this section. For details about how to replace a disk, see the *Parts Replacement*.
  - If there is no vacant slot in the storage system, contact Huawei technical support engineers.

Precautions

- This section describes how to erase data from disks using DeviceManager. This operation erases user data but retains disk authentication information. After data is erased, the disks can still be used. If you want to perform full erasure (which makes a disk unavailable), run the **change disk erase** command. For details about this command, see the *Advanced O&M Command Reference*.
- Disks whose data is being erased cannot be added to a storage pool.
- Data on unreadable and unwritable disks cannot be erased.
- Do not power off or remove disks whose data is being erased. Otherwise, the system may crash. If data erasure is interrupted due to power outage or other reasons, the system automatically resumes the data erasure after the system is powered on or the disk is inserted to the original storage system. In addition, the system reports a disk fault alarm (0XF00A0001), which will be cleared automatically after data erasure is complete.

  NOTE

  If the disk has been powered off or removed for more than 15 days, the system cannot resume data erasure and, therefore, cannot access the disk.
- If disks do not support data erasure, when you attempt to erase data from such disks, the storage system returns error code **0x40000A67** or **0x40000A68**.
- After data has been erased from a disk, a power cycle is automatically performed for this disk.
- When the block_erase or cryptographic_erase mechanism is used, the data erasure duration lasts for about 10 minutes. When the overwrite mechanism

is used, the data erasure duration greatly varies with erasure parameters and disk capacity specifications from hours to dozens of hours.

- Do not run any commands for clearing configuration during data erasing, including **ccdb.sh -c clearccdb**, **ccdb.sh -c cleardbfile**, **ccdb.sh -c repairdb**, **ccdb.sh -c clearall**, **ccdb.sh -c deletedb**, **restore system factory_mode**, **change ccdb general**, **change cluster controllers**, **change controllers_expansion cancel**, and **clear configuration_data**.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Click **System** > **Hardware** > **Devices**.

Step 3 Select a controller enclosure or disk enclosure and then select disks for data erasure.

Step 4 Erase data from the disks.

1. In the lower part of the window, click **Erase Data**.

   NOTE

   If one of the selected disks is a disk in a storage pool, the **Erase Data** option is unavailable.

   The **Erase Data** dialog box is displayed.

2. Set parameters.

   For details about the parameters, see **Table 5-43**.

Table 5-43 Data erasure parameters

Parameter	Description	Value
Data Erasure Mechanism	Data erasure mechanism. Possible values are as follows: – **block_erase**: Implements block-level data erasure. – **cryptographic_erase**: Erases security keys. **NOTE** This parameter applies only to SEDs. – **overwrite**: Writes specific hexadecimal numbers to overwrite disk data. **NOTE** Different types of disks support different data erasure mechanisms. When a system erases the data in a selected disk, if it reports an event indicating that the specified data erasure mechanism is not supported, use another data erasure mechanism.	[Example] overwrite

Parameter	Description	Value
Data Erasure Standard	Standard with which the **overwrite** data erasure mechanism complies. Possible values are **DoD 5220.22-M (E)**, **DoD 5220.22-M (ECE)**, **VSITR**, and **Custom**. **NOTE** – This parameter is valid only when **Data Erasure Mechanism** is set to **overwrite**. – If **Data Erasure Standard** is set to **Custom**, the system overwrites disk data according to the **Pattern Value** and **Number of Overwrites** set by a user. – **DoD 5220.22-M (E)**: DoD 5220.22-M standard that enables a storage system to write 0x55, 0xAA, and a pseudo random number in sequence. – **DoD 5220.22-M (ECE)**: DoD 5220.22-M (ECE) standard that enables a storage system to write 0x55, 0xAA, a pseudo random number, a pseudo random number, 0x55, 0xAA, and a pseudo random number in sequence. – **VSITR**: VSITR standard that enables a storage system to write 0x00, 0xFF, 0x00, 0xFF, 0x00, 0xFF, and a pseudo random number in sequence. – **Custom**: User-defined standard. You can customize the hexadecimal numbers to be written and the number of write times.	[Example] custom
Pattern Value	A one-byte pattern value used to overwrite disk data. **NOTE** – This parameter is valid only when **Data Erasure Mechanism** is set to **overwrite** and **Data Erasure Standard** is set to **Custom**. – The value can be **r** or a hexadecimal number starting with **0x**, both of which occupy one byte. A maximum of three values can be entered and separated by commas (,). – When **Pattern Value** is set to **r**, it represents a random number.	[Example] 0x00
Number of Overwrites	Number of times that disk data is overwritten by **Pattern Value**. **NOTE** This parameter is valid only when **Data Erasure Mechanism** is set to **overwrite** and **Data Erasure Standard** is set to **Custom**.	[Value range] 1 to 15 [Example] 5

Parameter	Description	Value
Verify Data Erasure	Indicates whether to enable data erasure verification. If this function is enabled, the system checks whether the data has been erased after executing data erasure. **NOTE** – This parameter is valid only when **Data Erasure Mechanism** is set to **overwrite** or **block_erase**. – The speed of verifying SSD data erasure is about 200 MB/s to 350 MB/s. Estimate the verification time and then determine whether to enable verification or select a proper percentage of data to be verified. – You can view the data erasure report to check whether data is successfully erased. If the value of **Result** in the report is **Completed**, data is successfully erased. For details, see **5.16.4 Exporting a Data Erasure Report**.	[Default] Disable
Data to Be Verified (%)	Percentage of to-be-verified data size to the total capacity of a disk. **NOTE** This parameter is valid only when **Data Erasure Mechanism** is set to **overwrite** or **block_erase** and **Verify Data Erasure** is set to **Enable**.	[Value range] 1 to 100 [Default] 10

Step 5 Click **OK**.

A **Danger** dialog box is displayed.

Step 6 Confirm the content in the dialog box, enter **I have read the preceding information and understood consequences of the operation.** as prompted, and click **OK**.

NOTE

If **Verify Data Erasure** is set to **Enable**, another **Danger** dialog box will be displayed. Confirm the content in the dialog box, select **I have read and understand the consequences associated with performing this operation**, and click **OK**.

----End

5.16.3 Viewing the Data Erasure Progress of a Disk

This section describes how to view the data erasure progress of a disk.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Click **System > Hardware > Devices**.

Step 3 Select a controller enclosure or disk enclosure, and then select on the device diagram the disk whose information you want to view.

Step 4 In the pop-up **Disk** window, view **Data Erasure Progress**.

NOTE

Data Erasure Progress is a percentage, and **100** indicates that data erasure is completed.

----End

5.16.4 Exporting a Data Erasure Report

You can export a data erasure report to view disks' data erasure logs.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose  > **Export Data**.

Step 3 Under **Disk Log**, click **Disk Data Erasure Report**. In the **Warning** dialog box that is displayed, select **I have read and understand the consequences associated with performing this operation** and click **OK**.

The system automatically exports a data erasure report.

----End

6 FAQ

This chapter describes frequently asked questions (FAQs) about the management and maintenance of the storage system. If a problem occurs when you maintain the feature, you can browse this chapter for the answer to the problem.

6.1 How Do I Use the Advanced Search Function of DeviceManager?

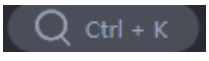
Question

How do I use the advanced search function of DeviceManager?

Answer

The advanced search function allows you to efficiently and conveniently search for resources in a storage system by status, performance, capacity, creation time, and associated resources. This function also supports quick resource provisioning, common page redirection, function updates, and quick start.

To meet different user habits, the global search function supports two search modes: simple and advanced search. You can perform the following steps to switch the search mode:

- Switch to the advanced search mode: On the DeviceManager home page, click the global search button 

and then click the advanced search button  on the displayed page. The advanced search function page

is displayed, as shown in **Figure 6-1**. **Table 6-1** describes the functional areas on the advanced search function page.

- Switch to the simple search mode: On the DeviceManager home page, click the global search button 

. On the displayed advanced search function page, click the simple search mode button at the end of the search bar.

Figure 6-1 The advanced search function page

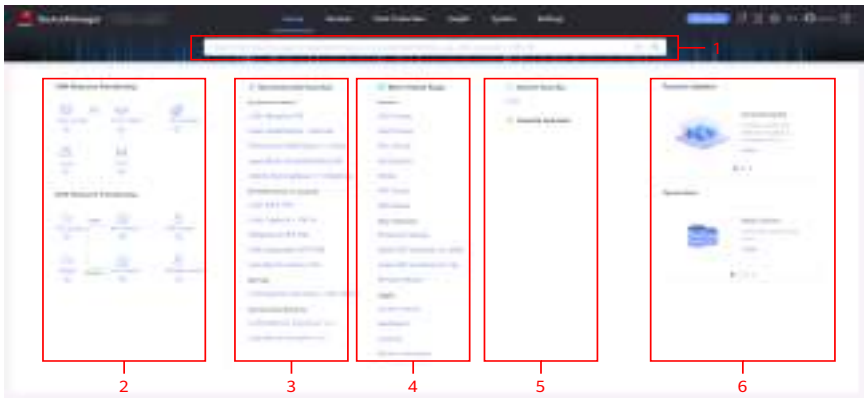


Table 6-1 Functional areas on the advanced search function page

No.	Name	Description
1	Search Bar	In the search bar, you can search for target pages and operation entries. In addition, you can click a search result of a common resource type to access the corresponding information page of the resource, as shown in **Figure 6-2**. Keywords for common resource types include LUNs, FileSystems, LUNGroups, PortGroups, Hosts, HostGroups, vStores, LogicalPorts, and LUNSnapshots. **NOTE** If the keywords entered in the search bar meet the rule of "*Keyword of a common resource type Name/Performance/Status (or other metric)*", the corresponding resource information page is displayed. The search results that meet the search criteria are displayed on the left of the page. After you click a search result, the basic information, performance metrics, and running status of the result are displayed in the middle of the page, and the events, alarms, operations, and help information related to the result are displayed on the right of the page.
2	Resource Provisioning area	This area contains the SAN and NAS resource provisioning flowcharts and quick redirection buttons.

No.	Name	Description
3	Recommended Searches area	This area displays search examples supported for resource related metrics: ● Search by resource status: *Resource Status of the resource Parameter of the status*. For example, **LUN Mapping status Yes**. ● Search by performance or capacity: *Resource A performance metric of the resource Value of the metric*. For example, **LUN IOPS TOP**. ● Search by time: *Resource A point in time of the resource Discriminant of the point in time.* For example, **LUN snapshot Activation point in time > 2020-01-01**. ● Search by associated resource: *Resource Resource associated with the resource.* For example, **LUN snapshot Source LUN**.
4	Most Visited Pages area	This area provides convenient redirection functions for services, data protection, and monitoring pages.
5	Recent Searches and Favorite Searches area	● The **Recent Searches** area displays the historical records of keywords that have been searched in the search bar and supports quick redirection. ● The **Favorite Searches** area displays the search keywords in favorites and supports quick redirection. **NOTE** ● To add a keyword to favorites, enter the keyword in the search bar and click ☆ at the end of the search bar. ● To remove a keyword from favorites, move the cursor onto the keyword and click ⊖ displayed following the keyword.
6	Function Updates and Quick Start area	● The **Function Updates** area displays and introduces updated functions by version. You can click a card to go to the related page on DeviceManager. ● The **Quick Start** area displays the end-to-end provisioning process of a resource.

Figure 6-2 Resource information display page

6.2 How Do I Query the Mapping Between Host Disks and LUNs When the UltraPath Software Is Not Installed?

When the UltraPath is not installed on a host, perform the following operations to query the mapping between host disks and LUNs.

Querying the Mapping Between Host Disks and LUNs (Windows)

Step 1 On the storage system, obtain the WWN of the LUN mapped to the host.

1. Log in to the command-line interface (CLI) of the storage system as a super administrator.
2. Run **show initiator initiator_type=? [wwn=? | iscsi_iqn_name=?]** to show the host corresponding to the WWN or iSCSI IQN.

```
admin:/>show initiator initiator_type=FC wwn=21000024ff53b640

WWN              : 21000024ff53b640
Running Status   : Online
Free             : Yes
Alias            : suse2_01
Host ID          : 2
Multipath Type   : Default
```

   In the preceding command output, the value of **Host ID** is the host corresponding to the WWN.

3. Run **show host lun host_id=***?* command to view all LUNs mapped to the host.

   host_id=*?* represents the ID of a host.

```
admin:/>show host lun host_id=2

 LUN ID  LUN Name
 ------  ------------
 34      lun_0000
 35      lun_0001
 36      lun_0002
```

   The value of **LUN ID** is the ID of a LUN mapped to the host in the storage system.

4. Run the **show lun general lun_id=***?* command to view the WWN of the LUN mapped to the host.

Step 2 On the host, obtain the WWN of the LUN corresponding to a disk.

1. Log in to the Windows application server as an administrator.
2. Press **Windows+R** (if the operation is performed remotely, perform it in full screen mode) to open the **Run** dialog box.
3. Enter **diskmgmt.msc** and press **Enter**.
4. In the displayed **Disk Management** window, right-click the disk you want to query, and choose **Properties**.
5. On the **Details** tab page, set **Property** to **Device Instance Path**. **Value** below **Property** is the serial number of the disk.

NOTE

The serial number is an ASCII character. You can obtain the WWN of the LUN corresponding to the disk by seeing the ASCII table.

Step 3 Check whether the WWN of the LUN mapped to the host and that of the host disk are the same. If they are, the LUN is just the one corresponding to the host disk.

----End

Querying the Mapping Between Host Disks and LUNs (Linux)

Step 1 On the storage system, obtain the WWN of the LUN mapped to the host.

1. Log in to the command-line interface (CLI) of the storage system as a super administrator.
2. Run **show initiator initiator_type=? [wwn=? | iscsi_iqn_name=?]** to show the host corresponding to the WWN or iSCSI IQN.

```
admin:/>show initiator initiator_type=FC wwn=21000024ff53b640

WWN              : 21000024ff53b640
Running Status   : Online
Free             : Yes
Alias            : suse2_01
Host ID          : 2
Multipath Type   : Default
```

   The value of **Host ID** is the ID of a host corresponding to the WWN.
3. Run **show host lun host_id=***?* to view all LUNs mapped to the host.

   host_id=*?* represents the ID of a host.

```
admin:/>show host lun host_id=2

 LUN ID  LUN Name
 ------  ------------
 34      lun_0000
 35      lun_0001
 36      lun_0002
```

   The value of **LUN ID** is the ID of a LUN mapped to the host in the storage system.
4. Run the **show lun general lun_id=***?* command to view the WWN of the LUN mapped to the host.

Step 2 Run the **ls /dev/disk/by-id/ -l** command to view the WWN of the LUN corresponding to the host disk.

Step 3 Check whether the WWN of the LUN mapped to the host and that of the host disk are the same. If they are, the LUN is just the one corresponding to the host disk.

----End

Querying the Mapping Between Host Disks and LUNs (AIX)

Step 1 On the storage system, obtain the WWN of the LUN mapped to the host.

1. Log in to the command-line interface (CLI) of the storage system as a super administrator.
2. Run the **show initiator initiator_type=? [wwn=? | iscsi_iqn_name=?]** command to view the WWN or IQN of an initiator to query information about the corresponding host.

```
admin:/>show initiator initiator_type=FC wwn=21000024ff53b640

WWN              : 21000024ff53b640
Running Status   : Online
Free             : Yes
Alias            : suse2_01
Host ID          : 2
Multipath Type   : Default
```

   The value of **Host ID** is the ID of a host corresponding to the WWN.
3. Run **show host lun host_id=***?* to view all LUNs mapped to the host.

   host_id=*?* represents the ID of a host.

```
admin:/>show host lun host_id=2

 LUN ID  LUN Name
 ------  ------------
 34      lun_0000
 35      lun_0001
 36      lun_0002
```

   The value of **LUN ID** is the ID of a LUN mapped to the host in the storage system.

Step 2 On the host, obtain the ID of the LUN corresponding to a disk.

1. Run the **lsdev -Cc disk** command to query scanned disk information.
2. Run the **lsattr -El hdiskX** command to query the information about disk **hidskx**. In the command output, the value of **lun_id** is the ID of the LUN corresponding to the disk.

Step 3 Check whether the two IDs are the same. If they are the same, you can determine that the LUN is the one corresponding to the host disk.

----End

Querying the Mapping Between Host Disks and LUNs (VMware)

Step 1 On the storage system, obtain the WWN of the LUN mapped to the host.

1. Log in to the command-line interface (CLI) of the storage system as a super administrator.
2. Run **show initiator initiator_type=? [wwn=? | iscsi_iqn_name=?]** to show the host corresponding to the WWN or iSCSI IQN.

```
admin:/>show initiator initiator_type=FC wwn=21000024ff53b640

WWN              : 21000024ff53b640
```



```
Running Status    : Online
Free              : Yes
Alias             : suse2_01
Host ID           : 2
Multipath Type    : Default
```

The value of **Host ID** is the ID of a host corresponding to the WWN.

3. Run **show host lun host_id=***?* to view all LUNs mapped to the host.

   host_id=*?* represents the ID of a host.

```
admin:/>show host lun host_id=2

 LUN ID  LUN Name
 ------  ------------
 34      lun_0000
 35      lun_0001
 36      lun_0002
```

The value of **LUN ID** is the ID of a LUN mapped to the host in the storage system.

4. Run the **show lun general lun_id=***?* command to view the WWN of the LUN mapped to the host.

Step 2 On the host, run the **esxcli storage core device list** command to query the WWN of a LUN corresponding to the disk.

Step 3 Check whether the WWN of the LUN mapped to the host and that of the host disk are the same. If they are, the LUN is just the one corresponding to the host disk.

----End

Querying the Mapping Between Host Disks and LUNs (Solaris)

Step 1 On the storage system, obtain the host ID.

1. Log in to the command-line interface (CLI) of the storage system as a super administrator.
2. Run **show initiator initiator_type=? [wwn=? | iscsi_iqn_name=?]** to show the host corresponding to the WWN or iSCSI IQN.

```
admin:/>show initiator initiator_type=FC wwn=21000024ff53b640

WWN               : 21000024ff53b640
Running Status    : Online
Free              : Yes
Alias             : suse2_01
Host ID           : 2
Multipath Type    : Default
```

The value of **Host ID** is the ID of a host corresponding to the WWN.

Step 2 On the host, obtain the host LUN ID corresponding to a disk.

1. Run the **cfgadm -al** and **devfsadm -C** command to scan the disk.
2. Run the **echo | format** command to update the number of devices and query the host LUN ID.

Step 3 On DeviceManager, view the host LUN ID of the LUN mapped to the host.

1. Log in to DeviceManager.
2. Choose **Hosts** > **Hosts**.
3. Choose the host queried in **Step 2.2**, and view the host LUN ID of the LUN mapped to the host.

Step 4 Check whether the two host LUN IDs are the same. If they are the same, the LUN is the one corresponding to the host disk.

----End

6.3 How Do I Obtain and Import the Email Certificates or Email OTP Certificates?

Question

How do I obtain and import the Email certificates or Email OTP certificates?

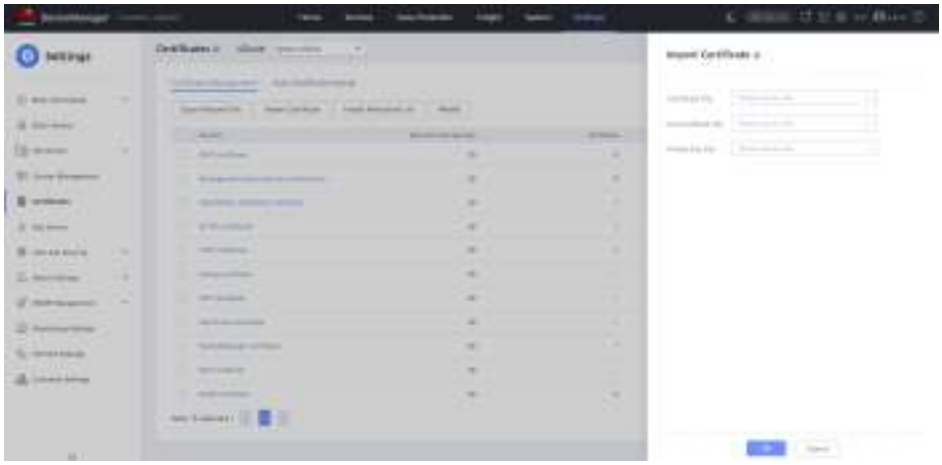
Answer

Step 1 Obtain the client CA certificate and server certificate using either of the following methods:

- Download the client CA certificate from the third-party CA center. After it is signed, export the server certificate.
- Obtain the CA certificates using the certificate management software. The following uses OpenSSL as an example. For details on how to use OpenSSL, refer to its documentation.
  a. Run the **openssl** command to generate the self-signed client CA certificate.
  b. Run the **openssl** command to generate the server certificate using the client CA.

Step 2 Import the self-signed root CA certificate of the client to the storage system.

1. Log in to DeviceManager.
2. Choose **Settings** > **Certificates** > **Certificate Management**.
3. Select **Email OTP certificate** or **Email certificate** and click **Import Certificate**.
4. Import the CA certificate file and click **OK**.

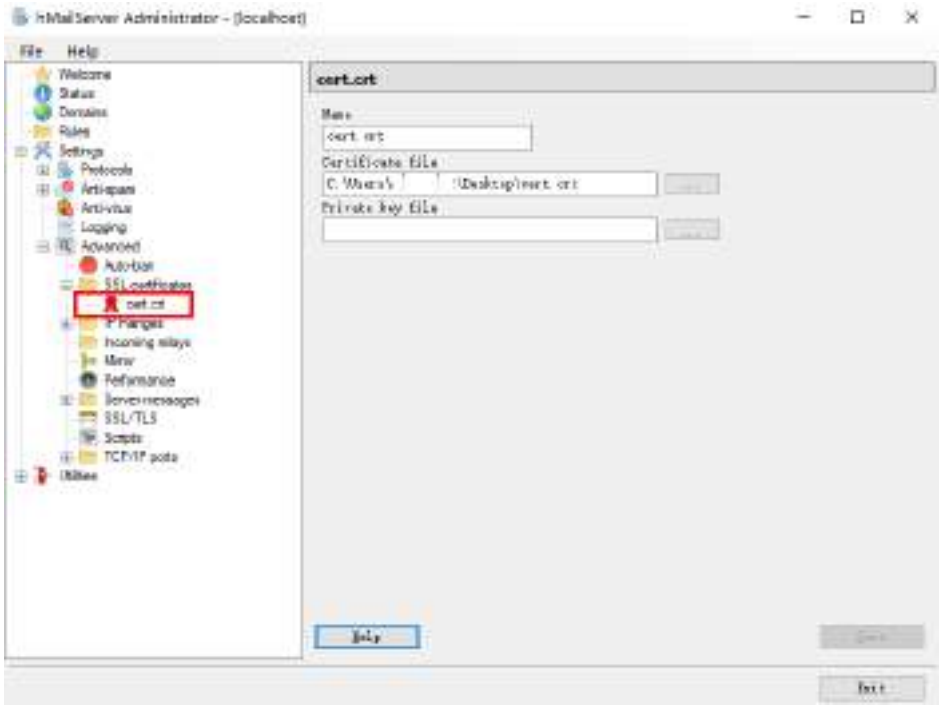


Step 3 Import the server certificate to the SMTP server.

NOTE

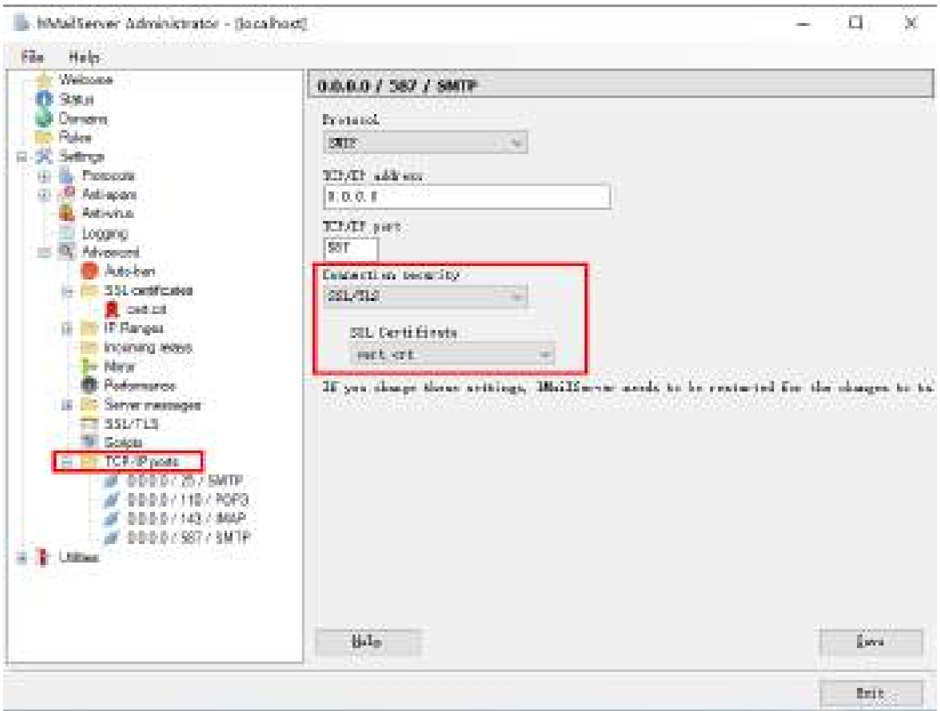
The following uses the hMailServer as an example.

1. Log in to the hMailServer.
2. Choose **Settings** > **Advanced** > **SSL certificates**.
3. Click **Add** and import the certificate.
4. Click **Save**.



5. Choose **Settings** > **Advanced** > **TCP/IP ports**.

6. Select the port of the mail server, set **Connection security** to **SSL/TLS**, and select the imported certificate in **SSL Certificate**.



7. Click **Save**.

----End

6.4 How Do I Update the Public Key When a Linux Host Fails to Remotely Log In to the Storage System's BMC System via SSH Due to the Invalid Public Key?

Question

I try to remotely log in to the BMC system of the storage system to be powered on from a Linux host or another storage system via SSH. The system displays a message indicating that the login fails due to the invalid ESDSA host key. How do I update the public key?

Answer

Step 1 View the file path of saving the public key from the command output.

In this example, the public key is saved in the following path: **/xxx/.ssh/known_hosts**.

```
host:~ # ssh admin@xxx.xxx.xxx.xxx
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
```

```
It is also possible that a host key has just been changed.
The fingerprint for the ECDSA key sent by the remote host is xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx
[MD5].
Please contact your system administrator.
Add correct host key in /xxx/.ssh/known_hosts to get rid of this message.
Offending ECDSA key in /xxx/.ssh/known_hosts:3
ECDSA host key for xxx.xxx.xxx.xxx has changed and you have requested strict checking.
Host key verification failed.
```

Step 2 Edit the **know_hosts** file to delete the IP address and public key of the inaccessible storage system.

NOTE

When you remotely log in to the storage system using SSH next time, a new public key will be generated in the **know_hosts** file.

Step 3 Use SSH to remotely log in to the storage system again.

----End

6.5 How Can I Adjust the Positions of Disk Enclosures in a Cabinet in the Device View of DeviceManager?

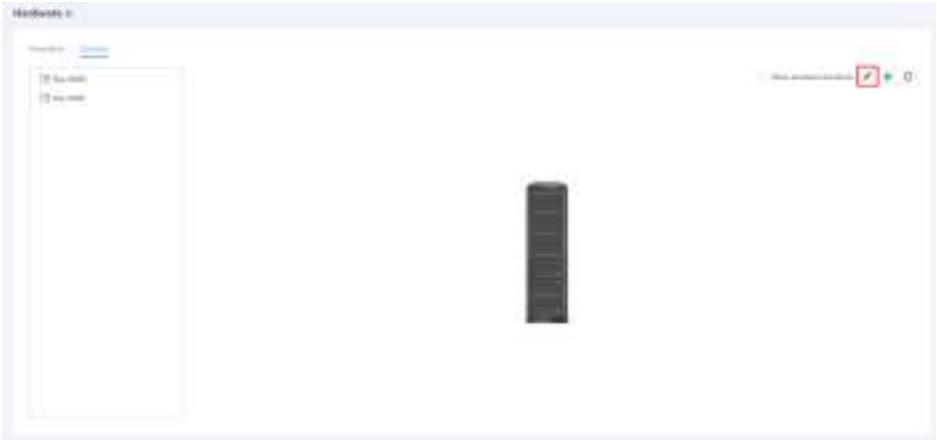
Question

For a 4 U storage system, the device view on DeviceManager displays the positions of disk enclosures in a cabinet. How can I adjust the positions of the disk enclosures on DeviceManager if expansion modules are not installed in the correct positions?

Answer

Step 1 Log in to DeviceManager and choose **System** > **Hardware** > **Devices**.

Step 2 Click  . The **Modify Enclosure** page is displayed.



Step 3 Modify the names of the disk enclosures and select the cabinet and positions of the disk enclosures.

Step 4 Click **OK**. In the displayed dialog box, click **OK**.

Step 5 Click **Close**.

----End

A Permission Matrix for Self-defined Roles

A.1 Permission Matrix for User-defined Roles (Applicable to 6.1.3)

Function Module and Object	Read and Write Permissions	Function Description	Owning Group
base			System group
base[a]	Read-only	To query information about the basic functions	
	Read and write	To manage the basic functions and query their information	
user			System group
ldap	Read-only	To query information about the domain authentication server	
	Read and write	To manage the domain authentication server and query its information	
safe_strategy	Read-only	To query information about security policies	
	Read and write	To manage security policies and query their information	
user[a]	Read-only	To query information about users	
	Read and write	To manage users and query their information	

Function Module and Object	Read and Write Permissions	Function Description	Owning Group
role[a]	Read-only	To query information about roles	
	Read and write	To manage roles and query their information	
security			System group, vStore group
safe_strategy	Read-only	To query information about security policies	
	Read and write	To manage security policies and query their information	
security_rule	Read-only	To query information about security rules	
	Read and write	To manage security rules and query their information	
certificate	Read-only	To query information about certificates	
	Read and write	To manage certificates and query their information	
disk_destroy_data	Read-only	To query information about the disk data destruction policy	
	Read and write	To manage the disk data destruction policy and query its information	
kmc	Read-only	To query information about the KMC	
	Read and write	To manage the KMC and query its information	
ssl_certificate[b]	Read-only	To query information about the digital certificates and private keys of DeviceManager	
	Read and write	To manage digital certificates and private keys of DeviceManager and query their information	
antivirus	Read-only	To query information about the antivirus function	
	Read and write	To manage the antivirus function and query its information	
pool			System group,

Function Module and Object	Read and Write Permissions	Function Description	Owning Group
disk_domain	Read-only	To query information about disk domains	vStore group
	Read and write	To manage disk domains and query their information	
storage_pool	Read-only	To query information about storage pools	
	Read and write	To manage storage pools and query their information	
disk	Read-only	To query information about disks	
	Read and write	To manage disks and query their information	
enclosure	Read-only	To query information about controller enclosures and disk enclosures	
	Read and write	To manage controller enclosures and disk enclosures as well as query their information	
performance			System group
storage_pool	Read-only	To query information about storage pools	
	Read and write	To manage storage pools and query their information	
disk	Read-only	To query information about disks	
	Read and write	To manage disks and query their information	
lun	Read-only	To query information about LUNs	
	Read and write	To manage LUNs and query their information	
lun_group	Read-only	To query information about LUN groups	
	Read and write	To manage LUN groups and query their information	
host_group	Read-only	To query information about host groups	

Function Module and Object	Read and Write Permissions	Function Description	Owning Group
	Read and write	To manage host groups and query their information	
host	Read-only	To query information about hosts	
	Read and write	To manage hosts and query their information	
remote_device	Read-only	To query information about remote devices	
	Read and write	To manage remote devices and query their information	
lun_snapshot	Read-only	To query information about block service snapshots	
	Read and write	To manage block service snapshots and query their information	
remote_replication	Read-only	To query information about remote replications	
	Read and write	To manage remote replications and query their information	
consistency_group	Read-only	To query information about consistency groups	
	Read and write	To manage consistency groups and query their information	
smart_qos	Read-only	To query information about SmartQoS	
	Read and write	To manage SmartQoS and query its information	
performance	Read-only	To query information about performance statistics policies	
	Read and write	To manage performance statistics policies and query their information	
port	Read-only	To query information about ports	
	Read and write	To manage ports and query their information	
controller	Read-only	To query information about controllers	

Function Module and Object	Read and Write Permissions	Function Description	Owning Group
	Read and write	To manage controllers and query their information	
nfs_service	Read-only	To query information about the NFS service	
	Read and write	To manage the NFS service and query its information	
share	Read-only	To query information about shares	
	Read and write	To manage shares and query their information	
file_system	Read-only	To query information about file services	
	Read and write	To manage file services and query their information	
nfsv3	Read-only	To query information about NFSv3	
	Read and write	To manage NFSv3 and query its information	
domain	Read-only	To query information about domain authentication	
	Read and write	To manage domain authentication and query its information	
fs_snapshot	Read-only	To query information about file service snapshots	
	Read and write	To manage file service snapshots and query their information	
cifs_service	Read-only	To query information about the CIFS service	
	Read and write	To manage the CIFS service and query its information	
resource_performance_tuning			System group, vStore group
disk	Read-only	To query information about disks	
	Read and write	To manage disks and query their information	
smart_qos	Read-only	To query information about SmartQoS	

Function Module and Object	Read and Write Permissions	Function Description	Owning Group
	Read and write	To manage SmartQoS and query its information	
smart_migration	Read-only	To query information about LUN migration	
	Read and write	To manage LUN migration and query its information	
enclosure	Read-only	To query information about controller enclosures and disk enclosures	
	Read and write	To manage controller enclosures and disk enclosures as well as query their information	
device			System group
disk	Read-only	To query information about disks	
	Read and write	To manage disks and query their information	
port	Read-only	To query information about ports	
	Read and write	To manage ports and query their information	
controller	Read-only	To query information about controllers	
	Read and write	To manage controllers and query their information	
bbu	Read-only	To query information about BBUs	
	Read and write	To manage BBUs and query their information	
interface_module	Read-only	To query information about interface modules	
	Read and write	To manage interface modules and query their information	
fan	Read-only	To query information about fan modules	
	Read and write	To manage fan modules and query their information	

Function Module and Object	Read and Write Permissions	Function Description	Owning Group
expansion_module	Read-only	To query information about expansion modules	
	Read and write	To manage expansion modules and query their information	
enclosure	Read-only	To query information about controller enclosures and disk enclosures	
	Read and write	To manage controller enclosures and disk enclosures as well as query their information	
power_supply	Read-only	To query information about power modules	
	Read and write	To manage power modules and query their information	
storage_engine	Read-only	To query information about controller enclosures	
	Read and write	To manage controller enclosures and query their information	
cabinet	Read-only	To query information about cabinets	
	Read and write	To manage cabinets and query their information	
bgp	Read-only	To query information about BGP configurations	
	Read and write	To manage BGP configurations and query their information	
bgp_peer	Read-only	To query information about BGP peers	
	Read and write	To manage BGP peers and query their information	
lun			System group, vStore group
lun	Read-only	To query information about LUNs	
	Read and write	To manage LUNs and query their information	
recycle_bin	Read-only	To query information about recycle bins	

Function Module and Object	Read and Write Permissions	Function Description	Owning Group
	Read and write	To manage recycle bins and query their information	
mapping_view			System group, vStore group
initiator	Read-only	To query information about initiators	
	Read and write	To manage initiators and query their information	
target	Read-only	To query information about targets	
	Read and write	To manage targets and query their information	
isns	Read-only	To query the IP address of the iSNS server	
	Read and write	To manage the iSNS server and query its information	
mapping_view	Read-only	To query information about mapping views	
	Read and write	To manage mapping views and query their information	
lun_group	Read-only	To query information about LUN groups	
	Read and write	To manage LUN groups and query their information	
host_group	Read-only	To query information about host groups	
	Read and write	To manage host groups and query their information	
host	Read-only	To query information about hosts	
	Read and write	To manage hosts and query their information	
port_group	Read-only	To query information about port groups	
	Read and write	To manage port groups and query their information	
remote_data_protection			System group,

Function Module and Object	Read and Write Permissions	Function Description	Owning Group
lun_group	Read-only	To query information about LUN groups	vStore group
	Read and write	To manage LUN groups and query their information	
remote_device	Read-only	To query information about remote devices	
	Read and write	To manage remote devices and query their information	
remote_replication	Read-only	To query information about remote replications	
	Read and write	To manage remote replications and query their information	
consistency_group	Read-only	To query information about consistency groups	
	Read and write	To manage consistency groups and query their information	
dr_star	Read-only	To query information about DR Star	
	Read and write	To manage DR Star and query its information	
local_data_protection			System group, vStore group
remote_device	Read-only	To query information about remote devices	
	Read and write	To manage remote devices and query their information	
lun_snapshot	Read-only	To query information about snapshots	
	Read and write	To manage snapshots and query their information	
hyper_cdp	Read-only	To query information about HyperCDP objects	
	Read and write	To manage HyperCDP objects and query their information	
snap_group	Read-only	To query information about snapshot consistency groups	

Function Module and Object	Read and Write Permissions	Function Description	Owning Group
	Read and write	To manage snapshot consistency groups and query their information	
hyper_clone	Read-only	To query information about HyperClone	
	Read and write	To manage HyperClone and query its information	
hyper_clone_group	Read-only	To query information about clone consistency groups	
	Read and write	To manage clone consistency groups and query their information	
lun_consistency_group	Read-only	To query information about LUN consistency groups	
	Read and write	To manage LUN consistency groups and query their information	
hyper_metro			System group, vStore group
remote_device	Read-only	To query information about remote devices	
	Read and write	To manage remote devices and query their information	
hyper_metro_consistency_group	Read-only	To query information about HyperMetro consistency groups	
	Read and write	To manage HyperMetro consistency groups and query their information	
hyper_metro_domain	Read-only	To query information about HyperMetro domains	
	Read and write	To manage HyperMetro domains and query their information	
hyper_metro_pair	Read-only	To query information about HyperMetro pairs	
	Read and write	To manage HyperMetro pairs and query their information	
quorum_server	Read-only	To query information about quorum servers	
	Read and write	To manage quorum servers and query their information	

Function Module and Object	Read and Write Permissions	Function Description	Owning Group
smart_virtualization			System group, vStore group
remote_device	Read-only	To query information about remote devices	
	Read and write	To manage remote devices and query their information	
port	Read-only	To query information about ports	
	Read and write	To manage ports and query their information	
network			System group, vStore group
port	Read-only	To query information about ports	
	Read and write	To manage ports and query their information	
controller	Read-only	To query information about controllers	
	Read and write	To manage controllers and query their information	
interface_module	Read-only	To query information about interface modules	
	Read and write	To manage interface modules and query their information	
dns_zone	Read-only	To query information about the DNS load balancing service	
	Read and write	To manage the DNS load balancing service and query its information	
bgp	Read-only	To query information about BGP configurations	
	Read and write	To manage BGP configurations and query their information	
bgp_peer	Read-only	To query information about BGP peers	
	Read and write	To manage BGP peers and query their information	
alarm			System group

Function Module and Object	Read and Write Permissions	Function Description	Owning Group
alarm	Read-only	To query information about alarm policies	
	Read and write	To manage alarm policies, query their information, and export system logs, configuration information, and diagnosis files	
system			System group, vStore group
dns_server	Read-only	To query information about the DNS server	
	Read and write	To manage the DNS server and query its information	
system	Read-only	To query the system information	
	Read and write	To manage and query the system information	
upgrade	Read-only	To query the upgrade status	
	Read and write	To manage the system upgrade and query the upgrade status	
version	Read-only	To query the system version	
	Read and write	To query the system version	
license	Read-only	To query information about licenses	
	Read and write	To manage licenses and query their information	
logfile	Read-only	To query system logs	
	Read and write	To manage system logs and query their information	
configuration_data	Read-only	To query information about configuration files	
	Read and write	To manage configuration files and query their information	
running_data	Read-only	To query configuration information	
	Read and write	To manage and query configuration information	

Function Module and Object	Read and Write Permissions	Function Description	Owning Group
snmp	Read-only	To query information about SNMP policies	
	Read and write	To manage SNMP policies and query their information	
system_reporter	Read-only	To query performance monitoring parameters	
	Read and write	To manage and query performance monitoring parameters	
smis	Read-only	To query information about the SMIS service	
	Read and write	To manage the SMIS service and query its information	
mirror_domain	Read-only	To query information about mirroring policies	
	Read and write	To manage mirroring policies and query their information	
ssh	Read-only	To query SSH information	
	Read and write	To manage and query SSH information	
call_home	Read-only	To query information about the Call Home service (eService)	
	Read and write	To manage the Call Home service (eService) and query its information	
boot	Read-only	This object has no actual meaning.	
	Read and write	To power off and restart the storage system	
task	Read-only	To query information about the omtask	
	Read and write	To manage the omtask and query its information	
support			System group
support_major	Read-only	To run the major O&M query commands in the developer view, engineer view, and diagnostic view	

Function Module and Object	Read and Write Permissions	Function Description	Owning Group
	Read and write	To run the major O&M management and query commands in the developer view, engineer view, and diagnostic view	
support_minor	Read-only	To run the minor O&M query commands in the developer view, engineer view, and diagnostic view	
	Read and write	To run the minor O&M management and query commands in the developer view, engineer view, and diagnostic view	
user_mode	Read-only	To query information about the CLI views that can be switched over	
	Read and write	To manage the CLI views that can be switched over and query their information	
protect_group			System group, vStore group
protect_group	Read-only	To query information about protection groups	
	Read and write	To manage protection groups and query their information	
file_storage_service			System group, vStore group
nfs_service	Read-only	To query information about the NFS service	
	Read and write	To manage the NFS service and query its information	
share	Read-only	To query information about shares	
	Read and write	To manage shares and query their information	
file_system	Read-only	To query information about file services	
	Read and write	To manage file services and query their information	
domain	Read-only	To query information about domain authentication	

Function Module and Object	Read and Write Permissions	Function Description	Owning Group
	Read and write	To manage domain authentication and query its information	
fs_snapshot	Read-only	To query information about file service snapshots	
	Read and write	To manage file service snapshots and query their information	
dtree	Read-only	To query information about dtree services	
	Read and write	To manage dtree services and query their information	
quota	Read-only	To query information about quota services	
	Read and write	To manage quota services and query their information	
cifs_service	Read-only	To query information about the CIFS service	
	Read and write	To manage the CIFS service and query its information	
global_secure_compliance_clock	Read-only	To query the global security regulation clock information	
	Read and write	To manage and query the global security regulation clock information	
kerberos	Read-only	To query information about Kerberos realm configurations	
	Read and write	To manage Kerberos realm configurations and query their information	
vstore			System group, vStore group
vstore	Read-only	To query information about vStore services	
	Read and write	To manage vStore services and query their information	
container			System group
container_application	Read-only	To query information about container applications	

Function Module and Object	Read and Write Permissions	Function Description	Owning Group
	Read and write	To manage container applications and query their information	
container_service	Read-only	To query information about container services	
	Read and write	To manage container services and query their information	
container_pod	Read-only	To query information about container pods	
	Read and write	To manage container pods and query their information	
container_node	Read-only	To query information about container nodes	
	Read and write	To manage container nodes and query their information	
• a: This object is used only for built-in roles and cannot be configured for a user-defined role. • b: This object is discarded. To manage digital certificates and private keys of DeviceManager and query their information, you can use the certificate.			-

A.2 Permission Matrix for User-defined Roles (Applicable to 6.1.5)

Function Module and Object	Read and Write Permissions	Function Description	Owning Group
base			System group
base[a]	Read-only	To query information about the basic functions	
	Read and write	To manage the basic functions and query their information	
user			System group
ldap	Read-only	To query information about the domain authentication server	

Function Module and Object	Read and Write Permissions	Function Description	Owning Group
	Read and write	To manage the domain authentication server and query its information	
safe_strategy	Read-only	To query information about security policies	
	Read and write	To manage security policies and query their information	
user[a]	Read-only	To query information about users	
	Read and write	To manage users and query their information	
role[a]	Read-only	To query information about roles	
	Read and write	To manage roles and query their information	
security			System group, vStore group
safe_strategy	Read-only	To query information about security policies	
	Read and write	To manage security policies and query their information	
security_rule	Read-only	To query information about security rules	
	Read and write	To manage security rules and query their information	
certificate	Read-only	To query information about certificates	
	Read and write	To manage certificates and query their information	
disk_destroy_data	Read-only	To query information about the disk data destruction policy	
	Read and write	To manage the disk data destruction policy and query its information	
kmc	Read-only	To query information about the KMC	
	Read and write	To manage the KMC and query its information	

Function Module and Object	Read and Write Permissions	Function Description	Owning Group
ssl_certificate[b]	Read-only	To query information about the digital certificates and private keys of DeviceManager	
	Read and write	To manage digital certificates and private keys of DeviceManager and query their information	
antivirus	Read-only	To query information about the antivirus function	
	Read and write	To manage the antivirus function and query its information	
kms	Read-only	To query information about the key management service	
	Read and write	To manage the key management service and query its information	
global_secure_compliance_clock	Read-only	To query information about the file system WORM	
	Read and write	To manage the file system WORM and query its information	
pool			System group, vStore group
disk_domain	Read-only	To query information about disk domains	
	Read and write	To manage disk domains and query their information	
storage_pool	Read-only	To query information about storage pools	
	Read and write	To manage storage pools and query their information	
disk	Read-only	To query information about disks	
	Read and write	To manage disks and query their information	
enclosure	Read-only	To query information about controller enclosures and disk enclosures	
	Read and write	To manage controller enclosures and disk enclosures as well as query their information	

Function Module and Object	Read and Write Permissions	Function Description	Owning Group
performance			System group
storage_pool	Read-only	To query information about storage pools	
	Read and write	To manage storage pools and query their information	
disk	Read-only	To query information about disks	
	Read and write	To manage disks and query their information	
lun	Read-only	To query information about LUNs and clone LUNs	
	Read and write	To manage LUNs and clone LUNs and query their information	
lun_group	Read-only	To query information about LUN groups	
	Read and write	To manage LUN groups and query their information	
host_group	Read-only	To query information about host groups	
	Read and write	To manage host groups and query their information	
host	Read-only	To query information about hosts	
	Read and write	To manage hosts and query their information	
remote_device	Read-only	To query information about remote devices	
	Read and write	To manage remote devices and query their information	
lun_snapshot	Read-only	To query information about block service snapshots	
	Read and write	To manage block service snapshots and query their information	
remote_replication	Read-only	To query information about remote replications	
	Read and write	To manage remote replications and query their information	

Function Module and Object	Read and Write Permissions	Function Description	Owning Group
consistency_group	Read-only	To query information about consistency groups	
	Read and write	To manage consistency groups and query their information	
smart_qos	Read-only	To query information about SmartQoS	
	Read and write	To manage SmartQoS and query its information	
performance	Read-only	To query information about performance statistics policies	
	Read and write	To manage performance statistics policies and query their information	
port	Read-only	To query information about ports	
	Read and write	To manage ports and query their information	
controller	Read-only	To query information about controllers	
	Read and write	To manage controllers and query their information	
nfs_service	Read-only	To query information about the NFS service	
	Read and write	To manage the NFS service and query its information	
share	Read-only	To query information about shares	
	Read and write	To manage shares and query their information	
file_system	Read-only	To query information about file systems and clone file systems	
	Read and write	To manage file systems and clone file systems and query their information	
nfsv3	Read-only	To query information about NFSv3	
	Read and write	To manage NFSv3 and query its information	

Function Module and Object	Read and Write Permissions	Function Description	Owning Group
domain	Read-only	To query information about domain authentication	
	Read and write	To manage domain authentication and query its information	
fs_snapshot	Read-only	To query information about file service snapshots	
	Read and write	To manage file service snapshots and query their information	
cifs_service	Read-only	To query information about the CIFS service	
	Read and write	To manage the CIFS service and query its information	
nas	Read-only	To query information about the NAS service	
	Read and write	To manage the NAS service and query its information	
ndmp_service	Read-only	To query information about the NDMP service	
	Read and write	To manage the NDMP service and query its information	
audit_strategy	Read-only	To query information about audit logs	
	Read and write	To modify audit logs and query their information	
resource_performance_tuning			System group, vStore group
disk	Read-only	To query information about disks	
	Read and write	To manage disks and query their information	
smart_qos	Read-only	To query information about SmartQoS	
	Read and write	To manage SmartQoS and query its information	
smart_migration	Read-only	To query information about LUN migration	

Function Module and Object	Read and Write Permissions	Function Description	Owning Group
	Read and write	To manage LUN migration and query its information	
enclosure	Read-only	To query information about controller enclosures and disk enclosures	
	Read and write	To manage controller enclosures and disk enclosures as well as query their information	
device			System group
disk	Read-only	To query information about disks	
	Read and write	To manage disks and query their information	
port	Read-only	To query information about ports	
	Read and write	To manage ports and query their information	
controller	Read-only	To query information about controllers	
	Read and write	To manage controllers and query their information	
bbu	Read-only	To query information about BBUs	
	Read and write	To manage BBUs and query their information	
interface_ module	Read-only	To query information about interface modules	
	Read and write	To manage interface modules and query their information	
fan	Read-only	To query information about fan modules	
	Read and write	To manage fan modules and query their information	
expansion_ module	Read-only	To query information about expansion modules	
	Read and write	To manage expansion modules and query their information	

Function Module and Object	Read and Write Permissions	Function Description	Owning Group
enclosure	Read-only	To query information about controller enclosures and disk enclosures	
	Read and write	To manage controller enclosures and disk enclosures as well as query their information	
power_supply	Read-only	To query information about power modules	
	Read and write	To manage power modules and query their information	
storage_engine	Read-only	To query information about controller enclosures	
	Read and write	To manage controller enclosures and query their information	
cabinet	Read-only	To query information about cabinets	
	Read and write	To manage cabinets and query their information	
bgp	Read-only	To query information about BGP configurations	
	Read and write	To manage BGP configurations and query their information	
bgp_peer	Read-only	To query information about BGP peers	
	Read and write	To manage BGP peers and query their information	
lun			System group, vStore group
lun	Read-only	To query information about LUNs and clone LUNs	
	Read and write	To manage LUNs and clone LUNs and query their information	
recycle_bin	Read-only	To query information about recycle bin policies and internal objects	
	Read and write	To manage recycle bin policies and internal objects and query their information	

Function Module and Object	Read and Write Permissions	Function Description	Owning Group
workload_type	Read-only	To query information about application type objects	
	Read and write	To manage application type objects and query their information	
mapping_view			System group, vStore group
initiator	Read-only	To query information about initiators	
	Read and write	To manage initiators and query their information	
target	Read-only	To query information about targets	
	Read and write	To manage targets and query their information	
isns	Read-only	To query the IP address of the iSNS server	
	Read and write	To manage the iSNS server and query its information	
mapping_view	Read-only	To query information about mapping views	
	Read and write	To manage mapping views and query their information	
lun_group	Read-only	To query information about LUN groups	
	Read and write	To manage LUN groups and query their information	
host_group	Read-only	To query information about host groups	
	Read and write	To manage host groups and query their information	
host	Read-only	To query information about hosts	
	Read and write	To manage hosts and query their information	
port_group	Read-only	To query information about port groups	
	Read and write	To manage port groups and query their information	

Function Module and Object	Read and Write Permissions	Function Description	Owning Group
remote_data_protection			System group, vStore group
lun_group	Read-only	To query information about LUN groups	
	Read and write	To manage LUN groups and query their information	
remote_device	Read-only	To query information about remote devices	
	Read and write	To manage remote devices and query their information	
remote_replication	Read-only	To query information about remote replications	
	Read and write	To manage remote replications and query their information	
consistency_group	Read-only	To query information about consistency groups	
	Read and write	To manage consistency groups and query their information	
dr_star	Read-only	To query information about DR Star	
	Read and write	To manage DR Star and query its information	
local_data_protection			System group, vStore group
remote_device	Read-only	To query information about remote devices	
	Read and write	To manage remote devices and query their information	
lun_snapshot	Read-only	To query information about snapshots	
	Read and write	To manage snapshots and query their information	
hyper_cdp	Read-only	To query information about HyperCDP objects	
	Read and write	To manage HyperCDP objects and query their information	
snap_group	Read-only	To query information about snapshot consistency groups	

Function Module and Object	Read and Write Permissions	Function Description	Owning Group
	Read and write	To manage snapshot consistency groups and query their information	
hyper_clone	Read-only	To query information about HyperClone	
	Read and write	To manage HyperClone and query its information	
hyper_clone_group	Read-only	To query information about clone consistency groups	
	Read and write	To manage clone consistency groups and query their information	
lun_consistency_group	Read-only	To query information about LUN consistency groups	
	Read and write	To manage LUN consistency groups and query their information	
hyper_metro			System group, vStore group
remote_device	Read-only	To query information about remote devices	
	Read and write	To manage remote devices and query their information	
hyper_metro_consistency_group	Read-only	To query information about HyperMetro consistency groups	
	Read and write	To manage HyperMetro consistency groups and query their information	
hyper_metro_domain	Read-only	To query information about HyperMetro domains	
	Read and write	To manage HyperMetro domains and query their information	
hyper_metro_pair	Read-only	To query information about HyperMetro pairs	
	Read and write	To manage HyperMetro pairs and query their information	
quorum_server	Read-only	To query information about quorum servers	
	Read and write	To manage quorum servers and query their information	

Function Module and Object	Read and Write Permissions	Function Description	Owning Group
smart_virtualization			System group, vStore group
remote_device	Read-only	To query information about remote devices	
	Read and write	To manage remote devices and query their information	
port	Read-only	To query information about ports	
	Read and write	To manage ports and query their information	
network			System group, vStore group
port	Read-only	To query information about ports	
	Read and write	To manage ports and query their information	
controller	Read-only	To query information about controllers	
	Read and write	To manage controllers and query their information	
interface_module	Read-only	To query information about interface modules	
	Read and write	To manage interface modules and query their information	
dns_zone	Read-only	To query information about the DNS load balancing service	
	Read and write	To manage the DNS load balancing service and query its information	
bgp	Read-only	To query information about BGP configurations	
	Read and write	To manage BGP configurations and query their information	
bgp_peer	Read-only	To query information about BGP peers	
	Read and write	To manage BGP peers and query their information	
alarm			System group

Function Module and Object	Read and Write Permissions	Function Description	Owning Group
alarm	Read-only	To query information about alarm policies	
	Read and write	To manage alarm policies, query their information, and export system logs, configuration information, and diagnosis files	
system			System group, vStore group
dns_server	Read-only	To query information about the DNS server	
	Read and write	To manage the DNS server and query its information	
system	Read-only	To query the system information	
	Read and write	To manage and query the system information	
upgrade	Read-only	To query the upgrade status	
	Read and write	To manage the system upgrade and query the upgrade status	
version	Read-only	To query the system version	
	Read and write	To query the system version	
license	Read-only	To query information about licenses	
	Read and write	To manage licenses and query their information	
logfile	Read-only	To query system logs	
	Read and write	To manage system logs and query their information	
configuration_data	Read-only	To query information about configuration files	
	Read and write	To manage configuration files and query their information	
running_data	Read-only	To query configuration information	
	Read and write	To manage and query configuration information	

Function Module and Object	Read and Write Permissions	Function Description	Owning Group
snmp	Read-only	To query information about SNMP policies	
	Read and write	To manage SNMP policies and query their information	
system_reporter	Read-only	To query performance monitoring parameters	
	Read and write	To manage and query performance monitoring parameters	
smis	Read-only	To query information about the SMIS service	
	Read and write	To manage the SMIS service and query its information	
mirror_domain	Read-only	To query information about mirroring policies	
	Read and write	To manage mirroring policies and query their information	
ssh	Read-only	To query SSH information	
	Read and write	To manage and query SSH information	
call_home	Read-only	To query information about the Call Home service (eService)	
	Read and write	To manage the Call Home service (eService) and query its information	
boot	Read-only	This object has no actual meaning.	
	Read and write	To power off and restart the storage system	
task	Read-only	To query information about the omtask	
	Read and write	To manage the omtask and query its information	
batch_configuration	Read-only	To download the batch configuration template	
	Read and write	To manage the batch configuration function and query its information	

Function Module and Object	Read and Write Permissions	Function Description	Owning Group
ping	Read-only	To query information about the storage connectivity	
	Read and write	To manage the storage connectivity and query its information	
support			System group
support_major	Read-only	To run the major O&M query commands in the developer view, engineer view, and diagnostic view	
	Read and write	To run the major O&M management and query commands in the developer view, engineer view, and diagnostic view	
support_minor	Read-only	To run the minor O&M query commands in the developer view, engineer view, and diagnostic view	
	Read and write	To run the minor O&M management and query commands in the developer view, engineer view, and diagnostic view	
user_mode	Read-only	To query information about the CLI views that can be switched over	
	Read and write	To manage the CLI views that can be switched over and query their information	
protect_group			System group, vStore group
protect_group	Read-only	To query information about protection groups	
	Read and write	To manage protection groups and query their information	
file_storage_service			System group, vStore group
nfs_service	Read-only	To query information about the NFS service	
	Read and write	To manage the NFS service and query its information	
share	Read-only	To query information about shares	

Function Module and Object	Read and Write Permissions	Function Description	Owning Group
	Read and write	To manage shares and query their information	
file_system	Read-only	To query information about file systems and clone file systems	
	Read and write	To manage file systems and clone file systems and query their information	
domain	Read-only	To query information about domain authentication	
	Read and write	To manage domain authentication and query its information	
fs_snapshot	Read-only	To query information about file service snapshots	
	Read and write	To manage file service snapshots and query their information	
dtree	Read-only	To query information about dtree services	
	Read and write	To manage dtree services and query their information	
quota	Read-only	To query information about quota services	
	Read and write	To manage quota services and query their information	
cifs_service	Read-only	To query information about the CIFS service	
	Read and write	To manage the CIFS service and query its information	
kerberos	Read-only	To query information about Kerberos realm configurations	
	Read and write	To manage Kerberos realm configurations and query their information	
worm_fingerprint	Read-only	To query information about file signatures	
	Read and write	To manage file signatures and query their information	

Function Module and Object	Read and Write Permissions	Function Description	Owning Group
worm_legal_hold	Read-only	To query information about litigation hold files	
	Read and write	To manage litigation hold files and query their information	
protocol	Read-only	To query information about the protocol status	
	Read and write	To manage the protocol status and query its information	
ndmp_service	Read-only	To query information about the NDMP service	
	Read and write	To manage the NDMP service and query its information	
workload_type	Read-only	To query information about application type objects	
	Read and write	To manage application type objects and query their information	
audit_strategy	Read-only	To query information about audit logs	
	Read and write	To modify audit logs and query their information	
vstore			System group, vStore group
vstore	Read-only	To query information about vStore services	
	Read and write	To manage vStore services and query their information	
container			System group
container_application	Read-only	To query information about container applications	
	Read and write	To manage container applications and query their information	
container_service	Read-only	To query information about container services	
	Read and write	To manage container services and query their information	

Function Module and Object	Read and Write Permissions	Function Description	Owning Group
container_pod	Read-only	To query information about container pods	
	Read and write	To manage container pods and query their information	
container_node	Read-only	To query information about container nodes	
	Read and write	To manage container nodes and query their information	
anti_ransomware			System group
anti_ransomware	Read-only	To query information about ransomware protection	
	Read and write	To manage ransomware protection and query its information	
s3_secret_key			System group
s3_secret_key	Read-only	To query information about S3 keys	
	Read and write	To manage S3 keys and query their information	
• a: This object is used only for built-in roles and cannot be configured for a user-defined role. • b: This object is discarded. To manage digital certificates and private keys of DeviceManager and query their information, you can use the certificate.			-

B How to Obtain Help

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

B.1 Preparations for Contacting Huawei

To better resolve the fault, you are advised to collect troubleshooting information and make debugging preparations before contacting Huawei.

B.1.1 Collecting Troubleshooting Information

You need to collect troubleshooting information before troubleshooting.

You need to collect the following information:

- Name and address of the customer
- Contact person and telephone number
- Time when the fault occurred
- Description of the fault phenomena
- Device type and software version
- Measures taken after the fault occurs and the related results
- Troubleshooting level and required solution deadline

B.1.2 Making Debugging Preparations

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

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

B.2 How to Use the Document

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

To better solve the problems, use the documents before you contact Huawei for technical support.

B.3 How to Obtain Help from Website

Huawei provides users with timely and efficient technical support through the regional offices, secondary technical support system, telephone technical support, remote technical support, and onsite technical support.

Contents of the Huawei technical support system are as follows:

- Huawei headquarters technical support department
- Regional office technical support center
- Customer service center
- Technical support website: **https://support.huawei.com/enterprise/**

You can query how to contact the regional offices at **https://support.huawei.com/enterprise/**.

B.4 Ways to Contact Huawei

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

Huawei Technologies Co., Ltd.

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

Website: **https://e.huawei.com/**

C 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) on the network. Application programs of data services run on the application server.

Asynchronous remote replication
A kind of remote replication. When the data at the primary site is updated, the data does not need to be updated synchronously at the mirroring site to finish the update. In this way, performance is not reduced due to data mirroring.

Air baffle
It optimizes the ventilation channels and improves the heat dissipation capability of the system.

Audit log guarantee mode
A mode for recording audit logs. This mode preferentially ensures that the audit log function is normal and no audit log is missing.

Audit log non-guarantee mode
A mode for recording audit logs. In this mode, services are running properly. Audit logs may be missing.

B

Backup
A collection of data stored on (usually removable) non-volatile storage media for purposes of recovery in case the original copy of data is lost or becomes inaccessible; also called a backup copy. To be useful for recovery, a backup must be made by copying the source data image when it is in a consistent state. The act of creating a backup.

Backup window	An interval of time during which a set of data can be backed up without seriously affecting applications that use the data.
Bandwidth	The numerical difference between the upper and lower frequencies of a band of electromagnetic radiation. A deprecated synonym for data transfer capacity that is often incorrectly used to refer to throughput.
Baud rate	The maximum rate of signal state changes per second on a communications circuit. If each signal state change corresponds to a code bit, then the baud rate and the bit rate are the same. It is also possible for signal state changes to correspond to more than one code bit, so the baud rate may be lower than the code 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	The probability that a transmitted bit will be erroneously received. The bit error rate (BER) is measured by counting the number of bits in error at the output of a receiver and dividing by the total number of bits in the transmission. BER is typically expressed as a negative power of 10.
Bonding	Bonding of multiple independent physical network ports into a logical port, which ensures the high availability of server network connections and improves network performance.
Boundary scan	A test methodology that uses shift registers in the output connections of integrated circuits (ICs). One IC is often connected to the next IC. 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 known as Joint Test Action Group (JTAG).
Browser/Server	Architecture that defines the roles of the browser and server. The browser is the service request party and the server is the service provider.
Built-in FRU Alarm indicator	It indicates errors on the built-in FRUs of a controller, such as errors on fans or memory modules.

C

Cache hit ratio	The ratio of the number of cache hits to the number of all I/Os during a read task, usually expressed as a percentage.
Captive screw	Specially designed to lock into place on a parent board or motherboard, allowing for easy installation and removal of attached pieces without release of the screw.
Challenge Handshake Authentication Protocol	A password-based authentication protocol that uses a challenge to verify that a user has access rights to a system. A hash of the supplied password with the challenge is sent for comparison so the cleartext password is never sent over the connection.
Compliance mode	A protection mode of WORM. In compliance mode, files within their protection period cannot be changed or deleted by either the file user or by the system administrator. Files with expired protection periods can be deleted but not changed by the file user or the system administrator.
Controller	The control logic in a disk or tape that performs command decoding and execution, host data transfer, serialization and deserialization of data, error detection and correction, and overall management of device operations. The control logic in a storage subsystem that performs command transformation and routing, aggregation (RAID, mirroring, striping, or other), high-level error recovery, and performance optimization for multiple storage devices.
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.
Copying	A pair state. The state indicates that the source LUN data is being synchronized to the target LUN.
Container root directory	Space used to store the metadata for running container images and container instances.
Container image	An image is a special file system, which provides the programs, libraries, resources, and configuration files required for running containers. It also contains configuration parameters, for example, for anonymous disks, environment variables, and users. The image does not contain dynamic data, and its content will not be modified after construction.
Containerized application	An image can start multiple containers, and an application can contain one or a group of containers.

Container node	Controller that runs the container service.
Configuration item list	A series of modifiable configuration items defined in the Helm chart of the container.
Container service	Containerized application management service, which manages the lifecycle of containerized applications.

D

Data compression	The process of encoding data to reduce its size. Lossy compression (i.e., compression using a technique in which a portion of the original information is lost) is acceptable for some forms of data (e.g., digital images) in some applications, but for most IT applications, lossless compression (i.e., compression using a technique that preserves the entire content of the original data, and from which the original data can be reconstructed exactly) is required.
Data flow	A process that involves processing data extracted from the source system. These processes include: 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	A movement of data or information between information systems, formats, or media. Migration is performed for reasons such as possible decay of storage media, obsolete hardware or software (including obsolete data formats), changing performance requirements, the need for cost efficiencies etc.
Data source	A system, database (database user; database instance), or file that can make BOs persistent.
Dirty data	Data that is stored temporarily on the cache and has not been written onto disks.
Disaster recovery	The recovery of data, access to data and associated processing through a comprehensive process of setting up a redundant site (equipment and work space) with recovery of operational data to continue business operations after a loss of use of all or part of a data center. This involves not only an essential set of data but also an essential set of all the hardware and software to continue processing of that data and business. Any disaster recovery may involve some amount of down time.

Disk array	A set of disks from one or more commonly accessible disk subsystems, combined with a body of control software. The control software presents the disks' storage capacity to hosts as one or more virtual disks. Control software is often called firmware or microcode when it runs in a disk controller. Control software that runs in a host computer is usually called a volume manager.
Disk domain	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 enclosure	Consists of the following parts in redundancy: expansion module, disk, power module, and fan module. System capacity can be expanded by cascading multiple disk enclosures.
Disk location	The process of locating a disk in the storage system by determining the enclosure ID and slot ID of the disk.
Disk utilization	The percentage of used capacity in the total available capacity.

E

eDevLUN	Logical storage array space created by a third-party storage array.
Expansion module	A component used for expansion.
Expansion	Connects a storage system to more disk enclosures through connection cables, expanding the capacity of the storage system.

F

Field replaceable unit	A unit or component of a system that is designed to be replaced in the field, i.e., without returning the system to a factory or repair depot. Field replaceable units may either be customer-replaceable or their replacement may require trained service personnel.
Firmware	Low-level software for booting and operating an intelligent device. Firmware generally resides in read-only memory (ROM) on the device.

Flash Translation Layer	Flash Translation Layer (FTL) organizes and manages host data, enables host data to be allocated to NAND flash chips of SSDs in an orderly manner, maintains the mapping relationship between logical block addresses (LBAs) and physical block addresses (PBAs), and implements garbage collection, wear leveling, and bad block management.
Front-end port	The port that connects the controller enclosure to the service side and transfers service data. Front-end port types are Fibre Channel and iSCSI.
Front-end interconnect I/O module (FIM)	On a storage device, all controllers share the front-end interface modules.

G

Garbage collection	The process of reclaiming resources that are no longer in use. Garbage collection has uses in many aspects of computing and storage. For example, in flash storage, background garbage collection can improve write performance by reducing the need to perform whole block erasures prior to a write.
Gateway	A device that receives data via one protocol and transmits it via another.
Global garbage collection	With a view to defragmentation of storage arrays and garbage collection of disks, global garbage collection reduces garbage of disks by enabling storage arrays to inform disks of not implementing invalid data relocation and of controlling space release so that disks and controllers consume less space, reducing costs and prolonging the useful life of storage arrays.
Global system for mobile communications	The second-generation mobile networking standard defined by the European Telecommunications Standards Institute (ETSI). It is aimed at designing a standard for global mobile phone networks. GSM consists of three main parts: mobile switching subsystem (MSS), base station subsystem (BSS), and mobile station (MS).
Global wear leveling	With a view to individual characteristics of a single disk, global wear leveling uses space allocation and write algorithms to achieve wear leveling among disks, preventing a disk from losing efficacy due to excessive writes and prolonging the useful life of the disk.

H

Hard disk tray	The tray that bears the hard disk.
Heartbeat	Heartbeat supports node communication, fault diagnosis, and event triggering. Heartbeats are protocols that require no acknowledgement. They are transmitted between two devices. The device can judge the validity status of the peer device.
Hit ratio	The ratio of directly accessed I/Os from the cache to all I/Os.
Hot swap	The substitution of a replacement unit (RU) in a system for a defective unit, where the substitution can be performed while the system is performing its normal functioning normally. Hot swaps are physical operations typically performed by humans.
HyperMetro	A value-added service of storage systems. HyperMetro means 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 generally; made up of two storage arrays and one quorum server. HyperMetro services can be created on a HyperMetro domain.
HyperMetro vStore pair	A HyperMetro vStore pair consists of two vStores, that is, two tenants. After a HyperMetro relationship is set up for a pair of vStores, the datasets in the two vStores work in redundancy mode and provide storage services in one dataset view, achieving hitless service failover.
HyperMetro-Inner	On an eight-controller network, with HyperMetro-Inner, continuous mirroring, back-end global sharing, and three-copy technologies, a storage system can tolerate one-by-one failures of seven controllers among eight controllers, concurrent failures of two controllers, and failure of a controller enclosure.
HyperDetect	HyperDetect is a feature that provides ransomware detection.
Handle	A handle resides on the structural part of a module. It is used to insert or remove a module into or from a chassis, not helpful in saving efforts.
Helm chart	A Helm chart is in TAR format. It is similar to the deb package of APT or the rpm package of Yum. It contains a group of yaml files that define Kubernetes resources.

I

In-band management	The management control information of the network and the carrier service information of the user network are transferred through the same logical channel. In-band management enables users to manage storage arrays through commands. Management commands are sent through service channels, such as I/O write and read channels. The advantages of in-band management include high speed, stable transfer, and no additional management network ports required.
Initiator	The system component that originates an I/O command over an I/O interconnect. The endpoint that originates a SCSI I/O command sequence. I/O adapters, network interface cards, and intelligent I/O interconnect control ASICs are typical initiators.
I/O	Shorthand for input/output. I/O is the process of moving data between a computer system's main memory and an external device or interface such as a storage device, display, printer, or network connected to other computer systems. This encompasses reading, or moving data into a computer system's memory, and writing, or moving data from a computer system's memory to another location.
Intelligent ransomware detection	The system detects known ransomware features to identify whether the file systems are attacked by ransomware. If no ransomware attack is identified, the system analyzes and compares the changes in file system snapshots, and uses machine learning algorithms to further check whether the file systems are infected by ransomware.
Interface module	A replaceable field 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/Os or computing requests to physical resources of the system.
Logical unit	The addressable entity within a SCSI target that executes I/O commands.
Logical unit number	The SCSI identifier of a logical unit within a target. Industry shorthand, when phrased as "LUN", for the logical unit indicated by the logical unit number.

LUN formatting	The process of writing 0 bits in the data area of the logical drive and generating related parity bits so that the logical drive can be in the ready state.
LUN mapping	A storage system maps LUNs to application servers so that application servers can access storage resources.
LUN migration	A method for the LUN data to migrate between different physical storage spaces while ensuring data integrity and uninterrupted operation of host services.
LUN snapshot	A type of snapshot created for a LUN. This snapshot is both readable and writable and is mainly used to provide a snapshot LUN from point-in-time LUN data.
Lever	A lever resides on the structural part of a module. It is used to insert or remove a module into or from a chassis, saving efforts.
Local image repository	A private repository used to store the container images and Helm charts imported by users. It is different from the standard image repository. The imported images and Helm charts must meet the compatibility requirements of the system.

M

Maintenance terminal	A computer connected through a serial port or management network port. It maintains the storage system.
Management interface module	The module that integrates one or more management network ports.
Management network	An entity that provides means to transmit and process network management information.
Management network port	The network port on the controller enclosure connected to the maintenance terminal. It is provided for the remote maintenance terminal. Its IP address can be modified with the change of the customer's environment.

N

NVM Express	A host controller interface with a register interface and command set designed for PCI Express-based SSDs.

NVMe SSD	A solid state disk (SSD) with a non-volatile memory express (NVMe) interface. Compared with other SSDs, such SSDs can deliver higher performance and shorter latency.

O

Out-of-band management	A management mode used during out-of-band networking. The management and control information of the network and the bearer service information of the user network are transmitted through different logical channels.

P

Power failure protection	When an external power failure occurs, the AC PEM depends on the battery for power supply. This ensures the integrity of the dirty data in the cache.
Pre-copy	When the system monitors a failing member disk in a RAID group, the system copies the data from the disk to a hot spare disk in advance.
Palm-sized NVMe SSD	A palm-sized NVMe SSD is a type of NVMe SSD of which the dimensions (H x W x D) are 160 mm x 79.8 mm x 9.5 mm (neither 3.5-inch nor 2.5-inch).

Q

Quorum server	A server that can provide arbitration services for clusters or HyperMetro to prevent the resource access conflicts of 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 redundancy 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.

Ransomware file interception	When launching attacks, ransomware usually generates encrypted files with special file name extensions. In light of this, the system intercepts the write to files with specific file name extensions to block the extortion from known ransomware and protect file systems in the storage system.
Real-time ransomware detection	Ransomware has similar I/O behavior characteristics. By analyzing file I/O behavior characteristics, the system quickly filters out abnormal files and performs deep content analysis on the abnormal files to detect files attacked by ransomware. Then, secure snapshots are created for file systems where files have been attacked, and alarms are reported to notify the data protection administrator, limiting the impact of ransomware and reducing losses.
Reconstruction	The regeneration and writing onto one or more replacement disks of all of the user data and check data from a failed disk in a mirrored or RAID array. In most arrays, a rebuild can occur while applications are accessing data on the array's virtual disks.
Redundancy	The inclusion of extra components of a given type in a system (beyond those required by the system to carry out its function) for the purpose of enabling continued operation in the event of a component failure.
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 mirrors 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.
Reverse synchronization	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. On a TCP/IP network, each IP packet is routed independently. Routes can change dynamically.

S

Script	A parameterized list of primitive I/O interconnect operations intended to be executed in sequence. Often used with respect to ports, most of which are able to execute scripts of I/O commands autonomously (without policy processor assistance). A sequence of instructions intended to be parsed and carried out by a command line interpreter or other scripting language. Perl, VBScript, JavaScript and Tcl are all scripting languages.
Serial port	An input/output location (channel) that sends and receives data (one bit at a time) to and from the CPU of a computer or a communications device. Serial ports are used for serial data communication and as interfaces for some peripheral devices, such as mouse devices 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.
Simple network management protocol	An IETF protocol for monitoring and managing systems and devices in a network. The data being monitored and managed is defined by an MIB. The functions supported by the protocol are the request and retrieval of data, the setting or writing of data, and traps that signal the occurrence of events.
Single point of failure	One component or path in a system, the failure of which would make the system inoperable.
Slot	A position defined by an upper guide rail and the corresponding lower guide rail in a frame. A slot houses a board.
Small computer system interface	A collection of ANSI standards and proposed standards that define I/O interconnects primarily intended for connecting storage subsystems or devices to hosts through host bus adapters. Originally intended primarily for use with small (desktop and desk-side workstation) computers, SCSI has been extended to serve most computing needs, and is arguably the most widely implemented I/O interconnect in use today.
Snapshot	A point in time copy of a defined collection of data. Clones and snapshots are full copies. Depending on the system, snapshots may be of files, LUNs, file systems, or any other type of container supported by the system.
Snapshot copy	A copy of a snapshot LUN.

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 system	An integrated system that 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 to the actual storage media used to back up data.
Streaming media	Streaming media is media continuously streamed over the network. Combining technologies concerning streaming media data collection, compression, encoding, storage, transmission, playback, and network communications, streaming media can provide high-quality playback effects in real time at low bandwidth.
Subnet	A type of smaller network that forms a larger network according to a rule, such as, forming a network according to different districts. This facilitates the management of a large network.
Smart disk enclosure	Being compared with traditional disk enclosures, the smart disk enclosures are equipped with Arm chips and DDR memories or other computing modules to achieve powerful computing capabilities. With such capabilities, the smart disk enclosures can help controllers to share some computing loads, accelerating data processing.
Share authentication	During vStore configuration synchronization, the share authentication information (including the share information and domain controller configuration) is synchronized to the secondary end.

T

Target	The endpoint that receives a SCSI I/O command sequence.
Target LUN	The LUN on which target data resides.
Thin LUN	A logic disk that can be accessed by hosts. It dynamically allocates storage resources from the thin pool according to the actual capacity requirements of users.

Topology	The logical layout of the components of a computer system or network and their interconnections. Topology deals with questions of what components are directly connected to other components from the standpoint of being able to communicate. It does not deal with questions of physical location of components or interconnecting cables. The communication infrastructure that provides Fibre Channel communication among a set of PN_Ports (e.g., a Fabric, an Arbitrated Loop, or a combination of the two).
Trim	A method by which the host operating system may inform a storage device of data blocks that are no longer in use and can be reclaimed. Many storage protocols support this functionality via various names, e.g., ATA TRIM and SCSI UNMAP.

U

User interface	The space where users interact with a machine.
U-shaped bracket	It is an optional structural part like letter "U". It is located between the mounting ear of a chassis and the mounting bar of a cabinet or bay and is used to adjust the locations of the chassis and mounting bar of the cabinet or bay.

W

Wear leveling	A set of algorithms utilized by a flash controller to distribute writes and erases across the cells in a flash device. Cells in flash devices have a limited ability to survive write cycles. The purpose of wear leveling is to delay cell wear out and prolong the useful life of the overall flash device.
Write amplification	Increase in the number of write operations by the device beyond the number of write operations requested by hosts.
Write amplification factor	The ratio of the number of write operations on the device to the number of write operations requested by the host.

Write back	A caching technology in which the completion of a write request is signaled as soon as the data is in the cache. Actual writing to non-volatile media occurs at a later time. Write back includes inherent risks: an application will take 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 these reasons, sufficient write back implementations include mechanisms to preserve cache contents across system failures (including power failures) and a flushed cache at system restart time.
Write Once Read Many	A type of storage, designed for fixed content, that preserves what is written to it in an immutable fashion. Optical disks are an example of WORM storage.
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 equipped with the write through technology is approximately that of a non-cached system. However, if the written data is also held in a cache, subsequent read performance may be dramatically improved.

Z

Zone	A collection of Fibre Channel N_Ports and/or NL_Ports (i.e., device ports) that are permitted to communicate with each other via the fabric. Any two N_Ports and/or NL_Ports that are not members of at least one common zone are not permitted to communicate via the fabric. Zone membership may be specified by: 1) port location on a switch, (i.e., Domain_ID and port number); or, 2) the device's N_Port_Name; or, 3) the device's address identifier; or, 4) the device's Node_Name. Well-known addresses are implicitly included in every zone.

D Acronyms and Abbreviations

B	
BBU	Backup Battery Unit
C	
CLI	Command Line Interface
E	
ESN	Equipment Serial Number
F	
FC	Fibre Channel
FRU	Field Replaceable Unit
FTP	File Transfer Protocol
G	
GUI	Graphical User Interface
H	
HBA	Host Bus Adapter
I	
I/O	Input/Output
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
iSCSI	Internet Small Computer Systems Interface

ISO	International Organization for Standardization
L	
LDAP	Lightweight Directory Access Protocol
LUN	Logical Unit Number
N	
NTP	Network Time Protocol
S	
SAS	Serial Attached SCSI
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
T	
TCP/IP	Transmission Control Protocol/Internet Protocol
U	
UDP	User Datagram Protocol
UTC	Coordinated Universal Time

OceanStor
6.1.x

Basic Storage Service Configuration Guide for Block

Issue	03
Date	2022-08-25

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: https://e.huawei.com

About This Document

Purpose

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

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

Product Model	Product Version
OceanStor 5310	6.1.3 6.1.5
OceanStor 5510	
OceanStor 5610	
OceanStor 6810	
OceanStor 18510	
OceanStor 18810	

NOTICE

This document is updated periodically with the software version. The operations described in this document use the latest version as an example. Note that the supported functions and features vary according to the software version. The content in this document is for reference only.

Intended Audience

This document is intended for:

- Technical support engineers
- Maintenance engineers

Symbol Conventions

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

Symbol	Description
DANGER	Indicates a hazard with a high level of risk which, if not avoided, will result in death or serious injury.
WARNING	Indicates a hazard with a medium level of risk which, if not avoided, could result in death or serious injury.
CAUTION	Indicates a hazard with a low level of risk which, if not avoided, could result in minor or moderate injury.
NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
NOTE	Supplements the important information in the main text. 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 03 (2022-08-25)

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

Optimized descriptions about some operations.

Issue 02 (2022-04-15)

This issue is the second official release.

Added section "In-band Management".

Issue 01 (2022-01-25)

This issue is the first official release.

Contents

1 Introduction

This chapter describes the organization of this guide, lists related documentation, and provides tips for use.

Organization of This Guide

This guide describes how to configure and manage basic storage services using the graphical user interface (GUI). It is assumed that you are already familiar with basics of storage systems and networks.

The guide is organized into the following major parts:

- Basic storage service overview

  Describes basic concepts, working principles, and application scenarios of storage systems.
- Planning basic storage services

  Describes how to plan storage pools, LUNs, and users.
- Configuring basic storage services

  Describes how to configure storage resources, including storage pools, LUNs, and LUN groups, and how to create mappings so that hosts can use the storage space provided by storage systems.
- Managing basic storage services

  Describes how to manage storage resources, including storage pools, LUNs, and LUN groups.

Related Documentation

Refer to the following documents when performing certain basic configurations and subsequent operations:

- Product description

  Refer to the product description specific to your product if you want to understand the market positioning, basic functions, and specifications of the product.
- Installation guide

  Refer to the guide specific to your product when initializing a storage system.

- Administrator guide

  Refer to the guide specific to your product when planning user roles and permissions.
- Host connectivity guide

  Refer to the guide specific to your product for details on how to configure host connectivity.
- Command reference

  Refer to the guide specific to your product if you want to configure storage services using the command-line interface (CLI).

Tips

GUIs may vary with product versions and models. The actual GUIs prevail.

2 Basic Storage Service Overview

This chapter describes basic concepts, basic storage principles, and application scenarios of storage systems.

2.1 Basic Storage Principles

Storage system uses the RAID 2.0+ and dynamic RAID technologies to achieve dynamic allocation and expansion of storage resources in storage pools.

2.1.1 Basic Concepts

- RAID: A storage virtualization technology which stores and replicates data in a disk group (logical disk) consisting of multiple physical disks. The disk group provides higher storage performance than a single disk and supports data redundancy. Different RAID levels are available.
- RAID 2.0+ block virtualization: A new type of RAID technology. Block virtualization divides disks into multiple chunks (CKs) of a fixed size and organizes them into multiple chunk groups (CKGs). When a disk fails, the disks of the CKG where the CKs in the faulty disk reside also participate in reconstruction. This significantly increases the number of disks involved in the reconstruction, improving the data reconstruction speed.
- Chunk (CK): Disks are divided into blocks with a fixed size (typically 4 MB). Each block is assigned a number and constitutes a CK. A CK is the smallest unit of a RAID group.
- Chunk group (CKG): A logical collection of *N*+*M* CKs on different disks. *N* is the number of data blocks in a CKG and changes with the number of disks involved. *M* is the number of parity blocks in a CKG. A CKG has the properties of a RAID group.
- RAID columns: Stripe length of each CKG: *N*+*M*.
- Dynamic RAID: A new RAID algorithm that dynamically adjusts the number of CKs in CKGs to ensure system reliability and storage capacity. If a CK is faulty and no CK is available from disks, the system dynamically reconstructs the original *N*+*M* CKs to (*N*-1)+*M* CKs. When an extra SSD is inserted, the system

then migrates data from (*N*-1)+*M* CKs to the newly constructed *N*+*M* CKs for efficient disk usage.

- Grain: CKGs are divided into small, fixed-size blocks called grains (the default size of a grain is 8 KB). Grains are the basic units that constitute a thin LUN.
- Disk domain: A disk domain consists of multiple disks. When a storage pool is created on DeviceManager, a disk domain is automatically created within the storage system but is not displayed on DeviceManager. By default, the capacity of a storage pool is equal to the available capacity of the corresponding disk domain.

  NOTE

  You can create disk domains and storage pools on the CLI. For details, see the command reference specific to your product model and version.
- Storage pool: A storage resource container. The storage resources used by application servers are all from storage pools.
- Hot spare space: Space used for data reconstruction of faulty blocks in block virtualization. If a CK is faulty, the system lets a CK of the hot spare space take over and instructs other CKs in the CKG to perform data reconstruction using the hot spare space. This ensures data integrity and read/write performance.
- Hot spare policy: A policy that specifies the hot spare capacity of a storage pool. RAID 2.0+ allows all member disks in a storage pool to provide hot spare capacity. For ease of understanding, the hot spare capacity is expressed in the number of hot spare disks on DeviceManager. The hot spare policy of a storage pool specifies the hot spare space size of the storage pool.
- Disk redundancy: CKs in a CKG come from different SSDs. This policy enables the system to tolerate a specific number of faulty disks allowed by the RAID redundancy capacity.
- LUN: Storage space in a storage pool is divided into logical units called LUNs. A host can use storage space provided by LUNs after LUNs are mapped to it.
- LUN group: A collection of multiple LUNs. If the data of an application is stored on multiple LUNs, you can create a LUN group for these LUNs. Operations on a LUN group apply to all its member LUNs. A LUN group can contain one or more LUNs.
- Host: A physical or virtual machine that can access a storage system.
- Host group: A collection of multiple hosts. If an application is deployed on a cluster consisting of multiple hosts, these hosts will access the data volumes of the application at the same time. In this case, you can create a host group for these hosts.
- Port: Endpoint of a connection. For physical connections, ports are physical interfaces, such as Fibre Channel ports and iSCSI ports.
- Port group: A collection of multiple physical ports. If a port group is specified during the creation of a mapping, storage resources and application servers in the mapping communicate with each other using only the ports in the specified port group.
- Reconstruction: A process of restoring the data saved on a faulty disk to hot spare CKs and replacing the CKs on the faulty disk with the hot spare CKs. During data reconstruction, valid data and parity data must be read and processed to restore the data saved on a faulty disk to hot spare space,

thereby ensuring data security and reliability. Traditional reconstruction technologies allow only all disks in the same RAID group as the faulty disk to participate in reconstruction. The RAID 2.0+ technology enables all disks in the same storage pool as the faulty disk to participate in reconstruction, boosting data reconstruction speed and shortening data recovery duration.

- Deduplication: Data reduction technology that deletes duplicate data in a storage system to reduce the capacity required for storing data.
- Data compression: Technology that compresses data without causing data loss, improving the efficiency in data storage, transfer, and processing.

2.1.2 Basic Storage Principles with Disk Redundancy

In common RAID mode (disk redundancy), CKs are distributed to different disks, and the system can tolerate disk failures within the RAID redundancy capacity.

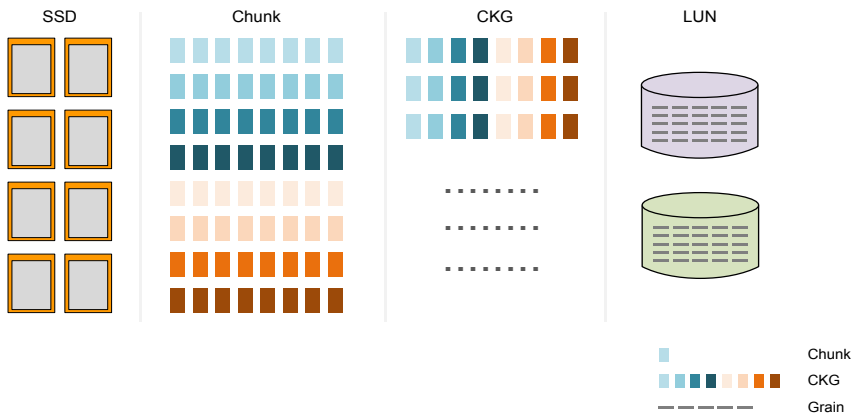
2.1.2.1 RAID 2.0+ Block Virtualization Process

SSDs with uneven data storage and heavy loads are potential system bottlenecks.

The storage system uses RAID 2.0+ for fine-grained division of SSDs to evenly distribute data to all LUNs on each SSD and balance loads.

Figure 2-1 shows the RAID 2.0+ block virtualization process when disk redundancy is used.

Figure 2-1 RAID 2.0+ block virtualization process



1. Multiple SSDs form a storage pool.
2. Each SSD is then divided into chunks (CKs) of a fixed size (typically 4 MB) for logical space management.
3. CKs from different SSDs form chunk groups (CKGs) based on the RAID policy specified on DeviceManager.
4. CKGs are further divided into grains (typically 8 KB). Grains are mapped to LUNs for refined management of storage resources.

RAID 2.0+ has the following advantages over traditional RAID:

- Balanced service loads for zero hotspots

  Even data distribution to all SSDs in a storage pool prevents individual SSDs from becoming hotspots to lower the SSD failure rate.
- Fast data reconstruction for reduced data loss

  Faulty SSDs trigger data reconstruction on all the other SSDs in the storage pool. This many-to-many reconstruction is rapid and significantly reduces data vulnerability.
- Total participation for seamless reconstruction

  All member SSDs in a storage pool participate in reconstruction, and each SSD only needs to reconstruct a small amount of data. As a result, reconstruction does not affect upper-layer applications.

2.1.2.2 RAID Usage

CKGs in RAID 2.0+ block virtualization have RAID properties. The number of RAID columns (*N*+*M*) is the stripe length of each CKG. *N* is the number of data columns in a CKG and changes with the number of CKG disks. *M* is the number of parity columns.

M Values

RAID levels determine the values of *M*. Dynamic RAID reconstruction only changes the value of *N*. **Table 2-1** describes M values for disk redundancy.

Table 2-1 M values

RAID Level	M
RAID 5	1
RAID 6 (default)	2
RAID-TP	3

Number of RAID Columns

For disk redundancy, the number of RAID columns (*N*+*M*) is calculated as follows:

- RAID 5

  NOTE

  RAID 5 cannot be configured on DeviceManager. To configure RAID 5, run the **create storage_pool name=***?* **disk_list=***?* **raid_level=RAID5 max_raid_member_number=***?* command to create a RAID 5 storage pool. The optional parameter **max_raid_member_number** specifies the maximum number of member disks in a RAID group. For details, refer to the command reference specific to your product model and version.

  RAID 6 or RAID-TP with higher reliability is recommended.

  – For OceanStor 5310, the value of **max_raid_member_number** can be 15 or 25. If the value of **max_raid_member_number** is not specified, the maximum number of member disks in a RAID group is 15 by default.

If the value of **max_raid_member_number** is 15 or not specified: Number of RAID columns = Min (Number of member disks in the storage pool – Number of reserved columns, 15)

If the value of **max_raid_member_number** is 25: Number of RAID columns = Min (Number of member disks in the storage pool – Number of reserved columns, 25)

– For OceanStor 5510, OceanStor 5610, OceanStor 6810, OceanStor 18510, and OceanStor 18810, the value of **max_raid_member_number** can be 12 or 25. If the value of **max_raid_member_number** is not specified, the maximum number of member disks in a RAID group is 12 by default.

If the value of **max_raid_member_number** is 12 or not specified: Number of RAID columns = Min (Number of member disks in the storage pool – Number of reserved columns, 12)

If the value of **max_raid_member_number** is 25: Number of RAID columns = Min (Number of member disks in the storage pool – Number of reserved columns, 25)

- RAID 6 or RAID-TP: Number of RAID columns = Min (Number of member disks in a storage pool – Number of reserved columns, 25)

Wherein, Number of reserved columns = Max (1, Number of hot spare disks)

NOTE

The methods for calculating the number of RAID columns in the following three scenarios are slightly different:

- On OceanStor 5510 and OceanStor 5610, a storage pool spans over multiple controller enclosures and contains disks from smart disk enclosures.
- On OceanStor 6810, OceanStor 18510, and OceanStor 18810, eight controllers are configured without back-end full interconnection, and a storage pool spans over multiple controller enclosures.
- A storage pool with a single controller enclosure is expanded to span over multiple controller enclosures.

Number of member disks in a storage pool in the preceding formulas refers to the number of disks owned by a single controller enclosure for a storage pool. **Example**: For RAID 6 or RAID-TP: Number of RAID columns = Min [Number of disks owned by a single controller enclosure for a storage pool – Number of reserved columns/2 (rounded up), 25]

Number of reserved columns = Max (1, Number of hot spare disks)

Example

A storage pool consists of 25 disks with RAID 6 (default value) and a hot spare policy of **Low (1 disk)**. The number of RAID columns is calculated as follows:

Number of reserved columns = Max (1, Number of hot spare disks) = 1

Number of RAID columns = Min (Number of member disks in a storage pool – Number of reserved columns, 25) = Min (25 – 1, 25) = 24

The number of RAID columns (*N*+*M*) is 24 in this example.

RAID Usage

RAID usage = [(Number of RAID columns – Number of RAID parity columns *M*)/ Number of RAID columns] x 100%

Example

The number of RAID columns (*N*+*M*) from the previous example is 24. The RAID level is RAID 6, so *M* is 2. RAID usage is therefore calculated as follows:

RAID usage = [(Number of RAID columns – Number of RAID parity columns *M*)/ Number of RAID columns] x 100% = [(24 - 2)/24] x 100% = 91.67%

The RAID usage is 91.67%.

2.1.3 Dynamic RAID Reconstruction

Data reconstruction is not possible if the number of available member disks in a disk domain with conventional RAID is less than the number of member disks in a RAID group due to continuous disk faults or disk replacement. Guaranteeing user data redundancy is impossible without reconstruction.

The storage system overcomes this problem with dynamic RAID reconstruction by CK. If the total number of available disks in a storage pool is less than the number of RAID member disks, the system retains the number of parity columns (*M*) and reduces the number of data columns (*N*) during reconstruction. After the reconstruction, the number of member disks in the RAID group decreases, but the RAID redundancy level remains unchanged. After the faulty disk is replaced, the system increases the number of data columns to *N* based on the number of available disks in the storage pool. *N*+*M* mode is used to write new data and gradually rebalance data from the fault period.

Example

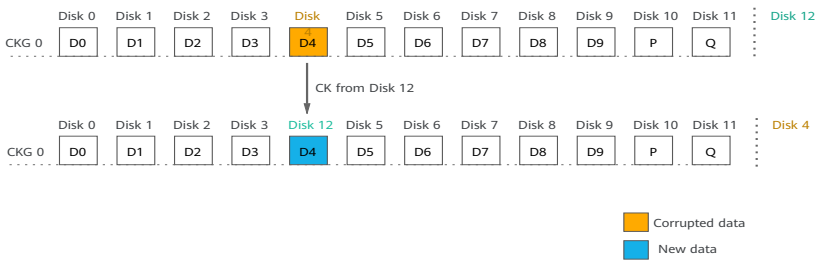
A storage pool consists of 13 disks with RAID 6 and a hot spare policy of **Low (1 disk)**. The stripe length of CKGs is *N*+*M* = 10+2.

RAID 2.0+ block virtualization uses CKs from 12 disks (Disk 0 to Disk 11) to form a CKG using the stripe structure with *N* as 10 and *M* as 2.

If a disk fails, the system excludes the disk IDs of the current CKG with mapping information and then performs the following operations:

- If new CKs are available from a disk outside of the CKG (for example, only Disk 4 is faulty and Disk 12 is available), the system directly reconstructs the failed CK and maintains the RAID level of *N*+*M*.

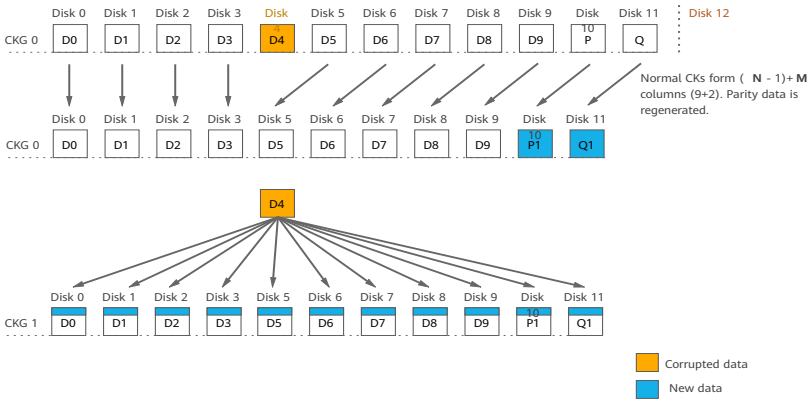
  Figure 2-2 Reconstruction with CKs from a disk outside of the CKG



- If external CKs are unavailable (for example, Disk 4 and Disk 12 fail simultaneously), the CKG is recycled with garbage collection. A new CKG

without the failed disk is formed. The number of RAID columns in the new CKG decreases to (*N*-1)+*M* or less after reconstruction, but *M* remains unchanged.

Figure 2-3 Reconstruction without CKs from a disk outside of the CKG



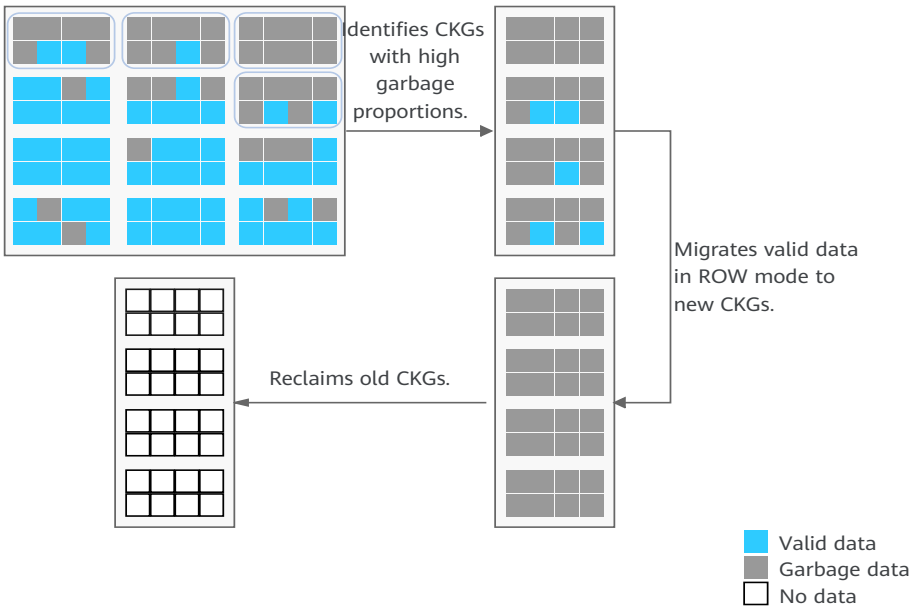
Dynamic RAID reconstruction reduces the number of RAID data disks. The system addresses faulty CKs by choosing new CKs from the available member disks for a new CKG to restore the corrupted data. The new CKG disks are all normal, so data redundancy remains the same. In this example, the original stripe is 10+2 and the new stripe is 9+2.

2.1.4 Global Garbage Collection

All the data and metadata in a storage pool are written into data blocks using redirect-on-write (ROW). The system writes data to new storage locations and marks data in the original locations as junk data. During system running, the system keeps overwriting data and modifying metadata, generating a great number of space fragments. Garbage must be collected in a timely manner to release space for writing service data. If only the garbage collection mechanism in SSDs is used, system performance will be affected because the triggering time of garbage collection is uncontrollable.

To solve this issue, the storage system uses global garbage collection. With global garbage collection, garbage collection triggering is centrally managed by controllers instead of SSDs. A controller periodically checks the garbage proportion on each CKG. Upon detecting that the garbage proportion on a CKG exceeds the threshold, the controller proactively migrates valid data from the CKG to a new one and delivers the Trim command to SSDs, to notify SSDs that the CKG is no longer used and can be reclaimed.

Figure 2-4 Global garbage collection



The global garbage collection mechanism reduces the amount of migrated data during garbage collection, minimizes the impact of garbage collection on system performance, and ensures system performance stability.

2.1.5 Terms Related to System Capacity

NOTE

- The storage system calculates the capacity as follows: 1 PB = 1,024 TB, 1 TB = 1,024 GB, 1 GB = 1,024 MB, 1 MB = 1,024 KB, 1 KB = 1,024 bytes

Object	Term	Description
System (traditional capacity mode)	Total	Total capacity of all storage pools in the storage system. If no storage pool exists, -- is displayed.
	Used	Used capacity of all storage pools in the storage system.
	Free	Free capacity = Capacity – Used capacity
Storage Pools	Total	Usable capacity of a storage pool (Total physical capacity of disks – Capacity consumed by RAID and metadata). **NOTE** This capacity is displayed as **Available Capacity** in the summary of a storage pool.

Object	Term	Description
	Used	Sum of the allocated capacity and data protection capacity of a storage pool.
	Free	Free capacity = Total capacity – Used capacity
	Total Subscribed	Total capacity of all LUNs and file systems in a storage pool.
	Used Subscribed	Total amount of data that has been written to all LUNs and file systems in a storage pool.
	Free Subscribed	Free subscribed capacity = Total subscribed capacity – Used subscribed capacity
	Subscribed Capacity Rate	(Total subscribed capacity/Total capacity) of a storage pool, indicating excess capacity allocation of a storage pool.
	Mapped Capacity	Total capacity of mapped LUNs in a storage pool. **NOTE** Mapped capacity rate = Mapped capacity/Total capacity
	Shared Capacity	Total capacity of shared file systems in a storage pool. **NOTE** Shared capacity rate = Shared capacity/Total capacity.
	Allocated capacity	Total capacity allocated to all LUNs and file systems in a storage pool. **NOTE**
	Data Protection	Total capacity of all LUNs and file systems for data protection in a storage pool.
	Thin Space Saving	Thin space saving rate = (Total subscribed capacity – Used subscribed capacity)/Total subscribed capacity
	Data Reduction Ratio	Total amount of user data written to the storage pool divided by the storage pool's used capacity. **NOTE** This parameter is displayed only after the deduplication and compression license is imported.
	Data Reduction Ratio for Block	Total amount of block data written to the storage pool divided by the storage pool's used block capacity. **NOTE** This parameter is displayed only after the deduplication and compression license is imported.

Object	Term	Description
	Data Reduction Ratio for File	Total amount of file data written to the storage pool divided by the storage pool's used file capacity. **NOTE** This parameter is displayed only after the deduplication and compression license is imported.
	Overall Space Saving Ratio	Space saving ratio of a storage pool. (Total subscribed capacity/Used subscribed capacity) x Data reduction ratio **NOTE** This parameter is displayed only after the deduplication and compression license is imported.
LUNs	Total	Capacity configured for the LUN.
	Allocated	Amount of user data written to the LUN.
	Data Protection	Capacity used for data protection on the LUN.
File Systems	Total	Capacity configured for the file system.
	Allocated	Amount of user data written to the file system.
	Data Protection	Capacity used for data protection on the file system.
	Available	Amount of user data that can be written to the file system.
Disks	Manufacturing Capacity	Nominal capacity defined by the disk manufacturer. 1 PB = 1,000 TB, 1 TB = 1,000 GB, 1 GB = 1,000 MB, 1 MB = 1,000 KB, 1 KB = 1,000 bytes
	Disk capacity	Converted in the unit of 1024 by the storage vendor from the manufacturing capacity of the disk.
	Total disk capacity	Total manufacture capacity of all disks on the device.

2.1.6 Scenarios Where the LUN Write Mode Changes to Write Protection

- Write back: A caching technique 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 protection: Data writing to storage systems is prohibited.

The default write mode of LUNs in a storage system is write back. However, the write mode will change to write protection if any of the faults listed in **Table 2-2** occurs.

Table 2-2 Scenarios where the write mode of LUNs changes to write protection

Malfunction Type	Scenario	Impact and Recommended Action
Backup battery units (BBUs) on a controller enclosure malfunction.	• Dual-controller storage device: If two BBUs malfunction and an alarm is generated, the write mode of LUNs changes from write back to write protection. • Four-controller storage device: If four BBUs malfunction and an alarm is generated, the write mode of LUNs changes from write back to write protection.	• Impact The write mode of all LUNs belonging to the controller enclosure changes to write protection. • Recommended action – Verify that the BBUs are properly installed. – Check whether the BBUs break down. If the BBUs break down, replace them. – Check whether the BBUs have sufficient power. If the BBUs have insufficient power, wait until the BBUs are fully charged.
The built-in coffer disks of multiple controllers malfunction.	• Dual-controller storage device: If the built-in coffer disks of both controllers break down, the write mode of LUNs changes from write back to write protection. • Four-controller storage device: If all coffer disks of controllers A and B or controllers C and D break down, the write mode of LUNs changes from write back to write protection.	• Impact The write mode of all LUNs belonging to the controller enclosure changes to write protection. • Recommended action Check whether the built-in coffer disks of controllers are faulty. If the coffer disks are faulty, replace them.

Malfunction Type	Scenario	Impact and Recommended Action
Controllers malfunction.	LUNs stay in write back mode for the write back hold time (192 hours by default) if only one controller on a storage system is properly working. If faults are not rectified within this period, the write mode of the LUNs changes from write back to write protection.	• Impact The write mode of all LUNs belonging to the controller enclosure changes to write protection if the fault persists for more than the write back hold time. • Recommended action – Replace the faulty controller at off-peak hours within the write back hold time. – If a spare part is unavailable during the write back hold time, you can extend the hold time properly after assessing risks to prevent write protection from adversely affecting services.
The capacity of a storage pool is used up.	An alarm is generated, indicating that the capacity of a storage pool is used up.	• Impact The write mode of LUNs changes to write protection. • Recommended action Expand the storage pool.

2.2 Application Scenarios

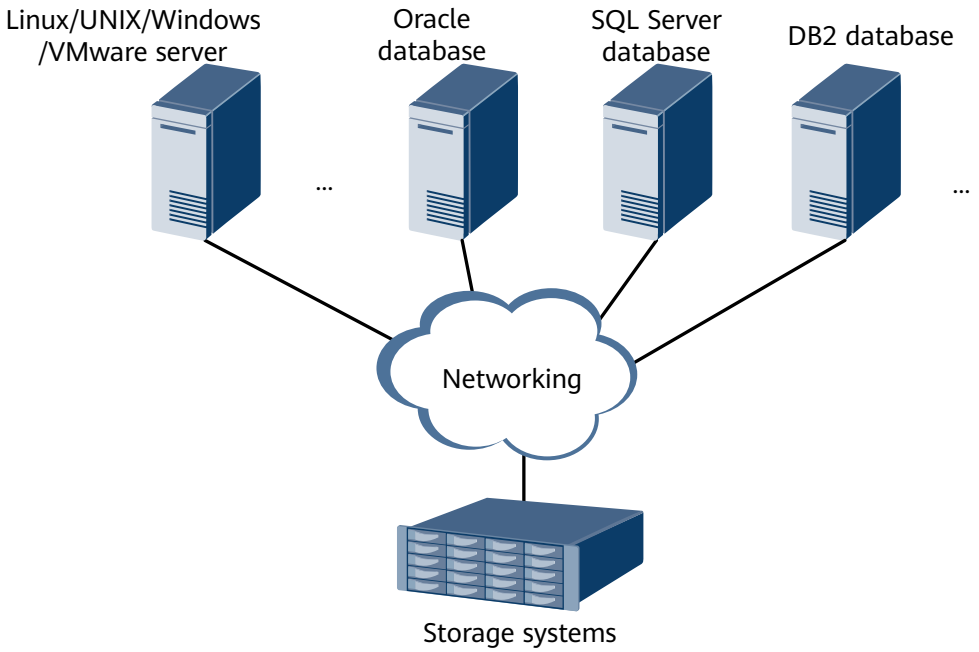
Huawei storage systems are dedicated to medium- and large-sized data centers of enterprises. They provide storage resources for storage of critical services, storage for virtual environments, and virtual desktop services.

Storage of Critical Services

The storage system boasts the innovative flash-oriented software architecture, leading hardware specifications, and 100% component redundancy. These advantages enable the storage systems to provide unparalleled levels of performance, consistently low latency, and 24/7 services for critical service storage.

These features are well suited for data processing of service systems such as OLTP/OLAP databases and HPC.

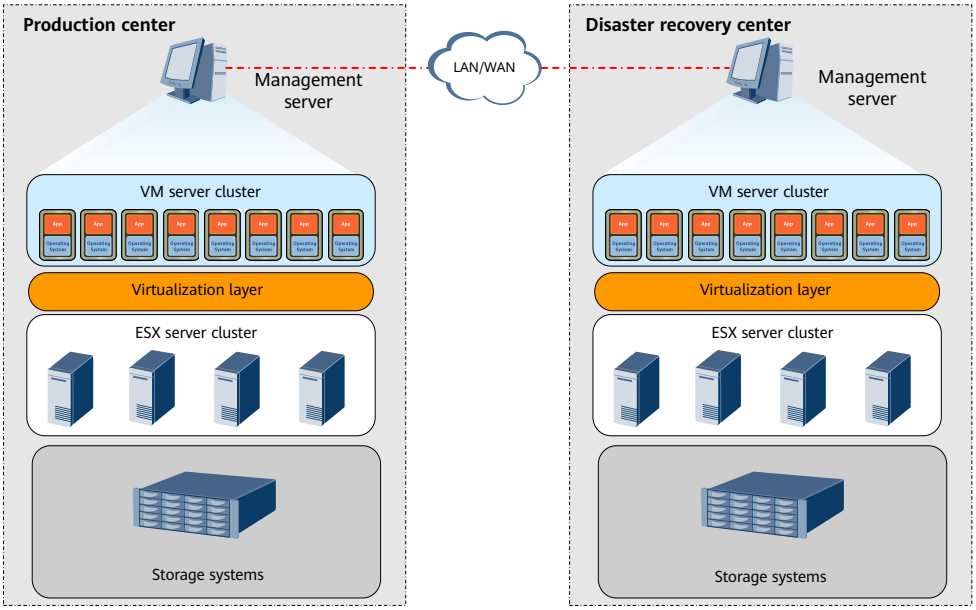
Figure 2-5 Storage of critical services



Storage for Virtual Environments

The storage system incorporates server virtualization optimization technologies such as vStorage APIs for Array Integration (VAAI), VMware vStorage APIs for Storage Awareness (VASA), and Site Recovery Manager (SRM). It also employs numerous key technologies in virtual machines (VMs) to deploy VMs fast, enhances VMs' bearing capability and operation efficiency, and streamlines storage management in virtual environments, removing the worry of complicated storage systems in virtual environments.

Figure 2-6 Storage for Virtual Environments



3 Planning Basic Storage Services

This chapter describes how to plan storage resources and management user accounts to facilitate subsequent configurations and management.

3.1 Planning Storage Resources

This section describes how to properly plan storage resources to better meet the service needs.

3.1.1 Planning the Available Capacity

The available capacity of a storage system must be properly planned to ensure sufficient capacity for service data.

For details about the available capacity and purchased capacity, contact your local Huawei representative office or Huawei authorized distributor.

When planning the available capacity, you must consider the nominal disk capacity, hot spare capacity, and RAID usage.

- Nominal disk capacity

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

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

- Hot spare capacity

  The storage system provides hot spare space to take over data from any failed disk.

- RAID usage

  The capacity used by parity data varies with the RAID level.

3.1.2 Planning Storage Pools

Storage resources are organized into storage pools. The storage resources used by application servers are all from storage pools. Storage pools must be properly planned for better storage utilization.

Planning Disk Types

Disks can be classified into self-encrypting disks (SEDs) and non-encrypting disks. They cannot exist in the same storage pool. SEDs are not sold in the Chinese mainland.

- SED: When data is written into or read from an SED, the data is encrypted or decrypted using the hardware circuits and internal encryption key of the SED.

  Before using SEDs to create a disk domain, you must configure the key service. For details, see the disk encryption user guide specific to your product model and version.
- Non-encrypting disk: does not support encryption.

Planning Disk Media Type

The storage systems can create storage pools by using solid-state drives (SSDs) and hard disk drives (HDDs). Details are as follows:

- For a hybrid flash storage pool (with both SSDs and HDDs):
  - At least four SSDs are required for OceanStor 5310, 5510, and 5610, and six SSDs for OceanStor 6810, 18510, and 18810.
  - The performance layer manages SSDs, and the storage pools only manage HDDs.
  - The SSDs form a performance layer and provide shared space for multiple storage pools. SmartAcceleration detects hot data and accelerates data processing in all scenarios and ranges throughout the lifecycle based on the performance layer. The data acceleration range varies with the capacity ratio of the performance layer.
  - Data is stored in HDDs in the storage pool. A small number of SSDs are exclusively used to store system metadata.
  - The storage pool supports SmartCompression but does not support SmartDedupe. You cannot create LUNs or file systems with a SmartDedupe attribute.
- For an all-flash storage pool (with only SSDs):
  - At least eight SSDs are required.
  - The storage pool supports only SSDs. Data and metadata are stored on SSDs.
  - The storage pool supports SmartCompression and SmartDedupe. You can create LUNs or file systems with a SmartDedupe attribute.
  - A storage pool with only HDDs is not supported.

Planning Capacity Quota for the Performance Layer

Each storage pool has a performance layer capacity quota, which limits the capacity of the performance layer used by the storage pool.

- There is a default performance layer quota on DeviceManager.
- To customize the performance layer quota when creating a storage pool, set the value of the **performance_layer_capacity** field in the **create storage_pool name=? disk_list=? performance_layer_id=? performance_layer_capacity=?** command. After a storage pool has been created, you can also change the value of the **performance_layer_capacity** field in the **change storage_pool general pool_id=? performance_layer_capacity=?** command to modify the performance layer quota. The restrictions on modifying a performance layer quota are as follows:
  - You can increase the quota as long as the performance layer has free capacity. The maximum value must not exceed the original quota plus the free capacity of the performance layer.
  - You can downsize the quota, which is not limited by the used SSD capacity. If the used capacity is greater than the new quota, the system evicts data in the read cache or the metadata to release the SSD capacity.
  - If the HDD capacity layer has no available space and the SSD performance layer cannot free up sufficient space, the quota cannot be downsized.
  - If the space released by a storage pool after downsizing is allocated to another storage pool, the space cannot be used until it is released by the storage pool.

Planning Redundancy Policies

The storage system supports only disk redundancy.

Planning RAID Policies

The storage system uses dynamic RAID for redundancy and provides different levels of protection based on the number of parity bits in a RAID group. **Table 3-1** describes RAID 5, RAID 6, and RAID-TP provided by storage systems when hot spare space is not considered.

Table 3-1 RAID levels

RAID Level	Number of Parity Bits	Redundancy and Data Recovery Capability	Maximum Number of Disks Allowed to Fail Simultaneously
RAID 5	1	Relatively high. In each CKG, the parity data occupies the space of one CK. RAID 5 is able to tolerate the failure on any one CK. If two or more CKs fail, RAID 5 protection can no longer be provided.	1

RAID Level	Number of Parity Bits	Redundancy and Data Recovery Capability	Maximum Number of Disks Allowed to Fail Simultaneously
RAID 6 (default)	2	High. In each CKG, the parity data occupies the space of two CKs. RAID 6 is able to tolerate simultaneous failures on two chunks. If three or more CKs fail, RAID 6 protection can no longer be provided.	2
RAID-TP	3	High. In each CKG, the parity data occupies the space of three CKs. RAID-TP is able to tolerate simultaneous failures on three chunks. If four or more CKs fail, RAID-TP protection can no longer be provided.	3

NOTE

- RAID 5 cannot be configured on DeviceManager. To configure RAID 5, run the **create storage_pool name=***?* **disk_list=***?* **raid_level=RAID5 max_raid_member_number=***?* command to create a RAID 5 storage pool. The optional parameter **max_raid_member_number** specifies the maximum number of member disks in a RAID group. For details, refer to the command reference specific to your product model and version.
- RAID 6 or RAID-TP with higher reliability is recommended.

The performance delivered by RAID 5, RAID 6, and RAID-TP slightly decreases in sequence as redundancy increases. For different I/O models (random/sequential, read/write), the same RAID level delivers:

- The same performance for random reads and sequential reads.
- Better performance for sequential writes than that for random writes.

Plan the most suitable RAID level based on site requirements, with performance, space efficiency, and reliability considered.

You can configure RAID policies according to the following rules:

- For critical service systems, such as billing systems of operators and class-A financial online transaction systems, you are advised to configure RAID-TP.
- For non-critical service systems, you are advised to configure RAID 6 or RAID 5.

Planning Hot Spare Policies

Hot spare policies **None**, **Low (1 disk)** (default for a new storage pool), **High (2 disks)**, **Custom (3 disks)**, **Custom (4 disks)**, **Custom (5 disks)**, **Custom (6 disks)**, **Custom (7 disks)**, and **Custom (8 disks)** are available.

NOTE

- RAID 2.0+ allows all member disks in a storage pool to provide hot spare capacity. For ease of understanding, the hot spare capacity is expressed in the number of hot spare disks on DeviceManager.
- Even if the hot spare space is used up, the system can use the free space of the storage pool to reconstruct data, ensuring storage system reliability.

Storage Pool Overcommitment Ratio Planning

Because the storage system uses thin LUNs and thin file systems, it dynamically allocates storage resources to the LUNs and file systems based on the actual capacity used by hosts instead of allocating all capacity at a time. As a result, the total capacity of the LUNs and file systems may exceed the total capacity of the storage pool.

If the capacity of the LUNs and file systems is not properly planned, the total configured capacity may be much greater than the actual total capacity of the storage pool. As the service volume increases, the storage pool space may be gradually exhausted. If capacity expansion is not performed in time, services will be affected.

The storage pool overcommitment ratio is to limit the total capacity of LUNs and file systems to a specified percentage of the storage pool capacity when they are created. This prevents the total LUN and file system capacity from greatly exceeding the actual total capacity of the storage pool.

When creating or modifying a storage pool, you can run CLI commands to set the overcommitment ratio.

- Creating a storage pool

  create storage_pool name=? disk_list=? [raid_level=? | full_threshold=? | used_up_threshold=? | pool_id=? | usage_type=? | block_size=? | description=? | **provisioning_limit_switch=?** [**provisioning_limit=?**] | protection_low_threshold=? | protection_high_threshold=? | automatic_deletion_switch=? | controller_enclosure_list=? | hotspare_strategy=? | disk_encryption_switch=? | max_raid_member_number=? | redundancy_strategy=?]

- Modifying a storage pool

  change storage_pool general { pool_id=? | pool_name=? } { name=? | full_threshold=? | used_up_threshold=? | **provisioning_limit_switch=?** | **provisioning_limit=?** | protection_low_threshold=? | protection_high_threshold=? | automatic_deletion_switch=? | performance_layer_capacity=? } * [description=? | clear_description=?]

In the commands:

- **provisioning_limit_switch** indicates whether to enable the overcommitment ratio of the storage pool. Possible values are **off** and **on**. The default value is **off**, indicating that the system does not limit the ratio of the total LUN and file system capacity to the total storage pool capacity.
- **provisioning_limit** indicates the upper limit for the percentage of the total LUN and file system capacity to the total storage pool capacity. That is, **provisioning_limit** = (Total capacity of LUNs and file systems/Total capacity of the storage pool) x 100. For example, **provisioning_limit=120** indicates

that the total LUN and file system capacity can be 120% of the total storage pool capacity.

- When a LUN or file system is created, the system determines whether [(Capacity of the new LUN or file system + Existing capacity)/Total capacity of the storage pool] x 100 exceeds the specified storage pool overcommitment ratio. If not, the creation is successful. If yes, the creation fails.
- When the capacity of a LUN or file system is expanded, the system determines whether [(Capacity added to the LUN or file system + Existing capacity)/Total capacity of the storage pool] x 100 exceeds the specified storage pool overcommitment ratio. If not, the expansion is successful. If yes, the expansion fails.
- When the storage pool overcommitment ratio is modified, the system only checks the parameter validity and does not check the capacity. For example, if the total capacity of LUNs and file systems has reached 130% of the total storage pool capacity and the current overcommitment ratio is **provisioning_limit=150**, you can still change **provisioning_limit** to **120** to limit later new or expanded LUNs and file systems.
- The **provisioning_limit** field is valid only when **provisioning_limit_switch** is set to **on**.

NOTE

- The **Provisioning Limit Switch** and **Provisioning Limit** fields in the **show storage_pool general pool_id=?** command output indicate the enabling status and configured value of the overcommitment ratio.
- For details on this command, refer to the Command Reference.

Storage Pool Configuration Rules

NOTE

For details about storage pool specifications, visit **Specifications Query**.

- When a storage pool is created on DeviceManager, a disk domain is automatically created within the storage system but is not displayed on DeviceManager. By default, the capacity of a storage pool is equal to the available capacity of the corresponding disk domain.

  NOTE

  - On the CLI, you can run the **create disk_domain name=***?* **disk_list=***?* and **create storage_pool name=***?* **disk_list=***?* to create a disk domain and a storage pool, respectively.
  - On the CLI, you can also directly run the **create storage_pool name=***?* **disk_list=***?* command to create a storage pool. After a storage pool is created, the system automatically creates the corresponding disk domain.
  - This document describes how to configure storage services on the GUI. For details about commands, refer to the command reference specific to your product model and version.

- A storage system supports one or more storage pools.
  - During the initial configuration of a storage system, you can configure that all disks constitute a unique storage pool. After this configuration applies, you do not need to manually create any storage pool.

NOTE

For details about how to initialize a storage system, see "Logging In and Starting Initialization" in the initialization guide specific to your product model and version.

  - You can manually create one or more storage pools. DeviceManager automatically selects appropriate disks to create a storage pool. Alternatively, you can select desired disks to create a storage pool.
- With disk redundancy, a single storage pool requires at least eight normal member disks. If a storage pool spans multiple controller enclosures, the minimum number of disks required for creating the storage pool is calculated as follows: Minimum number of disks = 8 x Number of controller enclosures that the storage pool spans.

3.1.3 Planning LUNs

Block storage uses LUNs as basic units for services. All LUNs on the storage system are thin LUNs.

Planning LUN Parameters

Table 3-2 lists the recommended settings for LUN parameters.

Table 3-2 LUN parameters

Parameter	Recommendation
Name	User-defined
Description	User-defined
Storage Pool	Select the storage pool to which the LUN belongs.
Capacity	Configure the capacity based on service requirements. This is the maximum capacity for each thin LUN. The total for dynamic allocation of storage resources for each thin LUN must not exceed this value. The maximum capacity of the LUN must not exceed system specifications.
Quantity	User-defined
Start Number	User-defined **NOTE** This parameter is displayed only when **Quantity** is greater than **1** and **Advanced** is selected.
Map to Host	Select the host for mapping with your created LUN.
Host LUN ID	Select a method for assignment of host LUN IDs. • **Automatic**: The system assigns a host LUN ID to each LUN mapped to a host. • **Manual**: You can manually set the host LUN ID.

Parameter	Recommendation
Application Type	Select an application type based on the service I/O model. Preset application types are provided for typical applications. In block service scenarios, possible options are **Default**, **Oracle_OLAP**, **Oracle_OLTP**, **Oracle_OLAP&OLTP**, **SQL_Server_OLAP**, **SQL_Server_OLTP**, **SQL_Server_OLAP&OLTP**, **SAP_HANA**, **Vmware_VDI**, **Hyper-V_VDI**, **Others**, and **FusionAccess_VDI**. **NOTE** • The preset application types specify the application request sizes. When SmartCompression and SmartDedupe licenses are imported to the system, the preset application types also display whether SmartCompression and SmartDedupe are enabled. For details, see *SmartDedupe and SmartCompression Feature Guide for Block* specific to your product model and version. • After you have set an application type for a LUN, you are unable to change it in follow-up operations. • If the application type configured for a LUN does not match the actual I/O model, the LUN performance may deteriorate. • If none of the preset application types matches the actual I/O model, you can run the **create lun_workload_type general** command to create one. For details on this command, refer to the Command Reference.

Planning Value-Added Features

For details about supported value-added features, visit **Specifications Query**.

For details about how to plan value-added features, see the corresponding feature guides. For example, to plan HyperSnap, see the *HyperSnap Feature Guide for Block* specific to your product model.

3.2 Planning Management User Accounts

To minimize the risk of human errors compromising storage system stability and service data security, the storage system defines user roles to determine user permission and scope of permission.

Plan the roles of local user accounts carefully and assign the accounts to the corresponding users.

For details about user roles, see the administrator guide specific to your product model and version.

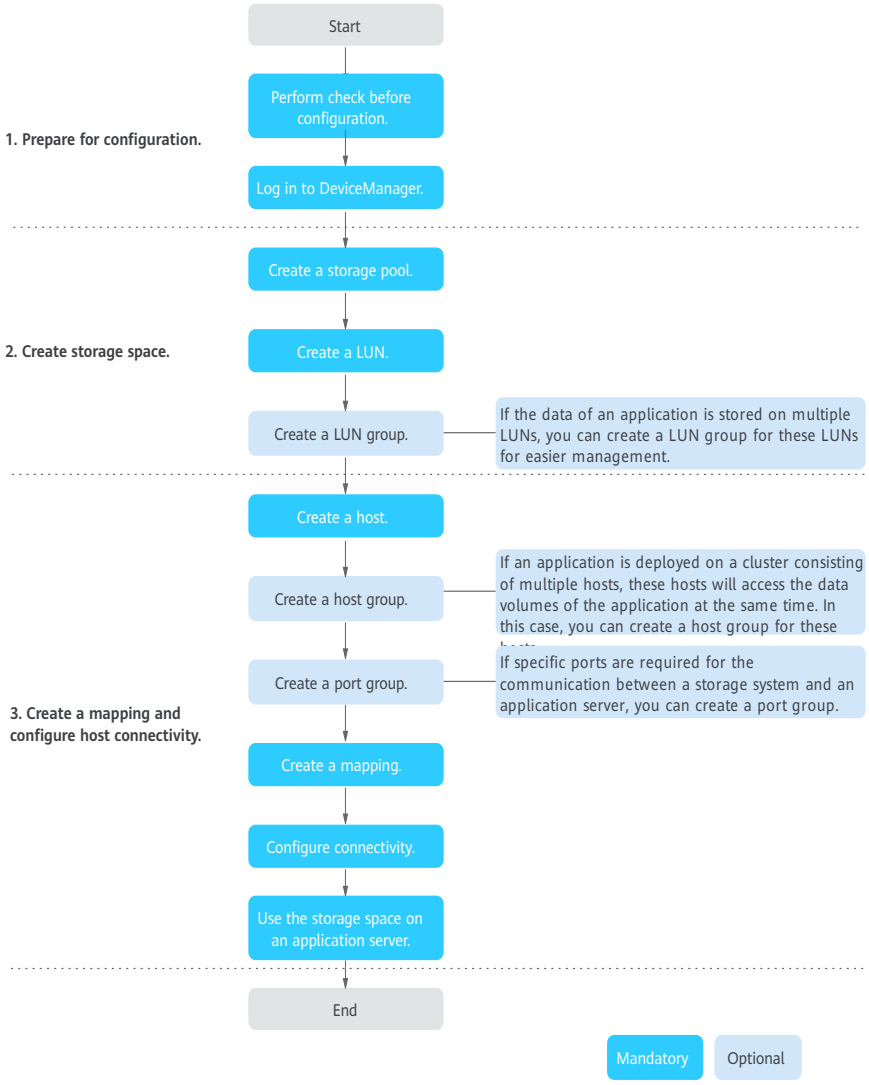
4 Configuring Basic Storage Services

This chapter describes how to configure the storage system to divide the storage space into LUNs and map them to application servers so that the application servers can read and write the storage space.

4.1 Configuration Process

This section describes the logic in configuring storage space.

Figure 4-1 Flowchart of configuring storage space



NOTE

The above flowchart shows a common configuration process. DeviceManager uses a brand-new interface interaction design, which simplifies resource allocation and supports various flexible configurations of mappings. You can select a proper one based on service requirements.

4.2 Check Before Configuration

Check the software installation and initial configuration to ensure that site requirements are met.

Checking Licenses

Log in to DeviceManager. Check whether licenses have been imported and contain the same basic or value-added features you purchased.

- If licenses have not been imported, import them by following instructions in "Logging In and Starting Initialization" in the initialization guide.
- If the licenses are different from those you purchased, contact technical support.

For OceanStor 18510 and 18810, find **OceanStor OS** on the **License Management** page of DeviceManager and ensure that the used capacity in the **Used/Total Capacity** column does not exceed the total capacity.

Checking Software Installation

Check whether the required software is properly installed on the storage system and application server.

Table 4-1 Software installation checklist

Check Item	Description
(Optional) iSCSI initiator **NOTE** The iSCSI initiators are required only for iSCSI connections.	• Windows On the Windows task bar, check whether **Microsoft iSCSI Initiator** exists in the **All Programs** list. If yes, an iSCSI initiator is installed on the application server. • SUSE On a SUSE application server, run the **rpm -qa | grep iscsi** command. If the iSCSI initiator information is displayed, an iSCSI initiator is installed on the application server. • Red Hat On a Red Hat application server, run the **rpm -qa | grep iscsi** command. If the iSCSI initiator information is displayed, an iSCSI initiator is installed on the application server. • Solaris On a Solaris application server, run the **pkginfo | grep iscsi** command. If the iSCSI initiator information is displayed, an iSCSI initiator is installed on the application server. • HP-UX On an HP-UX application server, run the **swlist iSCSI-00** command. If the iSCSI initiator information is displayed, an iSCSI initiator is installed on the application server. • VMware For VMware ESXi 4.1 and earlier versions, an iSCSI adapter already exists in a storage adapter. You can directly enable the iSCSI adapter. For VMware ESXi 5.0 and later versions, you must add an iSCSI adapter on the **Storage Adapters** page first. For details about installing an iSCSI initiator, refer to "Configuring Connectivity" in *Host Connectivity Guide*.
(Optional) UltraPath **NOTE** • Multipathing software is required when redundant paths exist between the storage system and the application server. • UltraPath is Huawei-developed multipathing software.	For details about installing UltraPath, refer to the *OceanStor UltraPath for XXX User Guide*. *XXX* represents a specific operating system, for example, Windows. **NOTE** You can log in to Huawei's technical support website at **https://support.huawei.com/enterprise/**. In the search box, enter **UltraPath**, and select a path from the paths that are automatically displayed to go to the document page. Then click the **Software Download** tab, and search for and download your desired software files.

Checking Security Settings

Check Item	Description
(Recommended) iSCSI initiator whitelist	Run the **show tgt_switch ini_white_list** command in developer mode to check whether the initiator whitelist switch is on. If the switch is off, you are advised to run the **change tgt_switch ini_white_list switch=on** command to turn it on. After this switch is turned on, iSCSI connections can be established only for manually created initiators. For details about this command, see the *Advanced O&M Command Reference*. **NOTE** • You can run the **show initiator** command to view created initiators. • After a host and a storage system are physically connected, the storage system with the initiator whitelist function enabled automatically checks whether the initiators are manually created according to their IQNs. If yes, the storage system allows the establishment of iSCSI connections. If no, the storage system does not allow the establishment of iSCSI connections. In this case, you need to manually create initiators, reconnect cables, and set up iSCSI connections.

Checking Network Connection Status

Table 4-2 lists the check items and provides the check methods.

Table 4-2 Network connection status checklist

Category	Check Item	Check Method
Connection between the maintenance terminal and the storage system	Check whether the management network port on the storage system is communicating with the maintenance terminal properly.	On the CLI of the maintenance terminal, run the following command: • For IPv4, run **ping** *ip* (where *ip* indicates the IP address of the management network port). • For IPv6, run **ping -6** *ip* (where *ip* indicates the IP address of the management network port). If the maintenance terminal receives data packets from the management network port, the storage system and maintenance terminal communicate properly. If the maintenance terminal receives no data packets from the management network port, change the IP address of the management network port and try again.
Connection between the storage system and the application server (using a Windows application server as an example)	When an iSCSI front-end port on the storage system is used for connection, check whether the iSCSI front-end port is communicating with the service network port on the application server properly.	On the CLI of the application server, run the following command: • For IPv4, run **ping** *ip* (where *ip* indicates the IP address of the front-end port). • For IPv6, run **ping -6** *ip* (where *ip* indicates the IP address of the front-end port). If the application server receives data packets from the front-end port, the storage system and application server communicate properly. If the communication is abnormal, replace the network cable, change the IP address of the front-end port, or add a route, and try again. For details on how to change the IP address of an iSCSI front-end port or add a route, see the DeviceManager online help.
	When a Fibre Channel front-end port on the storage system is used for connection, check whether the rate of the Fibre Channel front-end port is the same as that of the Fibre Channel host bus adapter (HBA) on the application server.	If the rates are different, change the rate of the Fibre Channel front-end port.

Category	Check Item	Check Method
	When a Fibre Channel front-end port on the storage system is used for connection, check whether the mode of the Fibre Channel front-end port is the same as that of the Fibre Channel HBA on the application server.	If the modes are different, change the mode of the Fibre Channel front-end port.
Connection between the storage system and switches (if switches are used)	To ensure that a link can be recovered as soon as possible after a fault occurs, you are advised to configure the ports on the switches connected to the storage system as edge ports. **NOTE** The commands for configuring a switch port as an edge port vary according to the switch vendor. For details, see the product documentation of the switch or consult the technical support of the corresponding vendor. Take Huawei CE series switches as an example. You can run the **stp edged-port enable** command to configure a port as an edge port.	Take Huawei CE series switches as an example. You can run the **display stp global** command and check the **Edged port default** field in the command output to determine whether the port is configured as an edge port. If the value is **Enabled**, the port is configured as an edge port. If the value is **Disabled**, the port is configured as a non-edge port.

4.3 Logging In to DeviceManager

DeviceManager is a device management program developed by Huawei. DeviceManager has been loaded to a storage system before delivery. You can log in to DeviceManager to manage storage resources in a centralized manner.

For details about how to log in to DeviceManager, see "Logging In to DeviceManager" in the initialization guide specific to your product model and version.

4.4 Creating a Storage Pool

This section describes how to create a storage pool from which application servers can use storage space.

Context

A storage pool supports two storage tiers. Data of different access frequencies is migrated among different storage tiers, optimizing storage performance allocation. The features are as follows:

- The performance layer consists of SSDs or NVMe SSDs and delivers high performance. The cost of storage media is high, and the capacity of a single disk is small.
- The capacity layer consists of SAS disks or NL-SAS disks and delivers low performance. The cost of storage media is moderate, the capacity of a single disk is large, and the reliability is high.

Prerequisites

When creating a storage pool for the first time, the system creates a performance layer automatically. The capacity of the performance layer is shared by all storage pools. To create a performance layer, the following conditions must be met:

- If multiple controller enclosures are used, the number and capacity of disks on all controller enclosures must be the same.
- A maximum of two disk capacity specifications are supported.
- (For 6.1.3 and earlier versions) SEDs and non-SEDs cannot be used at the same time. After data encryption is enabled, all disks must be SEDs.
- (For 6.1.5 and later versions) SEDs and non-SEDs can be used at the same time only when the HyperEncryption license is imported and data encryption is enabled.
- The total capacity of SSDs (that is, the available capacity of the performance layer) meets the minimal performance layer quota recommended for creating a storage pool.

Procedure

Step 1 Choose **System** > **Storage Pools**.

Step 2 Click **Create**.

The **Create Storage Pool** page is displayed on the right.

NOTE

The screenshot is for reference only and the actual displayed information may vary.

Step 3 Set the storage pool parameters.

Table 4-3 describes the parameters.

NOTE

- When a hybrid-flash storage pool is created, the system automatically recommends a quota of the performance layer for the storage pool based on the number and capacity of selected disks in the capacity layer.
- When creating an all-flash storage pool, you can set a quota of the performance layer for the storage pool. The minimum quota cannot be less than 2 TB.
- If both an all-flash storage pool and a hybrid-flash storage pool are required, create an all-flash storage pool before creating a hybrid-flash storage pool.

Table 4-3 Advanced storage pool parameters

Parameter	Description
Name	Name of the storage pool. [Value range] • The name must be unique. • The name can contain only letters, digits, periods (.), underscores (_), and hyphens (-). • The name contains 1 to 255 characters.

Parameter	Description
Description	Description of the storage pool.
Data Encryption	Indicates whether to enable data encryption ● If this function is disabled, the storage pool is not encrypted. ● If this function is enabled, the storage pool is encrypted. **NOTE** ● If this function is enabled, the system automatically checks whether the key service has been configured. If the key service has not been configured, the system will prompt you to configure the key service. For details, see the *Disk Encryption User Guide* specific to your product model and version. ● This parameter can be set only when no performance layer is created. Data encryption takes effect for both the performance and capacity layers. If a performance layer already exists, the data encryption attribute is the same as that of the performance layer. ● The data encryption attribute cannot be changed once being specified during storage pool creation.
Encryption Algorithm	For non-SEDs, the storage system uses DEKs to encrypt data and then writes the encrypted data to disks. When data is read, the storage system uses the DEKs to decrypt the data. If only non-SEDs are used, you must select an encryption algorithm after data encryption is enabled. Possible values are **SM4** and **AES**. If both SEDs and non-SEDs are used, after data encryption is enabled, the system uses the same algorithm as that used by the SEDs to encrypt data on the non-SEDs by default. **NOTE** ● This parameter is available only when a performance layer has not been created, **Data Encryption** is enabled, and the HyperEncryption license has been imported. ● The encryption algorithm takes effect for both the performance layer and capacity layer. If a performance layer already exists, the encryption algorithm is the same as that of the performance layer. ● Only the Sansec KMIP key server supports the SM4 encryption algorithm. ● The SM4 encryption algorithm is supported only in the Chinese Mainland. ● The encryption algorithm cannot be changed once being specified during storage pool creation. ● Only 6.1.5 and later versions support this parameter.

Parameter	Description
Redundancy Policy	**Disk redundancy**. CKs in a CKG come from different disks. Disk failures within the RAID redundancy capability are allowed. **NOTE** The redundancy policy of a storage pool cannot be changed once being specified during storage pool creation. [Default value] Disk redundancy
RAID Policy	The meaning of each RAID policy level is as follows: ● RAID 6: In each chunk group, the parity data occupies the space of two chunks. Failures on any two chunks can be tolerated. If three or more chunks fail, data in the chunk group cannot be recovered. ● RAID-TP: In each chunk group, the parity data occupies the space of three chunks. Failures on any three chunks can be tolerated. If four or more chunks fail, data in the chunk group cannot be recovered. [Default value] RAID 6
Controller Enclosure	Controller enclosure to which the storage pool belongs.
Capacity Layer	In the function pane of the capacity layer, **Capacity per Disk**, **Type**, **Available Disks**, and **Selectable Disk per Controller Enclosure** are displayed. In the text box of **Required Disks**, enter the number of disks in each controller enclosure used to create the storage pool. **NOTE** You can click **Select** to manually select disks.
Performance Layer	When creating a storage pool for the first time, you need to set the name of the performance layer to create a performance layer. By default, all SSDs are used to create the performance layer. On DeviceManager, you cannot change the disk selection for the performance layer. If the performance layer does not meet the creation requirements, manually remove and insert disks.

Parameter	Description
Capacity Layer Hot Spare Policy	Hot spare policy of a storage pool. Hot spare space stores data from the failed member disks to ensure system continuity and reliability. [Value range] None, Low (1 disk), High (2 disks), Custom (3 disks), Custom (4 disks), Custom (5 disks), Custom (6 disks), Custom (7 disks), and Custom (8 disks) **NOTE** • Hot spare capacity is provided by all member disks in each storage pool because the storage system uses RAID 2.0+ virtualization technology. For ease of understanding, the hot spare capacity is expressed in the number of hot spare disks on DeviceManager. • Even if the hot spare space is used up, the system can use the free space of the storage pool to reconstruct data, ensuring storage system reliability. • The hot spare policy of an all-flash storage pool is subject to that of the performance layer.
Performance Layer Hot Spare Policy	When creating a performance layer, you need to set a hot spare policy for the performance layer. Hot spare space is used to take over data from failed member disks to ensure stable running of the storage system. [Value range] Default, None, Low (1 disk), High (2 disks), Custom (3 disks), Custom (4 disks), Custom (5 disks), Custom (6 disks), Custom (7 disks), and Custom (8 disks)
Capacity Alarm Threshold (%)	When the percentage of the storage pool's allocated capacity to its total capacity reaches this threshold, the system generates a capacity alarm. A proper capacity alarm threshold helps you monitor the capacity usage of a storage pool. [Value range] 1 to 95 [Default value] 80

Parameter	Description
Capacity Used Up Alarm Threshold (%)	When the percentage of the storage pool's allocated capacity to its total capacity reaches this threshold, the system generates an alarm indicating that the capacity is being used up. The severity of this alarm is higher than that of the capacity alarm. [Value range] 2 to 99 [Default value] 90 **NOTE** The value of **Capacity Used Up Alarm Threshold (%)** must be greater than that of **Capacity Alarm Threshold (%)**.
Protection Data Auto Deletion	Indicates whether to automatically delete earliest scheduled HyperCDP objects when the percentage of the protection capacity or used capacity to the storage pool's total capacity reaches **Protection Capacity Upper Limit (%)**. The automatic deletion stops when the percentage becomes less than **Protection Capacity Lower Limit (%)**.
Protection Capacity Lower Limit (%)	Lower limit for the percentage of the protection capacity to the storage pool's total capacity for the system to stop deleting earliest scheduled HyperCDP objects. **NOTE** This parameter is available only when **Protection Data Auto Deletion** is enabled. [Value range] 1 to 95 [Default value] 20
Protection Capacity Upper Limit (%)	Maximum allowable percentage of the protection capacity to the storage pool's total capacity. **NOTE** • This parameter is available only when **Protection Data Auto Deletion** is enabled. • The value of **Protection Capacity Upper Limit (%)** must be greater than that of **Protection Capacity Lower Limit (%)**. [Value range] 2 to 99 [Default value] 30

NOTE

Description, **RAID Policy**, **Capacity Alarm Threshold (%)**, **Capacity Used Up Alarm Threshold (%)**, and **Protection Data Auto Deletion** are hidden. To display hidden parameters, select **Advanced**.

Step 4 Click **OK**.

Confirm your operation as prompted.

NOTE

After the task is created successfully, the **Execution Result** page is displayed. You can view details about the current task on this page.

----End

4.5 Creating a LUN

After creating a storage pool, you must create LUNs in it and map the LUNs to hosts. This allows the hosts to use the storage resources provided by the storage pool.

Context

- All LUNs created in a storage system are thin LUNs, which are logical disks accessible to hosts. The storage system dynamically allocates storage resources to thin LUNs based on actual capacities used by hosts, instead of allocating all preset capacities. The total capacity allocated to a thin LUN will not exceed its preset capacity.
- For details about the specifications, see the **Specifications Query** tool.
- Before creating a LUN, you are advised to clear any alarms indicating that the storage pool capacity is about to be used up.
- The total capacity configured for all LUNs in a storage pool can exceed the actual capacity of the storage pool. If an alarm is generated, indicating that the storage pool capacity is used up, you are advised to expand the storage pool as soon as possible.

Procedure

Step 1 Choose **Services** > **Block Service** > **LUN Groups** > **LUNs**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Click **Create**.

The **Create LUN** page is displayed on the right.

NOTE

The screenshot is for reference only and the actual displayed information may vary.

For some device models, you can click  in the upper right corner of the page to enable SmartGUI. SmartGUI mines users' historical operation data and builds a configuration parameter recommendation model based on user profiles to recommend configuration parameters for the block service and file service. After SmartGUI is enabled, the system presets parameters based on recommendations when you create a LUN. You can click **Modify** in the upper right corner to modify the parameters or directly click **OK** to create a LUN.

Step 4 Set the LUN parameters.

Table 4-4 describes the parameters.

Table 4-4 LUN parameters

Parameter	Description
Name	Name of the LUN. [Value range] • The name must be unique. • The name can contain only letters, digits, periods (.), underscores (_), and hyphens (-). • The name contains 1 to 255 characters when **Quantity** is **1** and 1 to 251 characters when **Quantity** is greater than **1**.
Owning vStore	vStore to which the newly created LUN belongs. **NOTE** This parameter is mandatory when **vStore** is set to **All vStores** in Step 2.

Parameter	Description
Description	Description of the LUN. [Value range] The description can be left blank or contain up to 255 characters.
Start ID	Start ID of the LUN.
Owning Storage Pool	Storage pool to which the LUN belongs.
Capacity	Capacity of the LUN. This is the maximum capacity that will be allocated to a thin LUN. The total storage resources dynamically allocated to the thin LUN must not exceed the value of this parameter. **NOTE** • The maximum capacity of the LUN must not exceed the system specifications. For details about the specifications, see the **Specifications Query** tool. • You can set the capacity unit to **Blocks** to create LUNs by block. A block is equal to 512 bytes. The LUN capacity must not be smaller than 1024 blocks (that is, 512 KB). • The storage system uses the following capacity algorithms defined by Windows: 1 PB = 1,024 TB, 1 TB = 1,024 GB, 1 GB = 1,024 MB, 1 MB = 1,024 KB, and 1 KB = 1,024 bytes.
Quantity	Number of LUNs created in a batch. Set this parameter based on site requirements. [Value range] 1 to 500 **NOTE** LUNs created in a batch have the same capacity.
Suffix Digits	Number of digits in the suffixes of the LUNs to be created in a batch. **NOTE** This parameter is displayed only when **Quantity** is greater than **1** and **Advanced** is selected.
Suffix	Set the start number of the suffixes of the LUNs to be created in a batch. The system adds a suffix to the end of each LUN name in ascending order based on the specified start suffix number. **NOTE** • This parameter is displayed only when **Quantity** is greater than **1** and **Advanced** is selected. • The value range of **Suffix** is 0 to (10000 – **Quantity**). • For example, if you want to create 300 LUNs, the value range of **Suffix** is 0 to 9700.

Parameter	Description
Application Type	Application type of the LUN. Preset application types are provided for typical applications. In block service scenarios, possible options are **Default**, **Oracle_OLAP**, **Oracle_OLTP**, **Oracle_OLAP&OLTP**, **SQL_Server_OLAP**, **SQL_Server_OLTP**, **SQL_Server_OLAP&OLTP**, **SAP_HANA**, **Vmware_VDI**, **Hyper-V_VDI**, and **FusionAccess_VDI**. **NOTE** • After you have set an application type for a LUN, you are unable to change it in follow-up operations. • If the application type configured for a LUN does not match the actual I/O model, the LUN performance may deteriorate. • If none of the preset application types matches the actual I/O model, you can run the **create lun_workload_type general** command to create one. For details on this command, refer to the *Command Reference*.
Add to LUN Group	Existing LUN group to which the created LUN is added. **NOTE** Parameters **Add to LUN Group** and **Map to Host** cannot be specified at the same time.
Map to Host	Host to which the LUN you are creating is mapped. **NOTE** • If no host is available in the system, click **Create**. • You can also map the LUNs after creating them.
Port Group	Port group to which the mapping is added. After this parameter is specified, the LUN and its mapped host are added to the port group for communication. **NOTE** • This parameter is displayed only when **Map to Host** is specified. • If no port group is available, click **Create** to create one.
Host LUN ID	ID of the LUN after being mapped to a host. • **Automatic**: The system assigns a host LUN ID to each LUN mapped to a host. • **Start ID**: Set a start ID ranging from 0 to 4095. The system assigns a host LUN ID to each LUN mapped to a host, starting from **Start ID**. • **Specified ID**: Manually assign a host LUN ID to each LUN mapped to a host.

NOTE

Description, **Start ID**, and **Host LUN ID** are hidden parameters. To display hidden parameters, click **Advanced**.

Step 5 Click **OK**.

Confirm your operation as prompted.

NOTE

If the LUN is mapped to a host, after the task is created successfully, the **Execution Result** page is displayed. You can view details about the current task on this page.

----End

4.6 (Optional) Creating a LUN Group

This section describes how to create a LUN group to facilitate the management of multiple LUNs that store data for the same user application.

Context

For details about the specifications, see the **Specifications Query** tool.

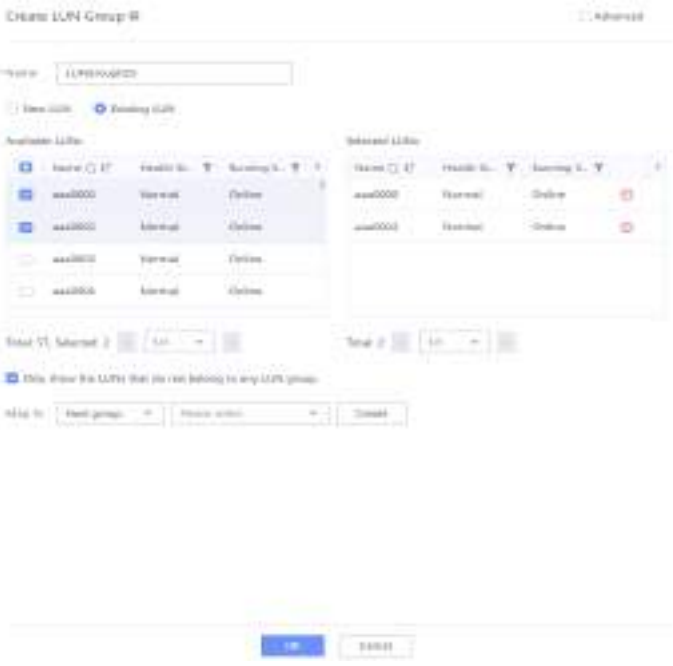
Procedure

Step 1 Choose **Services** > **Block Service** > **LUN Groups** > **LUN Groups**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Click **Create**.

The **Create LUN Group** page is displayed on the right.



NOTE

The screenshot is for reference only and the actual displayed information may vary.

For some device models, you can click  in the upper right corner of the page to enable SmartGUI. SmartGUI mines users' historical operation data and builds a configuration parameter recommendation model based on user profiles to recommend configuration parameters for the block service and file service. After SmartGUI is enabled, the system presets parameters based on recommendations when you create a LUN group. You can click **Modify** in the upper right corner to modify the parameters or directly click **OK** to create a LUN group.

Step 4 Set LUN group information.

1. Set the name of the new LUN group.

   NOTE

   - The name must be unique.
   - The name can contain only letters, digits, periods (.), underscores (_), and hyphens (-).
   - The name contains 1 to 255 characters.

2. In the **Owning vStore** drop-down list, select the vStore to which the newly created LUN belongs.
3. Input necessary information about the LUN group in **Description** to help you identify the LUN group.

   NOTE

   Description is hidden. You can click **Advanced** to display it.

4. Select LUNs.
   - If you select **New LUN**:
     i. Select the storage pool to which the LUN belongs and set **Application Type** for the LUNs.

     NOTE

     The following preset application types are provided for typical applications: **Default**, **Oracle_OLAP**, **Oracle_OLTP**, **Oracle_OLAP&OLTP**, **SQL_Server_OLAP**, **SQL_Server_OLTP**, **SQL_Server_OLAP&OLTP**, **SAP_HANA**, **Vmware_VDI**, **Hyper-V_VDI**, and **FusionAccess_VDI**.

     - After you have set an application type for a LUN, you are unable to change it in follow-up operations.
     - If the application type configured for a LUN does not match the actual I/O model, the LUN performance may deteriorate.
     - If none of the preset application types matches the actual I/O model, you can run the **create lun_workload_type general** command to create one. For details on this command, refer to the *Command Reference*.

     ii. Specify the LUN name prefix, capacity per LUN, and quantity. **Table 4-5** describes the parameters.

Table 4-5 LUN parameters

Parameter	Description
Name Prefix	Name prefix of the LUN. The names of the new LUNs are numbered in sequence based on the name prefix.
Capacity per LUN	Maximum capacity that will be allocated to a thin LUN. The total storage resources dynamically allocated to the thin LUN must not exceed the value of this parameter. **NOTE** ○ The maximum capacity of the LUN must not exceed the system specifications. ○ You can set the capacity unit to **Blocks** to create LUNs by block. A block is equal to 512 bytes. The LUN capacity must not be smaller than 1024 blocks (that is, 512 KB). ○ The storage system uses the following capacity algorithms defined by Windows: 1 PB = 1,024 TB, 1 TB = 1,024 GB, 1 GB = 1,024 MB, 1 MB = 1,024 KB, and 1 KB = 1,024 bytes.
Quantity	Number of LUNs created in a batch. Set this parameter based on site requirements. [Value range] 1 to 500 **NOTE** ○ LUNs created in a batch have the same capacity. ○ When LUNs are created in a batch, the system automatically adds suffixes to the names based on the number of LUNs for distinction. You can click to manually specify the suffixes.

iii. (Optional) When creating LUNs in a batch, click and set the suffixes of the LUNs. Related parameters include **Suffix Digits** and **Suffix** (start number of the suffixes). The system adds a suffix to the end of each LUN name in ascending order based on the specified start suffix number.

NOTE

- The value range of **Suffix** is 0 to (10000 – **Quantity**).
- For example, if you want to create 300 LUNs, the value range of **Suffix** is 0 to 9700.

iv. (Optional) Click + to add more LUNs.

v. (Optional) Click — to remove LUNs.

– If you select **Existing LUN**:

Select one or more LUNs from **Available LUNs** to add them to **Selected LUNs**.

NOTE

You can select **Only show the LUNs that do not belong to any LUN group** to view LUNs that do not belong to any LUN group.

5. (Optional) Configure a mapping for the LUN group.
   a. Select a host or host group.

      NOTE

      If no host or host group exists in the system, click **Create** to create one.

   b. Select a port group.

      NOTE

      - To display this option, select the host or host group to which the LUN group is to be mapped.
      - If no port group exists in the system, click **Create** to create one.

   c. Select **Advanced** in the upper right corner and set how to assign host LUN IDs.
      - **Automatic**: The system assigns a host LUN ID to each LUN mapped to a host.
      - **Start ID**: Set a start ID ranging from 0 to 4095. The system assigns a host LUN ID to each LUN mapped to a host, starting from **Start ID**.
      - **Specified ID**: Manually assign a host LUN ID to each LUN mapped to a host.
   d. If HyperMetro pairs have been created for the selected LUNs, determine whether to select **Same Host LUN ID**. If you select it, the system forcibly ensures that the host LUN IDs of the local and remote LUNs in the same HyperMetro pairs are the same. In SAN-based HyperMetro scenarios involving ESX hosts, if the host LUN IDs of the local and remote LUNs in the same HyperMetro pairs are different, data may be inconsistent.

Step 5 Click **OK**.

Confirm your operation as prompted.

NOTE

After the task is created successfully, the **Execution Result** page is displayed. You can view details about the current task on this page.

----End

4.7 Creating a Host

This section describes how to create a virtual host on a storage system and add an initiator for the host to establish a mapping between the storage system and application server.

4.7.1 Creating a Host

This section describes how to create a single virtual host on a storage system.

Context

- DeviceManager not only allows users to manually create hosts but also provides the host scan function. To use the host scan function, perform the following operations:
  a. Install UltraPath on a host and connect the host to the storage system over a physical network.
  b. On DeviceManager, choose **Settings** > **Block Service**. Click **Modify** in the upper right corner of the page. In the **UltraPath Host Scan** area, enable **Scan for Host**.
  c. Scan for disks on hosts and wait for about 4 minutes.
  d. On DeviceManager, choose **Services** > **Block Service** > **Host Groups** > **Hosts** and click **Scan for Host**. The system automatically scans for all hosts connected to the storage system, identifies their WWNs or IQNs, and creates corresponding virtual hosts on the storage system. If a host has multiple WWNs or IQNs, the system can automatically identify and configure them on the same host.
- When a host is created, the storage system automatically sets the default host access mode based on the host operating system. For details about how to change the host access mode, see **5.7.14 Modifying the Properties of a Host**.

Procedure

Step 1 Choose **Services** > **Block Service** > **Host Groups** > **Hosts**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 On the **Hosts** tab page, choose **Create** > **Create Host**.

The **Create Host** page is displayed on the right.

NOTE

The screenshot is for reference only and the actual GUI may vary.

Step 4 Set basic information for the host.

Table 4-6 describes the parameters.

Table 4-6 Host parameters

Parameter	Description
Name	Name of the host. [Value range] • The name must be unique. • The name can contain only letters, digits, periods (.), underscores (_), and hyphens (-). • The name contains 1 to 255 characters.
Owning vStore	vStore to which the newly created host belongs. **NOTE** This parameter is mandatory when **vStore** is set to **All vStores** in Step 2.
Description	Description of the host.

Parameter	Description
OS	Operating system used by the host. [Value range] The value can be **Linux**, **Windows**, **Solaris**, **HP-UX**, **AIX**, **XenServer**, **Mac OS**, **VMware ESX**, **LINUX_VIS**, **OpenVMS**, **Oracle_VM_Server_for_x86**, and **Oracle_VM_Server_for_SPARC**. **NOTE** The selected operating system must be the same as that of the application server connected to the storage system.
IP Address	IP address of the host. **NOTE** If a host is connected over iSCSI links, enter the service IP address of the host for easy management.
Location	Location of the host.

NOTE

Parameters **Description** and **Location** are hidden. You can click **Advanced** to display them.

Step 5 Configure initiators for the host.

1. Select an initiator type (FC, iSCSI, or NVMe over RoCE) based on service requirements.
2. For an FC initiator, you need to select the vStore to which the initiator belongs. An FC initiator whose owning vStore is the same as that of the created host or whose owning vStore is **--** can be added to the host.

   For iSCSI and NVMe over RoCE initiators, you can only add initiators whose owning vStore is the same as that of the created host to the host.
3. If initiators have been configured on the application server, select one or more initiators in the initiator list. If no initiator is available in the list, click **Create Initiator** below the initiator list to manually create an initiator.

NOTE

- Do not add initiators of different application servers to the same host.
- If the host operating system is HP-UX, create an initiator manually.
- You are advised to map a LUN to a host using initiators of the same type.

Step 6 (Optional) Click **Create Initiator**. On the **Create Initiator** page that is displayed, set the related parameters.

NOTE

- If initiators have been configured on an application server:
  - When initiators can be automatically discovered on DeviceManager, skip this step.
  - When initiators cannot be automatically discovered on DeviceManager, create initiators using the IQNs or WWPNs of initiators configured on the application server.
- If no initiator has been configured on an application server, configure initiators by following instructions in **Configuring Connectivity** in the corresponding *Host Connectivity Guide* and then add initiators on DeviceManager.
- On DeviceManager, set parameters of initiators manually created or automatically discovered based on the multipathing software and host operating system version. For details about recommended parameter settings in different scenarios, see **Configuring Multipathing** in the corresponding *Host Connectivity Guide* . For iSCSI initiators, you need to set CHAP authentication parameters based on the security authentication plan.

Table 4-7 describes the FC initiator parameters.

Table 4-7 FC initiator parameters

Parameter	Description
WWPN	World Wide Port Name (WWPN) of the initiator. [Value range] A WWPN is a hexadecimal value that contains 16 characters. It can contain letters A to F (uppercase and lowercase) and digits 0 to 9. It cannot be all 0, all F, or all f.
Alias	Alias of the initiator. [Value range] • An alias can be left blank or contain up to 31 characters. • An alias can contain only letters, digits, periods (.), underscores (_), and hyphens (-).

Table 4-8 describes the iSCSI initiator parameters.

Table 4-8 iSCSI initiator parameters

Parameter	Description
IQN	iSCSI Qualified Name (IQN) of the iSCSI initiator. **NOTE** The IQN of an initiator must be the same as the one on the application server. The IQN of an initiator must be unique. Do not configure the initiators of multiple application servers with the same IQN. [Value range] An IQN must contain 1 to 223 visible ASCII characters and start with a digit or letter.

Parameter	Description
Alias	Alias of the iSCSI initiator. [Value range] ● An alias can be left blank or contain up to 31 characters. ● An alias can contain only letters, digits, periods (.), underscores (_), and hyphens (-).
CHAP	CHAP authentication includes **Normal Authentication** and **Discovery Authentication** options. ● If you enable CHAP, you must configure a CHAP name and password for the storage system and the same CHAP name and password on the application server. ● If you do not enable CHAP, you do not need to configure a CHAP name or password. **NOTE** After changing the CHAP authentication password on the storage system, you must use the new password to configure the CHAP authentication again on the application server.
Normal Authentication	The normal session is the process during which the target and initiator transmit data between each other after connections have been set up. Authentication modes include: ● No authentication ● Unidirectional authentication The target authenticates the initiator. ● Bidirectional authentication The target and initiator authenticate each other.
Discovery Authentication	The discovery session is the process during which the target and initiator are setting up connections. Authentication modes include: ● No authentication ● Unidirectional authentication The target authenticates the initiator. ● Bidirectional authentication The target and initiator authenticate each other. **NOTE** When **Normal Authentication** or **Discovery Authentication** is set to **Bidirectional authentication**, you need to specify the **CHAP Name** and **Password**, and confirm the password in both the **Target Authenticates Initiator** and **Initiator Authenticates Target** areas.
CHAP Name	User name for CHAP authentication. **NOTE** ● The name must contain 4 to 223 characters. ● The name can contain only letters, digits, and special characters (!"#$&%'()*+,-./:;<=>?@[\]^_`{|}~). ● The first character must be a letter or digit.

Parameter	Description
Password	Password for CHAP authentication. **NOTE** • The password can contain 12 to 16 characters. • The password must contain at least three types of characters among uppercase letters, lowercase letters, digits, and special characters (`~!@#$%^&*()-_=+|[{}];:<,.\>/? and spaces). • The password must not be the same as the user name or the user name spelled backwards.
Confirm Password	Password for CHAP authentication. [Value range] The value of **Confirm Password** must be consistent with that of **Password**.

Table 4-9 describes the NVMe over RoCE initiator parameters.

Table 4-9 NVMe over RoCE initiator parameters

Parameter	Description
NQN	World Wide Port Name (WWPN) of the initiator. [Value range] • The value contains 1 to 223 characters. • The value must start with a digit or letter. • The value must be visible ASCII characters.
Alias	Alias of the initiator. [Value range] • An alias can be left blank or contain up to 31 characters. • The value can contain only letters, digits, underscores (_), hyphens (-), and periods (.).

NOTE

After you click **OK**, the new initiator is automatically added to the list on the right.

Step 7 Confirm your operation.

- If no initiator has been added for the host, no further action is required.
- If initiators have been added for the host, a security alert dialog box is displayed.
  a. Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation**.

b. Click **OK**.

The **Execution Result** page is displayed, indicating that the operation succeeded.

c. Click **Close**.

----End

4.7.2 Creating Hosts in Batches

This section describes how to create virtual hosts in batches.

Procedure

Step 1 Choose **Services** > **Block Service** > **Host Groups** > **Hosts**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 On the **Hosts** tab page, choose **Create** > **Create Hosts**.

The **Create Hosts** page is displayed on the right.

NOTE

The screenshot is for reference only and the actual GUI may vary.

Step 4 Set basic information for the hosts.

Table 4-10 describes the parameters.

Table 4-10 Host parameters

Parameter	Description
Name	Name of the host. [Value range] • The name must be unique. • The name can contain only letters, digits, periods (.), underscores (_), and hyphens (-). • The name contains 1 to 255 characters when **Quantity** is **1** and 1 to 251 characters when **Quantity** is greater than **1**.

Parameter	Description
Owning vStore	vStore to which the newly created host belongs. **NOTE** This parameter is mandatory when **vStore** is set to **All vStores** in **Step 2**.
Description	Description of the host.
Quantity	Number of hosts to be created in a batch. **NOTE** A maximum of 500 hosts can be created at a time.
Suffix Digits	Number of digits in the suffixes of the hosts to be created in a batch. **NOTE** This parameter is displayed only when **Quantity** is greater than **1**.
Suffix	Set the start number of the suffixes of the hosts to be created in a batch. The system adds a suffix to the end of each host name in ascending order based on the specified start suffix number. **NOTE** • This parameter is displayed only when **Quantity** is greater than **1**. • The value range of **Suffix** is 0 to (10000 – **Quantity**). • For example, if you want to create 300 hosts, the value range of **Suffix** is 0 to 9700.
OS	Operating system used by the host. [Value range] The value can be **Linux**, **Windows**, **Solaris**, **HP-UX**, **AIX**, **XenServer**, **Mac OS**, **VMware ESX**, **LINUX_VIS**, **OpenVMS**, **Oracle_VM_Server_for_x86**, and **Oracle_VM_Server_for_SPARC**. **NOTE** The selected operating system must be the same as that of the application server connected to the storage system.
Location	Location of the host.

NOTE

Parameters **Description** and **Location** are hidden. You can click **Advanced** to display them.

Step 5 Click **OK**.

Confirm your operation as prompted.

----End

4.8 (Optional) Creating a Host Group

If an application is deployed on a cluster consisting of multiple hosts, these hosts will access the data volumes of the application at the same time. In this case, you can create a host group for these hosts.

Context

Hosts in a host group can run different operating systems.

Procedure

Step 1 Choose **Services** > **Block Service** > **Host Groups** > **Host Groups**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 On the **Host Groups** tab page, click **Create**.

The **Create Host Group** page is displayed on the right.

NOTE

The screenshot is for reference only and the actual GUI may vary.

Step 4 Set the host group parameters listed in **Table 4-11**.

Table 4-11 Host group parameters

Parameter	Description
Name	Name of the host group. [Value range] • The name must be unique. • The name can contain only letters, digits, periods (.), underscores (_), and hyphens (-). • The name contains 1 to 255 characters.
Owning vStore	vStore to which the newly created host group belongs. **NOTE** This parameter is mandatory when **vStore** is set to **All vStores** in Step 2.
Description	Description of the host group.

Step 5 Select one or more hosts from **Available Hosts** and add them to **Selected Hosts**.

NOTE

- You can select **Only show the hosts that have not been added to any host group** below the host list, which helps you find the desired hosts.
- You can click **Create Host** below the host list to create a host.

Step 6 Click **OK**.

Confirm your operation as prompted.

----End

4.9 (Optional) Creating a Port Group

A port group is a logical collection of multiple physical ports. A storage system can use designated ports, that is, member ports in a port group to establish a mapping between LUNs and servers. After you create a port group and add it to a mapping, LUNs and hosts in the mapping use the ports in the port group to communicate with each other. If no port group is added to a mapping, available ports are randomly used.

Procedure

Step 1 Choose **Services** > **Block Service** > **Port Groups**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Click **Create**.

The **Create Port Group** page is displayed on the right.

NOTE

The screenshot is for reference only and the actual GUI may vary.

Step 4 Set parameters of the port group. **Table 4-12** describes the parameters.

Table 4-12 Port group parameters

Parameter	Description
Name	Name of the port group. [Value range] • The name must be unique. • The name can contain only letters, digits, periods (.), underscores (_), and hyphens (-). • The name contains 1 to 255 characters.
Owning vStore	Specifies the vStore to which the newly created host belongs. **NOTE** This parameter is mandatory when **vStore** is set to **All vStores** in **Step 2**.
Description	Description of the port group.
Port Type	Type of ports to be added to a port group. The value can be **Physical port** or **Logical port**. Only one type of ports can be added to a port group.

Step 5 Select one or more desired ports from the port list on the left and they are displayed in the port list on the right.

NOTE

- A port can be added to multiple port groups.
- You can select **Include the ports that are link down** below the port list, which helps you find the desired ports.

Step 6 Click **OK**.

Confirm your operation as prompted.

----End

4.10 Creating a Mapping

This section describes how to create a mapping between hosts/host groups and LUNs/LUN groups so that hosts can use the storage space provided by LUNs.

Context

- Skip this section if you have specified **Map to Host** when creating a LUN or **Map to Host (or Host Group)** when creating a LUN group.
- For details about specifications, visit **Specifications Query**.
- Based on the ports used by mappings, mappings can be classified into LUN mapping and LUN masking.
  - LUN mapping: A LUN is bound with the WWPN or IQN of a host's port to establish a one-to-one or N-to-one connection and access relationship with the host's port. A host can identify the same LUN regardless of which port on the storage system is connected to the host.
  - LUN masking: A LUN is bound with a front-end port on the storage system. The LUN that a host can access varies with the storage port connected to the host.

Creating a Mapping

DeviceManager provides various simple and flexible methods for you to create the following mappings:

- Mapping between LUNs and a host

  You can directly map one or more LUNs to a host in a simple application scenario or when no LUN groups are required.
- Mapping between a LUN group and a host

  If an application requires multiple LUNs, you can use a LUN group to manage these LUNs. In this case, create a mapping between the LUN group and the host.
- Mapping between a LUN group and a host group

  If an application has its data stored on multiple LUNs and is deployed on a cluster consisting of multiple hosts, you can use a LUN group to manage the LUNs and a host group to manage the hosts. In this case, create a mapping between the LUN group and the host group.

Table 4-13 describes how to create various types of mappings.

Table 4-13 Methods for creating mappings

Object To Be Selected	Mapped To	Method
One or more LUNs	One host + (optional) a port group	1. Choose **Services** > **Block Service** > **LUN Groups** > **LUNs**. The LUN management page is displayed. 2. Select one or more LUNs and click **Map**. On the displayed **Map LUN** page, set the required parameters.
One LUN group	One host + (optional) a port group One host group + (optional) a port group	1. Choose **Services** > **Block Service** > **LUN Groups** > **LUN Groups**. The LUN group management page is displayed. 2. Select a LUN group and click **Map**. On the displayed **Map LUN Group** page, set the required parameters.
One host	One or more LUNs One LUN group + (optional) a port group	1. Choose **Services** > **Block Service** > **Host Groups** > **Hosts**. The host management page is displayed. 2. Select a host, choose **Map** > **Map LUN** or **Map LUN Group**. On the displayed **Map LUN** or **Map LUN Group** page, set the required parameters.
One host group	One LUN group + (optional) a port group	1. Choose **Services** > **Block Service** > **Host Groups** > **Host Groups**. The host group management page is displayed. 2. Select a host group, choose **Map** > **Map LUN Group**. On the displayed **Map LUN Group** page, set the required parameters.

NOTE

- This section describes only the navigation paths in various scenarios. For details about the operations, see corresponding sections in "Managing Basic Storage Services."
- GUIs may vary with product versions and models. The actual GUIs prevail.

4.11 Configuring the Host Connectivity

This section describes how to configure the connectivity between a host and a storage system to ensure that the host can properly use the storage resources allocated by the storage system.

4.11.1 Configuring Storage Service Ports (Applicable to iSCSI Connections)

When a storage system and a host are connected over iSCSI connections, configure ports on the storage system based on service requirements before configuring connectivity to ensure that the storage system can communicate with the host properly.

The storage system uses logical ports to establish iSCSI connections with hosts. The home ports of logical ports can be Ethernet ports, bond ports, or VLANs.

- If the storage system communicates with the host using logical ports that reside on Ethernet ports, configure the storage service ports and other connectivity configurations by referring to "Establishing iSCSI Connections" in the *Host Connectivity Guide*.
- If the storage system communicates with the host using logical ports that reside on bond ports or VLANs, configure the storage service ports by following instructions in this section and then configure the connectivity by referring to "Establishing iSCSI Connections" in the *Host Connectivity Guide*.

NOTE

If the storage system is connected to a host over Fibre Channel connections, configure the host and storage system by referring to the *Host Connectivity Guide*.

Basic Concepts

Table 4-14 lists the basic concepts related to iSCSI Connections.

Table 4-14 Basic concepts related to iSCSI Connections

Concept	Description
Ethernet port	Ethernet ports on an interface module of a storage system. Bond ports, VLANs, and logical ports are created based on Ethernet ports.
Bond port	To improve reliability of paths for accessing file systems and increase bandwidth, you can bond multiple Ethernet ports on the same controller to form a bond port.

Concept	Description
VLAN	VLANs logically divide the Ethernet ports or bond ports of a storage system into multiple broadcast domains. On a VLAN, when service data is being sent or received, a VLAN ID is configured for the data to isolate it from other VLANs, ensuring data security and reliability.
Logical port	Logical ports are virtual ports created based on bond ports, VLANs, or Ethernet ports. A unique IP address is allocated to each logical port to carry host services.

Relationship Among Logical Ports, Ethernet Ports, VLANs, and Bond Ports

Logical ports can be created based on Ethernet ports, VLANs, or bond ports. Figure 4-2 shows the relationship among logical ports, Ethernet ports, VLANs, and bond ports.

Figure 4-2 Relationship among logical ports, Ethernet ports, VLANs, and bond ports

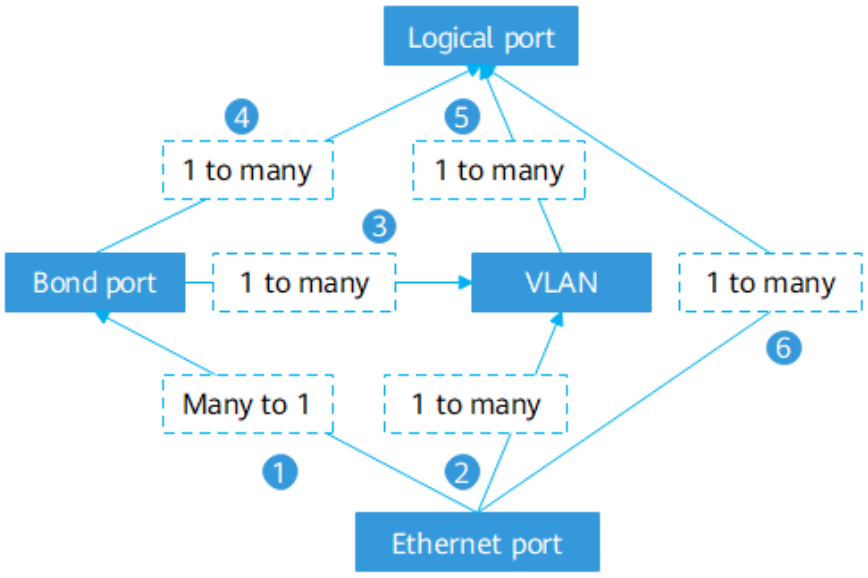


Table 4-15 explains the meaning of each mark number in the preceding figure.

Table 4-15 Meanings of the mark numbers

Mark Number	Description
1	Indicates that multiple Ethernet ports are bonded to form a bond port.
2	Indicates that an Ethernet port is added to multiple VLANs.
3	Indicates that a bond port is added to multiple VLANs.

Mark Number	Description
4	Indicates that a bond port is used to create multiple logical ports.
5	Indicates that a VLAN port is used to create multiple logical ports.
6	Indicates that an Ethernet port is used to create multiple logical ports.

4.11.1.1 Creating a Bond Port

To increase link bandwidth and redundancy, you can bond multiple Ethernet ports under the same controller.

Prerequisites

- The IP addresses of the Ethernet ports you want to bond have been cleared. Ethernet ports that have IP addresses cannot be bonded.
- If the **Security Type** of an interface module is **IPsec**, its ports cannot be bonded across interface modules.

Context

Port bonding provides more bandwidth and higher redundancy for links. Although ports are bonded, each session still transmits data through a single port and the total bandwidth can be increased only when there are multiple sessions. Determine whether to bond ports based on site requirements.

Port bonding has the following restrictions:

- Only Ethernet ports that have the same rate and are on the same controller can be bonded. Ports cannot be bonded across controllers. Non-Ethernet ports cannot be bonded.
- Link aggregation (IEEE 802.3ad) is supported.
- For OceanStor 5310, OceanStor 5510 and OceanStor 5610:
  - GE interface modules (not supporting TOE) support port bonding across modules by default.
  - 10GE, 25GE, 40GE, and 100GE interface modules (supporting TOE) do not support port bonding across modules by default. They support port bonding across modules after TOE is disabled.

    NOTICE

    To disable the TOE function of a port, contact Huawei technical support.

  - The onboard network ports of OceanStor 5310 can be bonded across interface modules and the port rates must be the same.

- For OceanStor 6810, OceanStor 18510, and OceanStor 18810, interface modules in the same quadrant can be bonded across interface modules, and the TOE function of the ports to be bonded must be disabled.

  NOTICE

  To disable the TOE function of a port, contact Huawei technical support.

  For OceanStor 6810, OceanStor 18510, and OceanStor 18810, each interface module can use only one bonding mode. That is, an interface module does not allow bonding across modules and bonding within the module at the same time.

- Read-only users are not allowed to bond Ethernet ports.
- Each Ethernet port can be added to only one bond port.
- A member port of a port group cannot be added to a bond port.
- Management network ports cannot be bonded.
- Member ports in the same bond port cannot connect to different switch networks.
- After Ethernet ports are bonded, their MTU changes to the default value and you need to configure the switch port mode. Take Huawei switches as an example. You must set the ports on the Huawei switches to work in static LACP mode.

  NOTICE

  The link aggregation modes vary with switch manufacturers. If a switch from another vendor is used, contact technical support of the switch manufacturer for specific link aggregation configurations.

Port bonding on the host has the following restriction:

If the TOE function is enabled on the storage system and the host port connecting to the switch must be bonded, the bonding mode must be set to 4.

NOTE

If the preceding restriction cannot be met, disable the TOE function of the port.

Procedure

Step 1 Choose **Services** > **Network** > **Ethernet Network** > **Bond Ports**.

Step 2 Click **Create**.

The **Create Bond Port** page is displayed on the right.

Step 3 Set a bond name and select ports you want to bond.

1. Specify a name for the bond port in **Name**.

NOTE

The name must meet the following requirements:

- The value can contain only letters, digits, underscores (_), hyphens (-), and periods (.).
- The name contains 1 to 31 characters.

2. Select the controller where the bond port resides.
3. In **Available Ports**, select one or more ports you want to bond.

Step 4 Click **OK**.

Confirm your operation as prompted.

----End

Follow-up Procedure

To configure an IP address for a bond port, run the **change bond_port ipv4_address bond_port_name=? ip=? mask=?** or **change bond_port ipv6_address bond_port_name=? ip=? prefix_length=?** command. For details about this command, see the command reference specific to your product model.

Example:

```
admin:/>change bond_port ipv4_address bond_port_name=bond1 ip=192.168.1.1 mask=255.255.0.0
DANGER: You are about to change the IP address of port. This operation will disconnect the storage system from hosts. This operation will also clear the configured routes on the IP address that is modified on this port.
Suggestion:
1. Check whether there are redundant connections to hosts. If there are no redundant connections, stop host services.
2. Ensure that the entered IP address is available.
Have you read danger alert message carefully?(y/n)y

Are you sure you really want to perform the operation?(y/n)y
Command executed successfully.
```

4.11.1.2 Creating a VLAN

You can add Ethernet ports or bond ports to multiple independent VLANs. Different services are configured in different VLANs to ensure the security and reliability of service data.

Context

- VLANs are created on Ethernet or bond ports.
- VLANs cannot be created on the Ethernet ports that are configured with IP addresses or carry services.
- A bond port instead of its member ports can be used to create a VLAN.
- The host ports and storage ports in the same VLAN must have the same VLAN IDs.

Procedure

Step 1 Choose **Services** > **Network** > **Ethernet Network** > **VLANs**.

Step 2 Click **Create**.

The **Create VLAN** page is displayed on the right.

Step 3 In the **Port Type** drop-down list, select the type of the ports used to create VLANs.

Possible values are **Ethernet Port** and **Bond Port**.

Step 4 In the **Home Port** list, select a home port.

Step 5 In **ID**, specify the ID of a VLAN, and then click **Add**.

NOTE

- The VLAN ID ranges from 1 to 4094. You can specify multiple VLAN IDs one by one or in a batch. When creating multiple VLANs and specifying VLAN IDs in a batch, the VLAN IDs are in the following format: Start VLAN ID-End VLAN ID.
- To delete a VLAN ID, click × next to it.

Step 6 Click **OK**.

----End

Follow-up Procedure

When creating a logical port based on a VLAN, ensure that the port type is VLAN and the home port is the VLAN's home port.

4.11.1.3 Creating a Logical Port

A logical port is a virtual port that carries host services. It can be created on an Ethernet port, a bond port, or a VLAN.

Context

Only logical ports that support iSCSI and NVMe over RoCE can be used to carry block services. For iSCSI connections, select iSCSI as the data protocol for a logical port.

Procedure

Step 1 Choose **Services** > **Network** > **Logical Ports**.

Step 2 Click **Create**.

The **Create Logical Port** page is displayed on the right.

Step 3 Set the parameters listed in **Table 4-16**.

Table 4-16 Logical port parameters

Parameter	Description
Name	Name of the logical port. The name must: ● Be unique. ● Contain only letters, digits, underscores (_), hyphens (-), and periods (.). ● Contain 1 to 255 characters.
Role	Roles of logical ports include the following: **Management**: A port of this role is used by a vStore administrator to log in to the system for management. **Service**: A port of this role is used to access services. **Management + service**: A port of this role is used to access services or for a vStore administrator to log in to the storage system for system management. **Replication**: A port of this role is used for replication link connection in remote replication or HyperMetro, or for quorum link connection in HyperMetro. **NOTE** ● For iSCSI connections, select **Service**. ● Only 6.1.3 and later versions support role types of **Management** and **Management + service**.
Data Protocol	Data protocol of the logical port. Possible values are **NFS**, **CIFS**, **NFS + CIFS**, **iSCSI**, and **NVMe over RoCE**. **NOTE** ● **NFS**, **CIFS**, and **NFS + CIFS** are applicable to file services. **iSCSI** and **NVMe over RoCE** are applicable to block services. ● For iSCSI connections, select **iSCSI**. ● This parameter is available only when **Role** is set to **Service** or **Management + service**.
Owning vStore	vStore to which the logical port belongs. **NOTE** This parameter is displayed only when **Role** is set to **Service**, **Management**, or **Management + service**.
IP Address Type	IP address type of the logical port, which can be **IPv4** or **IPv6**.
IP Address	IPv4 or IPv6 address of the logical port.
Subnet Mask	Subnet mask of the logical port's IPv4 address. **NOTE** This parameter is available only when **IP Address Type** is set to **IPv4**.
Prefix	Prefix length of the logical port's IPv6 address. **NOTE** This parameter is available only when **IP Address Type** is set to **IPv6**.

Parameter	Description
Gateway	Gateway of the logical port's IP address.
Port Type	Type of the logical port. Possible values are **Ethernet port**, **Bond port**, **VLAN**, and **RoCE port**. **NOTE** • If **Data Protocol** is set to **NFS**, **CIFS**, **NFS + CIFS**, or **iSCSI**, you can select **Ethernet port**, **Bond port**, or **VLAN**. • If **Data Protocol** is set to **NVMe over RoCE**, you can select **VLAN** or **RoCE port**. • Only 6.1.5 and later versions support RoCE ports.
Home Port	Ethernet port, bond port, VLAN, or RoCE port to which the logical port belongs. **NOTE** If **Port Type** is set to **RoCE port**, you can only select the RoCE port whose **Trust Mode** is **DSCP**.

Step 4 Click **OK**.

----End

4.11.2 Configuring Connectivity

Context

- For Fibre Channel networks, you can choose the SCSI-port-based FC-SCSI protocol or the NVMe-port-based FC-NVMe protocol.
- The storage system also supports NVMe over RoCE networking.
- You can query the models, versions, and OSs of the application servers and switches supported by the networks on the **Huawei Storage Interoperability Navigator**.

Configuration Method

Verify that storage resources required by services have been successfully created on the storage system. The storage resources include storage pools, LUNs, hosts, and mappings between hosts/host groups and LUNs/LUN groups.

- Network using the iSCSI or FC-SCSI protocol

  Configure the connectivity by following instructions in the "Configuring Connectivity" in *Host Connectivity Guide*.

  Table 4-17 Host connectivity guides for common operating systems

Host OS	Host Connectivity Guide
AIX	**https://support.huawei.com/enterprise/en/doc/EDOC1100113069**

Host OS	Host Connectivity Guide
HP-UX	https://support.huawei.com/enterprise/en/doc/EDOC1100117891
Red Hat	https://support.huawei.com/enterprise/en/doc/EDOC1100113070
Solaris	https://support.huawei.com/enterprise/en/doc/EDOC1100113071
SUSE	https://support.huawei.com/enterprise/en/doc/EDOC1100117892
VMware ESXi	https://support.huawei.com/enterprise/en/doc/EDOC1100116456
Windows	https://support.huawei.com/enterprise/en/doc/EDOC1100116985

- Network using the FC-NVMe or NVMe over RoCE protocol
  - For Linux hosts: Follow the instructions in the "Configuring Connectivity" section in **Host Connectivity Guide for Connecting to Linux Hosts Using NVMe over Fabrics**.
  - For VMware ESXi hosts: Follow the instructions in the "Configuring Connectivity" section in **Host Connectivity Guide for Connecting to VMware ESXi Hosts Using NVMe over Fabrics**.

4.12 Using the Storage Space on an Application Server

After a connection is established between a storage system and an application server, the application server must discover the newly-added logical disk (that is, the storage space specified by a mapped LUN) to use it as a common disk for data reads and writes.

Prerequisites

Note the following before using the LUN:

- The application server is communicating properly with the storage system.
- The planned storage capacity has been allocated to the application server.
- Multipathing software has been installed and configured for the application server when redundant paths exist between the application server and the storage system. This prevents multiple LUNs from being repetitively mapped to the application server.

NOTE

- For details about how to install and configure UltraPath, Huawei-developed multipathing software, refer to the UltraPath user guide specific to your operating system. For details about how to configure OS native multipathing software, refer to *Host Connectivity Guide*.
- If multipathing software is installed and configured after LUNs are mapped to the application server, you must restart the application server for the multipathing policies to take effect.

Precautions

- Note the following when using the storage space on application servers:
  - Do not allocate disks in use to other applications. Otherwise, data security will be compromised.
  - If a host login error occurs, operations on disks affect the running of applications.
  - If compatibility issues occur, use of the storage space on application servers may be compromised.
- When unmapping a LUN, delete the residual information of the original mapping on the host side to prevent exceptions. For details, see section "FAQs" in the *Host Connectivity Guide*.

Context

The maximum LUN capacity that can be identified by an application server varies according to the operating system and file system used by the application server. **Table 4-18** lists the maximum LUN capacity supported by various operating systems.

Table 4-18 Maximum LUN capacity supported by various operating systems

Operating System	File System	Maximum Allowed LUN Capacity
Windows Server 2003	NTFS	2 TB **NOTE** If a LUN mapped to a Windows Server 2003-based application server is larger than 2 TB, convert it into a GUID Partition Table (GPT) disk.
Windows Server 2003 SP1 and later	NTFS	256 TB
Windows XP 32bit	NTFS	2 TB
Windows XP 64bit	NTFS	256 TB
Windows Server 2008	NTFS	256 TB
Windows 7	NTFS	256 TB

Operating System	File System	Maximum Allowed LUN Capacity
SUSE Linux Enterprise Server	EXT3/ReiserFS/XFS	16 TB/16 TB/8 EB
Red Hat Enterprise Linux 5	EXT3/XFS	16 TB/100 TB
Red Hat Enterprise Linux 6	EXT3/EXT4/XFS	16 TB/16 TB/100 TB

NOTE

- Plan the capacity of a LUN before mapping it to an application server. If the LUN capacity exceeds the specifications, the application server will fail to identify the LUN.
- The above table lists the maximum LUN capacities supported by some common operating systems. For the maximum LUN capacities of other operating systems, consult technical support engineers. The actual specifications prevail.

Configuration Method

For details, see the *Host Connectivity Guide*.

4.13 More Configuration Scenarios

4.13.1 Configuring Basic Storage Services for VMware VVol

Virtual volume (VVol) is a new function in VMware ESXi 6.0. This section describes how to configure basic storage services for VMware VVol.

Procedure

Step 1 Create a PE LUN and map it to a VMware ESXi host.

NOTE

- For details about how to configure basic storage services, such as creating a storage pool, creating a PE LUN, creating a host, and mapping a PE LUN, see the corresponding sections in this document.
- For details about how to configure the connectivity between a storage system and a VMware ESXi host, see the ***Host Connectivity Guide***.

Step 2 Configure the VVol function by following instructions in the eSDK Enterprise Storage Plugins VASA user guide.

- Obtain the corresponding user guide.
  a. Go to resource pages of eSDK Enterprise Storage Plugins.
     Visit **https://support.huawei.com/enterprise/**, enter **eSDK Enterprise Storage Plugins** in the search box, and select the automatically associated path to go to the **Documentation** page.

b. Query the version mapping between the storage system and eSDK Enterprise Storage Plugins and download the mapping VASA software package.

i. On the **Documentation** page, obtain and view the eSDK Enterprise Storage Plugins Version Mapping of the corresponding version.

ii. On the **Software Download** page, download the VASA software package that matches the storage version and model.

c. On the **Documentation** page, download the eSDK Enterprise Storage Plugins User Guide (VASA 2.0) that matches the storage version and model.

- Perform the following operations by following instructions in the user guide:

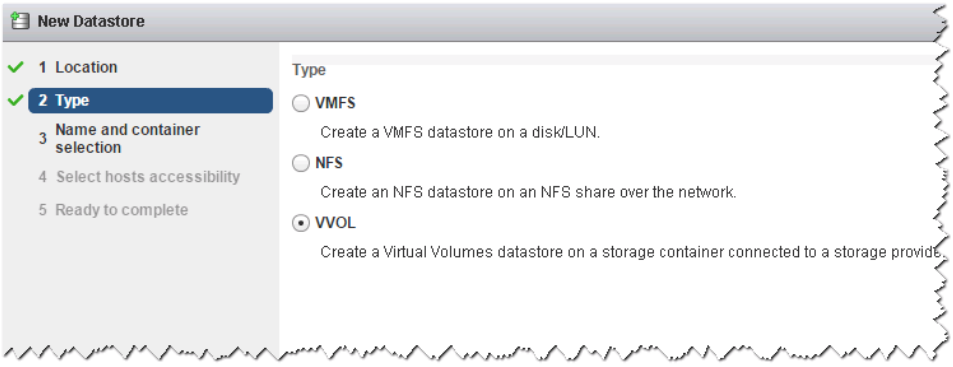
a. Install VASA Provider.

b. Register the storage system and configure a storage container on the eSDK Unified Management Portal.

c. Register VASA Provider with vCenter.

Step 3 Use a virtual datastore to create a VM.

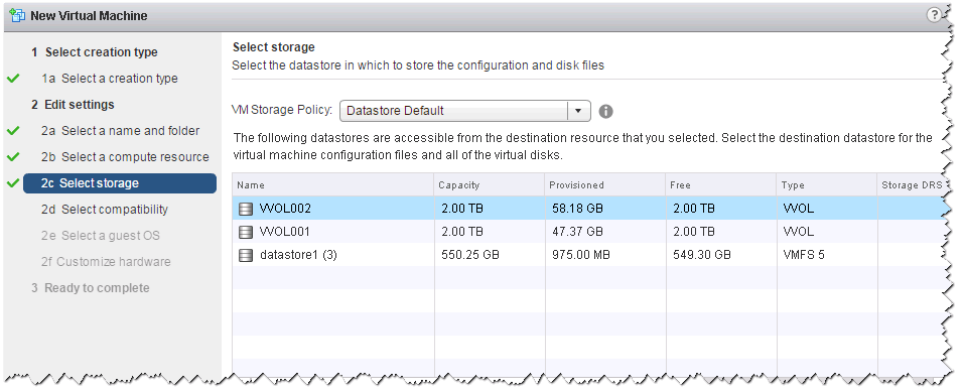
1. Log in to vSphere Web Client.
2. In **VM Storage Policies**, configure data service rules.
3. If the vCenter is newly built, you need to create a data center.
4. In the vCenter, click **Storage**, right-click the vCenter data center, and choose **Related Objects** > **Datastores** > . Create a datastore whose type is **VVOL**.



NOTE

GUIs may vary with software versions. The actual GUIs prevail.

5. Right-click the vCenter data center, choose **New Virtual Machine** > **New Virtual Machine**, and select an appropriate VM storage policy and a VVol datastore to create a VM.



----End

4.13.2 Configuring Storage Resources in Batches

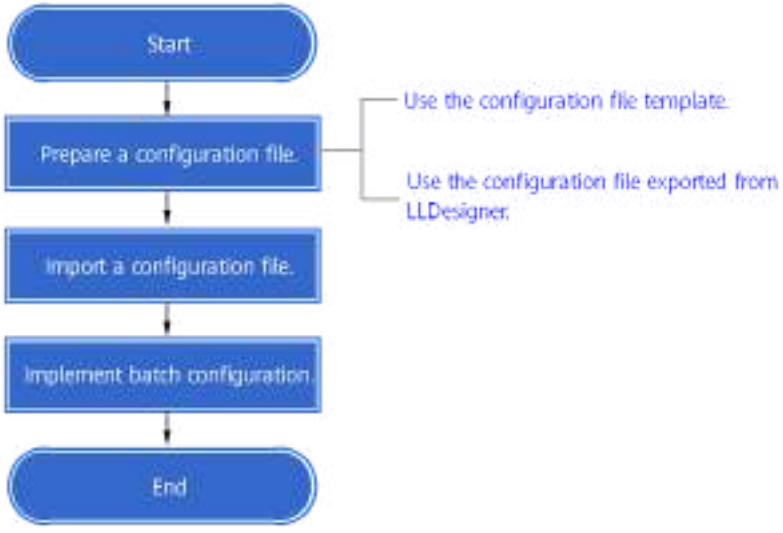
Batch configuration, a function provided by DeviceManager, uses configuration files to divide storage resources in batches to simplify resource management.

- Only the super administrator can use the batch configuration function.
- During batch configuration, CLI commands are used. You can obtain command reference of the related product to learn how to effectively use these commands.

4.13.2.1 Configuration Process

Figure 4-3 shows the process for configuring the storage space in batches.

Figure 4-3 Batch configuration process



4.13.2.2 Preparing a Configuration File

Before configuring the storage space in batches, prepare a .conf configuration file that contains commands to be executed in batches.

You can prepare a configuration file in either of the following ways:

1. Download the configuration file template provided by the storage system and edit commands in the template as required.
2. If the project is planned and designed using LLDesigner, you can contact Huawei engineers or Huawei certified resellers to provide the .conf configuration file exported from LLDesigner.

4.13.2.2.1 Using a Configuration File Template

You can download a configuration file template from DeviceManager and edit commands in the templates as required.

Prerequisites

DeviceManager is properly communicating with the storage system.

Context

- The exported default configuration file template is named **Example.conf**.
- The configuration file template downloaded from DeviceManager is in the ANSI encoding format.

Procedure

Step 1 In the upper right corner of the home page, choose  > **Batch Configure**.

Step 2 Download the configuration file template.

1. Click **Configuration File Template**.

   A file download dialog box is displayed. The following example is based on Internet Explorer 11.
2. Click **Save As**.

   The **Save As** dialog box is displayed.
3. Set the save path and file name.
4. Click **Save**.

----End

4.13.2.2.2 Using a Configuration File Exported from LLDesigner

If the project is planned and designed using LLDesigner, you can contact Huawei engineers or Huawei certified resellers to provide the .conf configuration file exported from LLDesigner.

4.13.2.3 Importing a Configuration File

This operation enables you to import a service configuration file.

Prerequisites

Only configuration files not being executed can be imported.

Context

- If a configuration file fails system check or is not executed during the import process, only the administrator who imports the configuration file can import a new configuration file.
- The latest imported configuration file will overwrite the earlier configuration file.
- The configuration file to be imported cannot be larger than 100 KB.

Procedure

Step 1 In **Service Configuration File**, click ***.

Step 2 Select the desired configuration file and click **Open**.

The selected configuration file is displayed in the file selection area.

Step 3 Click **Upload**.

Message **Configuration file uploaded successfully** is displayed.

----End

Follow-up Procedure

After a configuration file is uploaded, the storage system automatically verifies the commands in the configuration file.

- If the verification is passed, the system displays the message **Configuration file uploaded successfully**. You can start the batch configuration.
- If the verification fails, the system displays an error message. You need to modify the configuration file.

4.13.2.4 Implementing Batch Configuration

This operation enables a storage system to automatically allocate storage resources based on the parameters in the configuration file to improve the storage resource configuration efficiency.

Prerequisites

A configuration file has been imported.

Context

- The batch configuration command can be executed only by the user who imports the configuration file.
- If the user logs out during the command execution, the storage system immediately stops the batch configuration.
- The storage system executes the commands included in the configuration file one by one and prompts whether each command is executed successfully.

Procedure

Step 1 Click **Execute** to implement batch configuration.

When the progress reaches 100%, the operation is successful.

NOTE

- During the execution, you can click **Stop** to stop the configuration.
- If the execution fails and pauses, you can click **Resume** to continue the configuration.

Step 2 Click **Close**.

----End

4.13.3 Accessing and Configuring OpenStack Cinder Driver

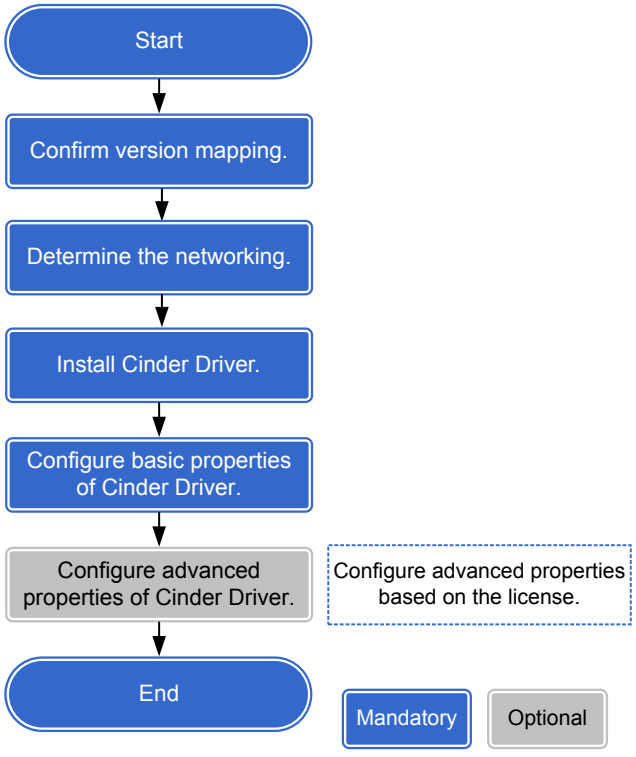
OpenStack Cinder Driver, a plug-in deployed on the OpenStack Cinder module, provides functions such as logical volume configuration for VMs in OpenStack. Cinder Driver supports both iSCSI and FC protocols.

Obtaining Cinder Driver

You can obtain the plug-in from Huawei OpenStack Driver repository (**https://github.com/Huawei/OpenStack_Driver**).

Configuration Process

Figure 4-4 Process for configuring Cinder Driver



For the specific configuration steps, see the configuration guide released with Cinder Driver.

4.13.4 In-band Management

4.13.4.1 Overview

Storage devices can be managed in either out-of-band or in-band mode.

For out-of-band management, the management control data of the storage device is transferred on a different link from the service data. In a typical connection, the maintenance terminal connects to the management network port or serial port of the storage device to manage the device, and the application server connects to the service network port of the storage device to transmit service data. The two links are independent of each other.

For in-band management, the management control data of the storage device is transferred on the same link as the service data. In a typical connection, the application server connects to the service network port of the storage device. With an in-band agent installed, the application server can manage the storage device while transmitting service data.

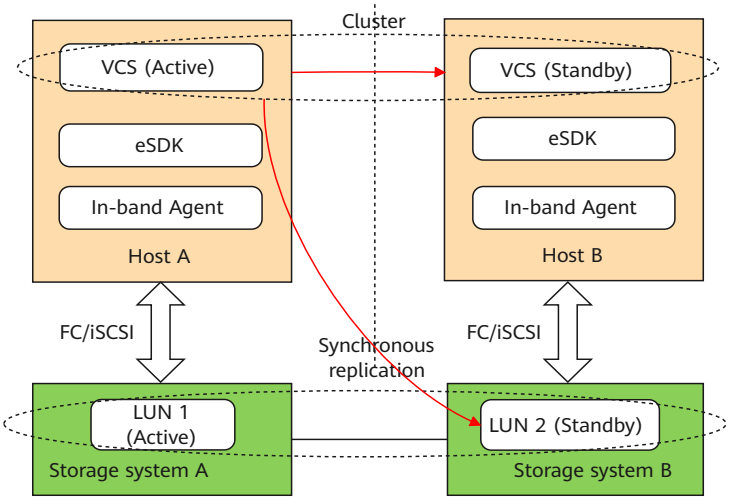
In-band management reduces the number of network cables because the management control data and service data are carried on the same link. In addition, in-band management enables application servers and storage devices to work together.

Application Scenario

In-band management applies to scenarios where the service network and the management network of storage systems cannot communicate with each other.

For example, a financial institution uses a solution that integrates service applications, Veritas Cluster Servers (VCSs) and active-active/synchronous replication. An active/standby switchover must be performed every half a year for DR drill. To do this, the VCSs should work with the active-active/synchronous replication feature of the storage system for active/standby switchover. However, according to the security specifications of the financial industry, the IP addresses of service servers must be isolated from the management IP addresses of the storage system. In this case, in-band management is applied to implement the active/standby switchover, as shown in **Figure 4-5**.

Figure 4-5 Typical application scenario



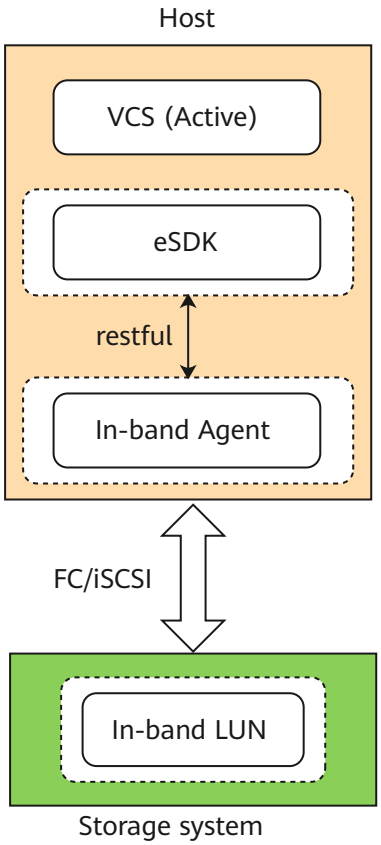
An ecosystem Software Development Kit (eSDK) and a VCS are installed on each host for ecosystem integration. The in-band agent manages in-band LUNs on the storage systems where synchronous remote replication is configured. The VCSs are in an active/standby mode. If the active VCS is faulty, an active/standby switchover is required. After the switchover, the standby VCS provides services to ensure service continuity.

During the active/standby switchover, the in-band management enables the storage systems to perform a primary/secondary switchover of remote replication.

Implementation Principles

Figure 4-6 shows how to connect to a VCS for in-band management.

Figure 4-6 Overall solution for connecting to a VCS



- The eSDK connects to a VCS on the host, converts VCS requests into RESTful interface messages, and sends them to the in-band agent.
- The in-band agent is an agent plug-in that converts messages delivered by the VCS into in-band commands, and encrypts and sends them to an in-band LUN of the storage system.
- After receiving the commands, the in-band LUN decrypts, authenticates, and executes the commands.

4.13.4.2 Configuring In-band Management

Installing Plug-ins on the Host

Specific plug-ins must be installed on the host to connect to third-party software. **Table 4-19** describes the plug-ins and application scenarios.

Table 4-19 Plug-ins on the host

Name	Application Scenario	Reference Manual
eSDK	Connecting to VCSs for in-band management	eSDK Enterprise Storage Plugins *XXX* User Guide (VCS) **NOTE** • *XXX* indicates the eSDK version that matches the current storage system. You can log in to Huawei technical support website (**https://support.huawei.com/enterprise/en/index.html**), enter the product model of the storage system in the search box, and select the suggested product model path to go to the documentation page of the desired product model. Search for and download the version mapping of the desired storage system version. • To obtain the user guide, visit **https://support.huawei.com/enterprise/en/index.html**, enter **eSDK Enterprise Storage Plugins** in the search box, select the suggested path to go to the documentation page, and search for the specific document.
OpenStack Cinder Driver	Connecting to OpenStack for in-band management	**OpenStack Cinder Driver Configuration Guide**

Installing the In-band Agent on the Host

The in-band agent is an agent plug-in that converts messages delivered by upper-layer services into in-band commands, and encrypts and sends them to in-band LUNs of the storage system. For details about how to install the in-band agent plug-in, see the *In-band Agent 1.0.RC1 Usage Guide*.

Configuring In-band LUNs

The storage system uses in-band LUNs for in-band management.

To configure in-band LUNs, perform the following steps:

Step 1 Run the **create lun name=? inband_type=IN_BAND_LUN storage_pool_id=?** command to create in-band LUNs.

NOTE

The storage system supports a maximum of 32 in-band LUNs, while two are recommended.

Step 2 Run the **create mapping general host_id=? lun_id_list=?** command to map the in-band LUNs to the host.

NOTE

- A maximum of two in-band LUNs can be mapped to a host. You are advised to map the same in-band LUN to different hosts.
- When OpenStack is connected for in-band management, the name of the host created on the storage system must be the same as that on the host. To obtain the host name, run the **hostname** command on the host. The host name is displayed in the command output. For details about how to create a host, see **4.7.1 Creating a Host**.

Step 3 The host scans for the LUNs. The method of LUN scanning varies depending on the operating system. For details, see section "Scanning LUNs on Hosts" in the *Host Connectivity Guide* specific to your operating system.

----End

Creating a Role

Storage systems use roles to control the object operation permission. A user of a specific role has the permission to operate the objects specified by the role.

To implement in-band management, you must log in to the system using a newly created in-band user and role to deliver requests.

To create a role, perform the following steps:

Step 1 Log in to DeviceManager and choose **Settings** > **User and Security** > **Users and Roles** > **Roles**.

Step 2 Click **Create**.

The **Create Role** page is displayed.

NOTE

The screenshot is for reference only and the actual displayed information may vary.

Step 3 Set the **Role Name**, **Owning Group**, and **Description**.

Table 4-20 describes related parameters.

Table 4-20 Role parameters

Parameter	Description
Role Name	Name of the role to be created. [Value range] • The name must be unique. • The value can contain only letters, digits, periods (.), underscores (_), and hyphens (-). • The name contains 1 to 63 characters.
Owning Group	There are two types of owning groups: **System group** and **vStore group**. • **System group**: A role of this group applies to the entire system view. • **vStore group**: A role of this group applies to the entire vStore view.
Description	Supplementary information about the role. [Value range] The description can be left blank or contain up to 255 characters.

Step 4 Set permission on objects. Possible values are **Read-only** and **Read and write**.

- **Read-only**: You can only query the objects.
- **Read and write**: You can add, delete, modify, and query the objects.

Step 5 Click **OK**.

Confirm your operation as prompted.

----End

Creating a User (System Group Role)

A super administrator can create different levels of users based on service requirements to restrict users' operations on a storage system, ensuring the stability of the service system and the security of service data.

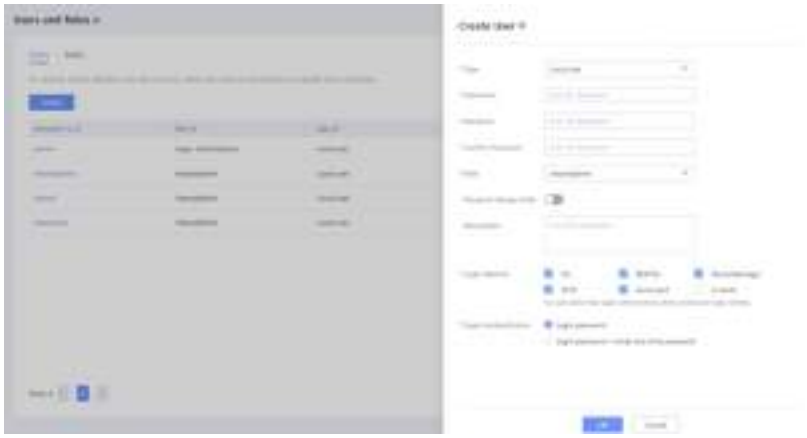
To create a user for in-band management, select **Local user** and set **Role** to the customized role created in **Creating a Role**.

If you set **Owning Group** to **System group** when creating a role, perform the following steps to create a user:

Step 1 Log in to DeviceManager and choose **Settings** > **User and Security** > **Users and Roles** > **Users**.

Step 2 Click **Create**.

The **Create User** page is displayed.



NOTE

The screenshot is for reference only and the actual displayed information may vary.

Step 3 Set user information.

Set **Type** to **Local user**, and configure the local user information. **Table 4-21** describes the parameters.

Table 4-21 User parameters

Parameter	Description
Type	User type. Select **Local user**.
Username	Name of the user to be created. [Value range] • The user name must be unique. • A user name can only contain letters, digits, and underscores (_) and must start with a letter. • The name contains 6 to 32 characters.

Parameter	Description
Password	Password of the user to be created. [Value range] • The password contains 8 to 16 characters. • The password must contain special characters !"#$ %&'()*+,-./:;<=>?@[\]^`{_|}~ and spaces. • The password must contain any two types of the uppercase letters, lowercase letters, and digits. • The password cannot contain three consecutive identical characters. • The password cannot be the same as the user name or the mirror writing of the user name.
Confirm Password	Password of the user to be created for confirmation. [Value range] • The password contains 8 to 16 characters. • The password must contain special characters !"#$ %&'()*+,-./:;<=>?@[\]^`{_|}~ and spaces. • The password must contain any two types of the uppercase letters, lowercase letters, and digits. • The password cannot contain three consecutive identical characters. • The password cannot be the same as the user name or the mirror writing of the user name.
Role	Role of the user to be created. Select the customized role created in **Creating a Role**.
Password Always Valid	Indicates whether to render the password always valid. If this function is enabled, the password is not restricted by the password validity period specified in the security policy. **NOTE** If **Password Always Valid** is enabled, you do not need to change the password upon the first login.
Description	Description of the user to be created. [Value range] The description can be left blank or contain up to 255 characters.
Login Method	Login method of the user to be created. The login method includes **CLI**, **RESTful**, **DeviceManager**, **SFTP**, **Serial port**, and **In-band**. **In-band** must be selected.

Parameter	Description
Login Authentication	Login authentication method of the user to be created. **NOTE** The in-band login method does not support the **Login password + email one-time password** authentication mode.

Step 4 Click **OK**.

Confirm your operation as prompted.

NOTE

After a user is created successfully, the **Execution Result** page is displayed. You can view details about the user on this page.

----End

Creating a User (vStore Group Role)

A super administrator can create different levels of users based on service requirements to restrict users' operations on a storage system, ensuring the stability of the service system and the security of service data.

To create a user for in-band management, select **Local user** and set **Role** to the customized role created in **Creating a Role**.

If you set **Owning Group** to **vStore group** when creating a role, perform the following steps to create a user:

Step 1 Log in to DeviceManager and choose **Services** > **vStore Service** > **vStores**.

Step 2 Click the name of the vStore. On the page that is displayed on the right, click the **User Management** tab and then **Create**.

The **Create User** page is displayed.

NOTE

The screenshot is for reference only and the actual displayed information may vary.

Step 3 Set user information.

Set **Type** to **Local user**, and configure the local user information. **Table 4-22** describes the parameters.

Table 4-22 User parameters

Parameter	Description
Type	User type. Select **Local user**.
Username	Name of the user to be created. [Value range] • The user name must be unique. • A user name can only contain letters, digits, and underscores (_) and must start with a letter. • The name contains 6 to 32 characters.
Password	Password of the user to be created. [Value range] • The password contains 8 to 16 characters. • The password must contain special characters !"#$ %&'()*+,-./:;<=>?@[\]^`{_|}~ and spaces. • The password must contain any two types of the uppercase letters, lowercase letters, and digits. • The password cannot contain three consecutive identical characters. • The password cannot be the same as the user name or the mirror writing of the user name.
Confirm Password	Password of the user to be created for confirmation. [Value range] • The password contains 8 to 16 characters. • The password must contain special characters !"#$ %&'()*+,-./:;<=>?@[\]^`{_|}~ and spaces. • The password must contain any two types of the uppercase letters, lowercase letters, and digits. • The password cannot contain three consecutive identical characters. • The password cannot be the same as the user name or the mirror writing of the user name.
Role	Role of the user to be created. Select the customized role created in **Creating a Role**.

Parameter	Description
Password Always Valid	Indicates whether to render the password always valid. If this function is enabled, the password is not restricted by the password validity period specified in the security policy. **NOTE** If **Password Always Valid** is enabled, you do not need to change the password upon the first login.
Description	Description of the user to be created. [Value range] The description can be left blank or contain up to 255 characters.
Login Method	Login method of the user to be created. The login method can be **RESTful**, **DeviceManager**, or **In-band**. **In-band** must be selected.
Login Authentication	Login authentication method of the user to be created. **NOTE** The in-band login method does not support the **Login password + email one-time password** authentication mode.

Step 4 Click **OK**.

Confirm your operation as prompted.

NOTE

After a user is created successfully, the **Execution Result** page is displayed. You can view details about the user on this page.

----End

Configuring an In-band Management Certificate

To implement in-band management, you must configure an in-band management certificate.

For details about how to configure in-band management certificates, see section "Managing Certificates" in *OceanStor 6.1 Security Configuration Guide*.

5 Managing Basic Storage Services

This chapter describes how to manage basic storage services on DeviceManager.

5.1 Managing the Service Network

This section describes how to manage the service network of the storage system.

5.1.1 Managing the FC Network

This section describes how to manage the FC network of the storage system.

5.1.1.1 Viewing FC Network Information

This operation enables you to view information about the FC network.

Procedure

Step 1 Choose **Services** > **Network** > **FC Network**.

Step 2 View information about the FC network in the function pane. **Table 5-1** describes the parameters.

Table 5-1 FC network parameters

Parameter	Description
Name	Name of an FC port.
Location	Location of an FC port.
ID	ID of an FC port.
Health Status	Health status of an FC port. • **Unknown**: The system fails to query the port status. • **Normal**: Functions and running performance of the port are normal and without error. • **Bit errors found**: Bit errors occur when the port transmits data. • **Faulty**: The port is functioning improperly and cannot work normally.
Running Status	Running status of an FC port. • **Unknown**: The system fails to query the port status. • **Link up**: A cable is connected to the port. • **Link down**: No cable is connected to the port.
WWPN	WWPN of an FC port.
Working Rate (Gbit/s)	Data transmission rate of an FC port.
Max. Working Rate (Gbit/s)	Maximum data transmission rate of an FC port.
Operation Mode	Operation mode of an FC port.
Port State	Isolation status of an FC port. Possible values are **Enabled** and **Disabled**. A port cannot be used if its **Port State** is **Disabled**.
Initiators	Number of initiators connected to an FC port.
Port Protocol	Protocol used by an FC port.
Immediate Data	Indicates whether the immediate data function is enabled for the FC port.

NOTE

Click the name of a port to view its details, including **Summary**, **Initiators**, and **Owning Port Groups**.

----End

5.1.1.2 Modifying an FC Port

When the networking mode between a storage device and an application server changes, modify the parameters of the FC port to ensure proper communication between them.

Procedure

Step 1 Choose **Services** > **Network** > **FC Network**.

Step 2 Click the name of the desired FC port. In the upper right corner of the page that is displayed, click **Modify**.

The **Modify** page is displayed.

Step 3 In **Configured Rate (Gbit/s)**, select a data transmission rate for the FC port.

NOTICE

- The FC port must have the same rate and mode as the HBA port on the application server to prevent a communication failure.
- When two storage systems are interconnected by FC ports, ensure that the rates and modes of the FC ports are the same on the two storage systems. Using different rates or modes may cause communication failure.

The rate of an FC port can be 2 Gbit/s, 4 Gbit/s, 8 Gbit/s, 16 Gbit/s, 32 Gbit/s, or self-adaptive. Select a correct value after obtaining necessary information.

NOTE

- If the maximum rate of the port is 4 Gbit/s, you can set the value to 2 Gbit/s or 4 Gbit/s.
- If the maximum rate of the port is 8 Gbit/s, you can set the value to 2 Gbit/s, 4 Gbit/s, or 8 Gbit/s.
- If the maximum rate of the port is 16 Gbit/s, you can set the value to 4 Gbit/s, 8 Gbit/s, or 16 Gbit/s.
- If the maximum rate of the port is 32 Gbit/s, you can set the value to 8 Gbit/s, 16 Gbit/s, or 32 Gbit/s.
- If the value is set to **Self-adaptive**, the interconnected FC ports negotiate the rate automatically. If the negotiated rates do not match, modify the rate manually.

Step 4 In **Port Protocol**, select **FC-SCSI** or **FC-NVMe**.

Step 5 Determine whether to enable **Immediate Data**. In scenarios where FC replication links are used to transmit service data between storage arrays, the **Immediate Data** function can improve the data transmission performance. You are advised to enable this function.

Step 6 Click **OK**.

----End

5.1.1.3 Viewing Bit Error Statistics

A port's bit error statistics reflect the data transmission efficiency of this port. A high bit error rate compromises the read and write performance of the application server using this port.

Procedure

Step 1 Choose **Services** > **Network** > **FC Network**.

Step 2 Click **Bit Error Statistics**.

The **Bit Error Statistics** page is displayed on the right.

Step 3 Query the bit error statistics of the Fibre Channel ports.

NOTE

You can click **Clear** to clear bit error statistics.

----End

5.1.2 Managing the Ethernet Network

This section describes how to manage the Ethernet network of the storage system.

5.1.2.1 Managing Ethernet Ports

This section describes how to manage Ethernet ports.

5.1.2.1.1 Viewing Ethernet Ports

This operation enables you to view information about Ethernet ports.

Procedure

Step 1 Choose **Services** > **Network** > **Ethernet Network** > **Ethernet Ports**.

Step 2 View information about Ethernet ports in the function pane. **Table 5-2** describes the parameters.

Table 5-2 Ethernet port parameters

Parameter	Description
Name	Name of an Ethernet port.
Location	Location of an Ethernet port.
ID	ID of an Ethernet port.

Parameter	Description
Health Status	Health status of an Ethernet port. • **Unknown**: The system fails to query the port status. • **Normal**: Functions and running performance of the Ethernet port are normal and without error. • **Bit errors found**: Bit errors occur when the port transmits data. • **Faulty**: The Ethernet port is functioning improperly and cannot work normally.
Running Status	Running status of an Ethernet port. • **Unknown**: The system fails to query the port status. • **Link up**: A cable is connected to the port. • **Link down**: No cable is connected to the port. • **To be recovered**: For a 4 U device, if the owning controller of a port is faulty, the running status of the port is **To be recovered**.
MAC Address	MAC address of an Ethernet port.
IPv4 Address/ Subnet Mask	IPv4 address and subnet mask of an Ethernet port.
IPv6 Address/Prefix	IPv6 address and prefix length of an Ethernet port.
Working Rate (Gbit/s)	Data transmission rate of an Ethernet port.
Max. Working Rate (Gbit/s)	Maximum data transmission rate of an Ethernet port.
MTU (Bytes)	Maximum size of a data packet that can be transferred between an Ethernet port and an application server.
Bond Name	Bond name of an Ethernet port.
Logical Type	Logical type of an Ethernet port. Possible values are **Front-end port**, **Management port**, **Maintenance port**, **Expansion port**, **Scale-out interconnect port**, **Container front-end port**, and **Container back-end port**.
Port State	State of an Ethernet port. An Ethernet port disconnects after it is disabled.
Initiators	Number of initiators connected to an Ethernet port.

NOTE

You can click the name of an Ethernet port to view its details.

----End

5.1.2.1.2 Viewing Bit Error Statistics

A port's bit error statistics reflect the data transmission efficiency of this port. A high bit error rate compromises the read and write performance of the application server using this port.

Procedure

Step 1 Choose **Services** > **Network** > **Ethernet Network** > **Ethernet Ports**.

Step 2 Click **Bit Error Statistics**.

The **Bit Error Statistics** page is displayed on the right.

Step 3 Query the bit error statistics of the Ethernet ports.

NOTE

You can click **Clear** to clear bit error statistics.

----End

5.1.2.1.3 Configuring LLDP

By configuring LLDP on devices, you can obtain detailed information about the network devices, such as topology and interface status.

Prerequisites

- The health status of the storage system is normal.
- The host or switch supports and has enabled the LLDP.

Context

- The Link Layer Discovery Protocol (LLDP) is a standard Layer 2 topology discovery protocol defined in IEEE 802.1ab. LLDP allows a device to send local management information such as management IP address, device ID, and port ID to neighbors. Neighbors save the received information in their management information bases (MIBs). The network management system (NMS) can search required information in MIBs to determine link status.
- If the host or switch connected to the front-end service port of the storage system also supports the LLDP, the host or switch can discover the port information of the storage system through the LLDP.
- For Ethernet ports on a 4 U device, only their owning controller sends LLDP packets. In addition, the peer device only displays the neighbor information of the owning controller. If the owning controller of the port is faulty, the port does not send LLDP packets.

Procedure

Step 1 In developer mode, run the **change system lldp working_mode=?** command to change the LLDP working mode.

In the preceding command, the default value of the **working_mode** field is **lldp_mode_disable**. Its value can be any of the following:

1. **lldp_mode_disable**: indicates that LLDP packets can neither be sent nor received.
2. **lldp_mode_tx**: indicates that LLDP packets can only be sent.
3. **lldp_mode_rx**: indicates that LLDP packets can only be received.
4. **lldp_mode_txrx**: indicates that LLDP packets can be sent and received.

Example:

```
developer:/>change system lldp working_mode=lldp_mode_txrx
WARNING: You are about to change the LLDP working mode.
After the working mode of the LLDP protocol is changed, the host or switch may discover the array port information through the LLDP protocol, and the host or switch information may also be discovered by the array through the LLDP protocol.
Suggestion: Before performing this operation, ensure that you want to perform this operation.
Have you read warning message carefully?(y/n)y
Are you sure you really want to perform the operation?(y/n)y
Command executed successfully.
```

NOTE

You can run the **change user_mode current_mode user_mode=developer** command to enter the developer mode.

Step 2 In developer mode, run the **show system lldp** command to check whether the LLDP working mode is successfully changed.

Example:

```
developer:/>show system lldp
  Working Mode : lldp_mode_txrx
```

----End

5.1.2.2 Managing Bond Ports

This section describes how to manage bond ports.

5.1.2.2.1 Viewing Bond Ports

This operation enables you to view information about bond ports.

Procedure

Step 1 Choose **Services** > **Network** > **Ethernet Network** > **Bond Ports**.

Step 2 View information about bond ports in the function pane. **Table 5-3** describes the parameters.

Table 5-3 Bond port parameters

Parameter	Description
Name	Name of a bond port.
ID	ID of a bond port.

Parameter	Description
Health Status	Health status of a bond port. • **Unknown**: The system fails to query the port status. • **Normal**: Functions and running performance of the port are normal and without error. • **Faulty**: The port is functioning improperly and cannot work normally. • **Partially damaged**: The bond port has a faulty member port.
Running Status	Running status of a bond port. • **Unknown**: The system fails to query the port status. • **Link up**: A cable is connected to a member port. • **Link down**: No cable is connected to a member port. • **To be recovered**: For a 4 U device, if the owning controller of a port is faulty, the running status of the port is **To be recovered**.
IPv4 Address/ Subnet Mask	IPv4 address and subnet mask of a bond port.
IPv6 Address/Prefix	IPv6 address and prefix length of a bond port.
MTU (Bytes)	Maximum size of a data packet that can be transferred between a bond port and an application server.
Ports	Number of ports bonded to a bond port.
Initiators	Number of initiators connected to a bond port.

NOTE

You can click the name of a bond port to view its details and modify it.

----End

5.1.2.2.2 Modifying a Bond Port

This operation enables you to modify a bond port.

Prerequisites

- A bond port has been created.
- After the MTU is changed to a non-default value, ensure that the MTU is the same as that of the peer device (switch or network adapter).

Procedure

Step 1 Choose **Services** > **Network** > **Ethernet Network** > **Bond Ports**.

Step 2 Click **More** on the right of the desired bond port and select **Modify**.

The **Modify** page is displayed.

NOTE

Alternatively, click the name of the desired port. In the upper right corner of the page that is displayed, select **Modify** from the **Operation** drop-down list.

Step 3 Set **MTU (Bytes)** of the bond port. The value ranges from 1280 to 9000.

Step 4 In **Logical Port**, specify **Name**, **IP Address**, and **Subnet Mask/Prefix** of a logical port bonded to the bond port.

NOTE

You can click + to add more ports to the bond port.

Step 5 Click **OK**.

----End

5.1.2.2.3 Deleting a Bond Port

This operation enables you to delete a bond port.

Prerequisites

- All services on the bond port to be deleted have been stopped.
- No VLAN or logical port is created for the bond port to be deleted.

Precautions

After a bond port is deleted, the IP addresses of the bonded Ethernet ports are cleared. You must reset IP addresses for the Ethernet ports if needed.

Procedure

Step 1 Choose **Services** > **Network** > **Ethernet Network** > **Bond Ports**.

Step 2 Select one or more desired bond ports and click **Delete**.

NOTE

You can also click **More** on the right of a desired bond port and select **Delete**.

Confirm your operation as prompted.

----End

5.1.2.3 Managing VLANs

This section describes how to add Ethernet ports or bond ports in the storage system to multiple independent VLANs. You can configure different services in different VLANs to ensure the security and reliability of service data.

5.1.2.3.1 Viewing VLANs

This operation enables you to view information about created VLANs.

Procedure

Step 1 Choose **Services** > **Network** > **Ethernet Network** > **VLANs**.

Step 2 View information about VLANs in the function pane. **Table 5-4** describes the parameters.

Table 5-4 VLAN parameters

Parameter	Description
Name	Name of a VLAN.
ID	ID of a VLAN.
Running Status	Running status of a VLAN. • **Unknown**: The system fails to query the VLAN status. • **Link up**: The running status of the home port of a VLAN is link up. • **Link down**: The running status of the home port of a VLAN is link down. • **To be recovered**: When the home port of a VLAN is in the **To be recovered** state, the running status of the VLAN is refreshed to **To be recovered**.
MTU (Bytes)	Maximum transmission unit of a VLAN.

----End

5.1.2.3.2 Modifying a VLAN

This operation enables you to modify a VLAN.

Procedure

Step 1 Choose **Services** > **Network** > **Ethernet Network** > **VLANs**.

Step 2 Click **More** on the right of the desired VLAN and select **Modify**.

The **Modify VLAN** page is displayed.

Step 3 Set **MTU (Bytes)**.

Step 4 Click **OK**.

----End

5.1.2.3.3 Deleting a VLAN

This operation enables you to delete an unnecessary VLAN.

Prerequisites

All services in the VLAN to be deleted have been stopped.

Procedure

Step 1 Choose **Services** > **Network** > **Ethernet Network** > **VLANs**.

Step 2 Select one or more desired VLANs and click **Delete**.

NOTE

You can also click **More** on the right of a desired VLAN and select **Delete**.

Confirm your operation as prompted.

----End

5.1.3 Managing Logical Ports

This section describes how to manage logical ports. A logical port is created based on an Ethernet port, a bond port, a VLAN, or a RoCE port.

5.1.3.1 Viewing Logical Ports

This section describes how to view information about logical ports.

Procedure

Step 1 Choose **Services** > **Network** > **Logical Ports**.

Step 2 View information about logical ports in the function pane. **Table 5-5** describes the parameters.

Table 5-5 Logical port parameters

Parameter	Description
Name	Name of a logical port.
ID	ID of a logical port.
Owning vStore	Name of the vStore to which a logical port belongs.
vStore ID	ID of the vStore to which a logical port belongs.

Parameter	Description
Running Status	Running status of a logical port. • **Unknown**: The system fails to query the port status. • **Link up**: The running status of the home port of a logical port is link up. • **Link down**: The running status of the home port of a logical port is link down. • **Standby**: In a HyperMetro scenario, when a logical port works at the owning site of the primary or secondary end, the running status of the logical port at the non-owning site of the peer end is **Standby**. • **To be recovered**: When the home port of a logical port is in the **To be recovered** state or a logical port used for the file service fails to be failed over, the running status of the logical port changes to **To be recovered**.
Activation Status	Indicates whether a logical port is activated.
Role	Role of a logical port.
Data Protocol	Data protocol of a logical port. In block service scenarios, the data protocol of logical ports can be **iSCSI** or **NVMe over RoCE**.
IP Address	IP address of a logical port.
Subnet Mask/ Prefix	Subnet mask of a logical port's IPv4 address or prefix length of a logical port's IPv6 address.
Gateway	Gateway of a logical port's IP address.
Home Port/ Current Port	Home port and current port of a logical port.
Home Controller/ Current Controller	Home controller and current controller of a logical port.
Failover Group	In block service scenarios, the value is --.
Owning Site	Site to which the logical port belongs. Site to which the logical port in the HyperMetro vStore pair that processes service access belongs.

NOTE

You can click the name of a logical port to view its details and manage it.

----End

5.1.3.2 Modifying a Logical Port

This section describes how to modify a logical port.

Context

For block services, the data protocol of the logical port is iSCSI or NVMe.

Procedure

Step 1 Choose **Services** > **Network** > **Logical Ports**.

Step 2 Click **More** on the right of the desired logical port and select **Modify**.

The **Modify Logical Port** page is displayed.

Step 3 Set the parameters listed in **Table 5-6**.

Table 5-6 Logical port parameters

Parameter	Description
Name	Name of the logical port. The name must: • Be unique. • Contain only letters, digits, underscores (_), hyphens (-), and periods (.). • Contain 1 to 255 characters.
IP Address Type	IP address type of the logical port, which can be **IPv4** or **IPv6**.
IP Address	IPv4 or IPv6 address of the logical port.
Subnet Mask	Subnet mask of the logical port's IPv4 address. **NOTE** This parameter is available only when **IP Address Type** is set to **IPv4**.
Prefix	Prefix length of the logical port's IPv6 address. **NOTE** This parameter is available only when **IP Address Type** is set to **IPv6**.
Gateway	Gateway of the logical port's IP address.

Step 4 Click **OK**.

----End

5.1.3.3 Managing Routes

This section describes how to configure route information for a logical port.

Prerequisites

A logical port has been configured with an IP address.

Procedure

Step 1 Choose **Services** > **Network** > **Logical Ports**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Select the desired logical port and click **Manage Route**.

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

NOTE

Alternatively, perform either of the following operations to go to the **Manage Route** page:

- Click **More** on the right of the desired logical port and select **Manage Route**.
- Click the name of the desired logical port. In the upper right corner of the page that is displayed, click **Manage Route** from the **Operation** drop-down list.

Step 4 Configure the route information for the logical port.

1. In the **IP Address** drop-down list, select the IP address of the logical port for which you want to add a route.
2. Click **Add**.
3. Set the parameters listed in **Table 5-7**.

Table 5-7 Route parameters

Parameter	Description
Type	Three types of routes are available: – **Default route** A route through which data is forwarded by default if no preferred route is available. The destination address and mask (IPv4) or prefix (IPv6) of the default route are automatically set to 0. To use this option, you only need to add a gateway. – **Host route** A route to a host. The destination mask (IPv4) or prefix (IPv6) of the host route are automatically set to 255.255.255.255 or 128. To use this option, you only need to add the destination address and gateway. – **Network segment route** A route to a network segment. You must add the destination address, destination mask (IPv4) or prefix (IPv6), and gateway.
Destination Address	IPv4 address, IPv6 address, or network segment of the destination service network port on the application server or destination logical port on another storage system.
Subnet Mask/ Prefix	Subnet mask of the IPv4 address or prefix of the IPv6 address for the destination service network port on the application server or destination logical port on another storage system.

Parameter	Description
Gateway	Gateway where the local logical port's IP address resides. **NOTE** The IP address of the gateway must be different from all internal heartbeat IP addresses. Otherwise, routing will fail.

4. Click ✓. The route information is added to the list.

   NOTE

   Click 🗑 on the right of a desired route to delete it.

Step 5 Click **Close**.

----End

5.1.3.4 Failing Back a Logical Port

After a fault of the home port is rectified, you can fail back services to the home port.

Procedure

Step 1 Choose **Services** > **Network** > **Logical Ports**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Select the desired logical port and click **Fail Back**.

NOTE

Alternatively, perform either of the following operations to fail back a logical port:

- Click **More** on the right of the desired logical port, and select **Fail Back**.
- Click the name of the desired logical port. In the upper right corner of the page that is displayed, click **Fail Back** from the **Operation** drop-down list.

----End

5.1.3.5 Deleting a Logical Port

This section describes how to delete a logical port that is no longer used.

Prerequisites

All services on the logical port to be deleted have been stopped.

Procedure

Step 1 Choose **Services** > **Network** > **Logical Ports**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Select one or more desired logical ports and click **Delete**.

NOTE

Alternatively, perform either of the following operations to delete a logical port:

- Click **More** on the right of the desired logical port, and select **Delete**.
- Click the name of the desired logical port. In the upper right corner of the page that is displayed, click **Delete** from the **Operation** drop-down list.

Confirm your operation as prompted.

----End

5.1.4 Managing the RoCE Network

This section describes how to manage the RoCE network of the storage system.

5.1.4.1 Managing RoCE Ports

RoCE ports are used to connect a storage device with application servers, allowing them to communicate with each other over RoCE networks. You can view or modify parameters of RoCE ports as required.

5.1.4.1.1 Viewing RoCE Ports

This operation enables you to view information about RoCE ports.

Procedure

Step 1 Choose **Services** > **Network** > **RoCE Network** > **RoCE Ports**.

Step 2 View information about RoCE ports in the function pane. **Table 5-8** describes the parameters.

Table 5-8 RoCE port parameters

Parameter	Description
Name	Name of a RoCE port.
Location	Location of a RoCE port.
ID	ID of a RoCE port.
Health Status	Health status of a RoCE port. • **Unknown**: The system fails to query the port status. • **Normal**: Functions and running performance of the port are normal and without error. • **Bit errors found**: Bit errors occur when the port transmits data. • **Faulty**: The port is functioning improperly and cannot work normally.

Parameter	Description
Running Status	Running status of a RoCE port. • **Unknown**: The system fails to query the port status. • **Link up**: A cable is connected to the port. • **Link down**: No cable is connected to the port. • **To be recovered**: For a 4 U device, if the owning controller of a port is faulty, the running status of the port is **To be recovered**.
MAC Address	MAC address of a RoCE port.
Working Rate (Gbit/s)	Data transmission rate of a RoCE port.
Max. Working Rate (Gbit/s)	Maximum data transmission rate of a RoCE port.
MTU (Bytes)	Maximum size of a data packet that can be transferred between a RoCE port and an application server.
Logical Type	Logical type of a RoCE port. Possible values are **Management port**, **Maintenance port**, **Expansion port**, **Scale-out interconnection port**, **Container front-end port**, and **Container back-end port**.
Port State	State of a RoCE port. A RoCE port will be disconnected after it is disabled.
SNSD	State of Storage Network Smart Discovery (SNSD). When **SNSD** of a RoCE port is set to **Enabled**, hosts detect the state changes of all logical ports of the RoCE port and determine whether to automatically establish or cancel connections based on logical port states. **NOTE** • **SNSD** has enterprise or standard modes. When **SNSD** is switched from **Disabled** to **Enabled**, the standard mode is used by default. To use the enterprise mode, run the **change port eth_snsd_switch** command on the CLI. For details about this command, see the command reference specific to your product model. • Only 6.1.5 and later versions support the enterprise mode.
Initiators	Number of initiators connected to a RoCE port.
Trust Mode	Trust mode of a RoCE port. Possible values are **PCP** and **DSCP**. **NOTE** Only 6.1.5 and later versions support this parameter.

NOTE

You can click the name of a port to view its details, including **Summary**, **Initiators**, **Owning Port Groups**, and **VLANs**.

----End

5.1.4.1.2 Modifying a RoCE Port

When the networking mode between a storage device and an application server changes, modify the parameters of the RoCE port to ensure proper communication between them.

Procedure

Step 1 Choose **Services** > **Network** > **RoCE Network** > **RoCE Ports**.

Step 2 Click the name of the desired RoCE port. In the upper right corner of the page that is displayed, click **Modify**.

The **Modify** page is displayed.

Step 3 In **Working Mode**, select a working mode for the RoCE port.

NOTE

- This parameter may be invalid for some interface modules.
- The forward error correction (FEC) technology is used. With this technology, a sender sends data with a certain redundancy error correction code, and a receiver performs error detection on the received data according to the redundancy error correction code. If an error is detected, the receiver can correct the error.
- The working mode varies according to the port type. The value can be **Self-adaptive**, **RSFEC**, **NOFEC**, or **BASEFEC**.
- When the working mode of a port is set to **Self-adaptive**, it can automatically match the FEC mode of the peer network device (such as a NIC or switch). In this case, if the peer network device also has the self-adaptive capability enabled, the link negotiation time may be prolonged.
- When the working mode of a port is set to **RSFEC**, **NOFEC**, or **BASEFEC**, ensure that the mode matches the FEC mode of the peer network device. Before setting the working mode, you are advised to confirm it by referring to the product description of the peer network device.

Step 4 In **MTU (Bytes)**, enter a maximum transmission unit (MTU) for the packets transmitted between the RoCE port and the application server.

Step 5 Determine whether to enable **SNSD**. When **SNSD** of a RoCE port is set to **Enabled**, hosts detect the state changes of all logical ports of the RoCE port and determine whether to automatically establish or cancel connections based on logical port states.

NOTE

- **SNSD** has enterprise or standard modes. When **SNSD** is switched from **Disabled** to **Enabled**, the standard mode is used by default. To use the enterprise mode, run the **change port eth_snsd_switch** command on the CLI. For details about this command, see the command reference specific to your product model.
- Only 6.1.5 and later versions support the enterprise mode.

Step 6 Set **Trust Mode** of the port, which can be **PCP** or **DSCP**.

NOTE

- The default trust mode is **PCP**. If you want to create a logical port directly on the RoCE port, select **DSCP**.
- Only 6.1.5 and later versions can set the trust mode of a port.

Step 7 Click **OK**.

----End

5.1.4.1.3 Batch Setting SNSD

This section describes how to enable or disable SNSD for RoCE ports in a batch.

Procedure

Step 1 Choose **Services** > **Network** > **RoCE Network** > **RoCE Ports**.

Step 2 Select desired RoCE ports and click **Batch Set SNSD**. Then select **Batch Enable SNSD** or **Batch Disable SNSD**.

NOTE

- When **SNSD** of a RoCE port is set to **Enabled**, hosts detect the state changes of all logical ports of the RoCE port and determine whether to automatically establish or cancel connections based on logical port states.
- **SNSD** has enterprise or standard modes. When **SNSD** is switched from **Disabled** to **Enabled**, the standard mode is used by default. To use the enterprise mode, run the **change port eth_snsd_switch** command on the CLI. For details about this command, see the command reference specific to your product model.
- Only 6.1.5 and later versions support the enterprise mode.

Confirm your operation as prompted.

----End

5.1.4.1.4 Viewing Bit Error Statistics

A port's bit error statistics reflect the data transmission efficiency of this port. A high bit error rate compromises the read and write performance of the application server using the port.

Procedure

Step 1 Choose **Services** > **Network** > **RoCE Network** > **RoCE Ports**.

Step 2 Click **Bit Error Statistics**.

The **Bit Error Statistics** page is displayed on the right.

Step 3 Query the bit error statistics of the RoCE ports.

NOTE

You can click **Clear** to clear bit error statistics.

----End

5.1.4.2 Managing VLANs

This section describes how to add RoCE ports in the storage system to multiple independent VLANs. You can configure different services in different VLANs to ensure the security and reliability of service data.

5.1.4.2.1 Creating a VLAN

This section describes how to create a VLAN for each RoCE port in specific scenarios.

Context

Determine whether a VLAN is needed based on the following information:

- In 6.1.3 and earlier versions, you must create a VLAN for each RoCE port.
- In versions later than 6.1.3, if **Trust Mode** of a RoCE port is **PCP**, you must create a VLAN for each RoCE port.
- In versions later than 6.1.3, if **Trust Mode** of a RoCE port is **DSCP**, you can choose to create a logical port based on the RoCE port or VLAN. In this case, determine whether a VLAN is needed based on your service plan.

  Choose **Services > Network > RoCE Network** and click the name of a RoCE port to check its trust mode.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Services** > **Network** > **RoCE Network** > **VLANs**.

Step 3 Click **Create**.

The **Create VLAN** page is displayed on the right.

Step 4 In the **Home Port** list, select a home port.

Step 5 In **ID**, specify the ID of a VLAN, and then click **Add**.

NOTE

- The same VLAN IDs must be configured for the interconnected replication ports on the local device, remote device, and switch.
- The VLAN ID ranges from 1 to 4094. You can specify multiple VLAN IDs one by one or in a batch. When creating multiple VLANs and specifying VLAN IDs in a batch, the VLAN IDs are in the following format: Start VLAN ID-End VLAN ID.
- To delete a VLAN ID, click × next to it.

Step 6 Click **OK**.

----End

5.1.4.2.2 Viewing VLANs

This operation enables you to view information about created VLANs.

Procedure

Step 1 Choose **Services** > **Network** > **RoCE Network** > **VLANs**.

Step 2 View information about VLANs in the function pane. **Table 5-9** describes the parameters.

Table 5-9 VLAN parameters

Parameter	Description
Name	Name of a VLAN.
ID	ID of a VLAN.
Running Status	Running status of a VLAN. • **Unknown**: The system fails to query the VLAN status. • **Link up**: The running status of the home port of a VLAN is link up. • **Link down**: The running status of the home port of a VLAN is link down. • **To be recovered**: When the home port of a VLAN is in the **To be recovered** state, the running status of the VLAN is refreshed to **To be recovered**.
MTU (Bytes)	Maximum transmission unit of a VLAN.

----End

5.1.4.2.3 Modifying a VLAN

This operation enables you to modify a VLAN.

Procedure

Step 1 Choose **Services** > **Network** > **RoCE Network** > **VLANs**.

Step 2 Click **More** on the right of the desired VLAN and select **Modify**.

The **Modify VLAN** page is displayed.

Step 3 Set **MTU (Bytes)**.

Step 4 Click **OK**.

----End

5.1.4.2.4 Deleting a VLAN

This operation enables you to delete an unnecessary VLAN.

Prerequisites

All services in the VLAN to be deleted have been stopped.

Procedure

Step 1 Choose **Services** > **Network** > **RoCE Network** > **VLANs**.

Step 2 Select one or more desired VLANs and click **Delete**.

NOTE

You can also click **More** on the right of a desired VLAN and select **Delete**.

Confirm your operation as prompted.

----End

5.2 Managing Ports on Controller Enclosures

You can manage controller enclosures and their components including controllers and interface modules, as well as configure parameters for these components.

NOTE

Some device models may not support some interface modules. For details, visit **Specifications Query**.

5.2.1 Managing Ethernet Ports

This section describes how to manage Ethernet ports.

5.2.1.1 Viewing Ethernet Ports

Ethernet ports are used to connect storage devices to application servers through Ethernet links. This section describes how to view information about an Ethernet port on a storage device.

Prerequisites

An Ethernet interface module has been properly installed on a controller.

Procedure

Step 1 Choose **System** > **Hardware** > **Devices**.

Step 2 Click the controller enclosure where the desired Ethernet port resides.

Step 3 Click  to switch to the rear view of the controller enclosure.

Step 4 Click the desired Ethernet port.

NOTE

Alternatively, you can choose **Services** > **Network** > **Ethernet Network** > **Ethernet Ports**.

Step 5 View the Ethernet port information in the displayed **Ethernet Port:** *Port location* page on the right or the table in the lower function pane.

Table 5-10 describes the parameters.

Table 5-10 Ethernet port parameters

Parameter	Description
Name	Name of the Ethernet port.
Location	Location of the Ethernet port.
ID	ID of the Ethernet port.
Health Status	Health status of the Ethernet port. • **Unknown**: The system fails to query the port status. • **Normal**: The Ethernet port is functioning properly. • **Bit errors found**: Bit errors occur when the port transmits data. • **Faulty**: The Ethernet port is functioning improperly.
Running Status	Running status of the Ethernet port. • **Unknown**: The system fails to query the port status. • **Link up**: A cable is connected to the port. • **Link down**: No cable is connected to the port. • **To be recovered**: For a 4 U device, if the owning controller of a port is faulty, the running status of the port is **To be recovered**.
MAC Address	MAC address of the Ethernet port.
IPv4 Address/ Subnet Mask	IPv4 address and subnet mask of the Ethernet port.
IPv6 Address/ Prefix	IPv6 address and prefix length of the Ethernet port.
Working Rate (Gbit/s)	Data transmission rate of the Ethernet port.
Max. Working Rate (Gbit/s)	Maximum data transmission rate of the Ethernet port.
MTU (Bytes)	Maximum size of a data packet that can be transferred between the Ethernet port and the application server.
Bond Name	Bond name of the Ethernet port.
Logical Type	Logical type of the Ethernet port. Possible values are **Front-end port**, **Management port**, **Maintenance port**, **Expansion port**, **Scale-out interconnect port**, **Container front-end port**, and **Container back-end port**.
Port State	State of the Ethernet port. An Ethernet port will be disconnected after it is disabled.
Initiators	Number of initiators connected to the Ethernet port.

Parameter	Description
Working Mode	Working mode of the Ethernet port. **NOTE** • This parameter may be invalid for some interface modules. • The forward error correction (FEC) technology is used. With this technology, a sender sends data with a certain redundancy error correction code, and a receiver performs error detection on the received data according to the redundancy error correction code. If an error is detected, the receiver can correct the error. • The FEC mode can be RSFEC, NOFEC, or BASEFEC. RSFEC stands for Reed Solomon Forward Error Correction, BASEFEC stands for the basic FEC mode, and NOFEC stands for no FEC. For details about FEC, see related IEEE 802.3bj documents. • The working mode varies according to the port type. The value can be **Self-adaptive**, **RSFEC**, **NOFEC**, **BASEFEC**, or **Autonegotiation**. • When the port working mode is set to self-adaptive, the interface card attempts to match the FEC mode and auto-negotiation switch of the peer network device (NIC or switch) until the operation succeeds. In this case, if the self-adaptive function is also enabled on the peer network device, the link negotiation time may be prolonged. • When the working mode of a port is set to **RSFEC**, **NOFEC**, or **BASEFEC**, ensure that the mode matches the FEC mode of the peer network device. Before setting the working mode, you are advised to confirm it by referring to the product documentation of the peer network device. • When the port working mode is set to auto-negotiation, the storage device and the peer network device negotiate the rate, network flow control, and FEC capability to achieve communication.
iSCSI Target Name	Target name of the iSCSI network where the Ethernet port resides.

NOTE

- Click the **Initiators** or **Owning Port Groups** tab to view the initiators or owning port groups of the Ethernet port.
- If one or more bond ports have been created for the Ethernet port, you can click the **Bond Ports** tab to view details of the bond ports.

----End

5.2.1.2 Modifying an Ethernet Port

When the networking mode between a storage device and an application server changes, modify the parameters of Ethernet ports to ensure proper communication between them.

Precautions

- Change the IP address of an Ethernet port only when necessary. Before changing the IP address of an Ethernet port, either ensure that redundant connections are available or stop services carried by this port.
- The IP address of an Ethernet port must be on a different network segment from the internal heartbeat IP addresses.

  The default IP addresses of internal heartbeat on a dual-controller storage system are 127.127.127.10 and 127.127.127.11, and those on a four-controller storage system are 127.127.127.10, 127.127.127.11, 127.127.127.12, and 127.127.127.13.
- Internal heartbeat links are established between controllers for the controllers to detect each other's working status. Heartbeat links do not require separate cable connections. The internal heartbeat IP addresses have been assigned before delivery and cannot be changed.
- The IP address of an Ethernet port must not be in the same network segment as that of a management network port.
- The IP address of an Ethernet port must not be in the same network segment as that of a maintenance network port. The default IP address of the maintenance network port must fall within the **172.31.***XXX.XXX* segment.
- If an Ethernet port connects to an application server, the IP address of the Ethernet port must be in the same network segment as that of the service network port on the application server. If an Ethernet port connects to another storage device, the IP address of the Ethernet port must be in the same network segment as that of the peer Ethernet port on the other storage device. If available IP addresses are insufficient for a network segment for which you want to add an IP address, add routes.
- After Ethernet ports are bonded, their properties cannot be modified.

Procedure

Step 1 Choose **System** > **Hardware** > **Devices**.

Step 2 Click the controller enclosure where the desired Ethernet port resides.

Step 3 Click  to switch to the rear view.

Step 4 Click the desired Ethernet port.

The **Ethernet Port:** *Port location* page is displayed on the right.

Step 5 Modify the Ethernet port.

1. Click **Modify** in the upper right corner.

   NOTE

   Alternatively, you can choose **Services** > **Network** > **Ethernet Network** > **Ethernet Ports** and click the name of the desired Ethernet port. In the upper right corner of the page that is displayed, click **Modify**.
2. In **Working Mode**, select a working mode for the Ethernet port.

NOTE

- This parameter may be invalid for some interface modules.
- The forward error correction (FEC) technology is used. With this technology, a sender sends data with a certain redundancy error correction code, and a receiver performs error detection on the received data according to the redundancy error correction code. If an error is detected, the receiver can correct the error.
- The working mode varies according to the port type. The value can be **Self-adaptive**, **RSFEC**, **NOFEC**, or **BASEFEC**.
- When the working mode of a port is set to **Self-adaptive**, it can automatically match the FEC mode of the peer network device (such as a NIC or switch). In this case, if the peer network device also has the self-adaptive capability enabled, the link negotiation time may be prolonged.
- When the working mode of a port is set to **RSFEC**, **NOFEC**, or **BASEFEC**, ensure that the mode matches the FEC mode of the peer network device. Before setting the working mode, you are advised to confirm it by referring to the product description of the peer network device.
- Retaining the default value is recommended. After modifying the port, verify that its **Running Status** is **Link up**. If **Running Status** is **Link down**, select another working mode to ensure that **Running Status** is **Link up**.

3. In **MTU (Bytes)**, enter a maximum transmission unit (MTU) for the packets transmitted between the Ethernet port and the application server.
4. In **Logical Port**, specify **Name**, **IP Address**, and **Subnet Mask/Prefix** of the logical port.

NOTE

You can click + or − to add or remove a logical port.

Step 6 Click **OK**.

Confirm your operation as prompted.

----End

5.2.1.3 Modifying a Management Port

When the network changes, you must modify the parameters of the management port to ensure proper communication between the storage system and the maintenance terminal.

Context

Modifying the management port will interrupt the existing connection between the storage system and the maintenance terminal.

Procedure

Step 1 Choose **System** > **Hardware** > **Devices**.

Step 2 Click the controller enclosure where the desired management port resides.

Step 3 Click to switch to the rear view.

Step 4 Click the management port you want to modify.

The **Ethernet Port:** *Port location* page is displayed on the right.

Step 5 Modify the management port.

1. Click **Modify** in the upper right corner.

   NOTE

   Alternatively, you can choose **Services** > **Network** > **Ethernet Network** > **Ethernet Ports** and click the name of the desired management port. In the upper right corner of the page that is displayed, click **Modify**.

2. Set the IPv4 address.
   a. Set **IPv4 Address** for the management port.
   b. Set **Subnet Mask** for the management port.
   c. Set **IPv4 Gateway** for the management port.
3. Set the IPv6 address.
   a. Set **IPv6 Address** for the management port.
   b. Set **Prefix** for the management port.
   c. Set **IPv6 Gateway** for the management port.

Step 6 Click **OK**.

Confirm your operation as prompted.

----End

5.2.1.4 Viewing Bit Error Statistics

A port's bit error statistics reflect the data transfer efficiency of the port. A high bit error rate compromises the read and write performance of the application server using the port.

Procedure

Step 1 Choose **System** > **Hardware** > **Devices**.

Step 2 Click the controller enclosure where the desired Ethernet port resides.

Step 3 Click to switch to the rear view.

Step 4 Click the desired Ethernet port.

Step 5 In the lower function pane, click **Bit Error Statistics**.

The **Bit Error Statistics** page is displayed on the right.

NOTE

Alternatively, you can choose **Services** > **Network** > **Ethernet Network** > **Ethernet Ports** and click **Bit Error Statistics**.

Step 6 Select **Ethernet Port** from the drop-down list in the upper-right corner.

Step 7 Query the bit error statistics in the port list.

NOTE

You can click **Clear** to clear bit error statistics.

----End

5.2.1.5 Managing Routes

If iSCSI networking is used and data needs to be transmitted across network segments, you must configure routes.

Prerequisites

You have configured an IP address for an Ethernet port.

NOTE

If redundant links are configured, you must configure an IP address and routing information for each involved Ethernet port.

Precautions

- The IP address of an Ethernet port must be on a different network segment from the internal heartbeat IP addresses.

  The default IP addresses of internal heartbeat on a dual-controller storage system are 127.127.127.10 and 127.127.127.11, and those on a four-controller storage system are 127.127.127.10, 127.127.127.11, 127.127.127.12, and 127.127.127.13.
- Internal heartbeat links are established between controllers for the controllers to detect each other's working status. Heartbeat links do not require separate cable connections. The internal heartbeat IP addresses have been assigned before delivery and cannot be changed.

Procedure

Step 1 Choose **System** > **Hardware** > **Devices**.

Step 2 Click the controller enclosure where the desired Ethernet port resides.

Step 3 Click  to switch to the rear view.

Step 4 Select the Ethernet port you want to configure.

Step 5 Click **Manage Route**.

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

NOTE

Alternatively, perform any of the following operations to go to the **Manage Route** page:

- Click **Manage Logical Port**. On the **Manage Logical Port** page that is displayed, select the desired logical port and click **Manage Route**.
- Choose **Services** > **Network** > **Logical Ports**.
  - Select the desired logical port and click **Manage Route**.
  - Click **More** on the right of the desired logical port and select **Manage Route**.

Step 6 Configure the route information for the Ethernet port.

1. In the **IP Address** drop-down list, select the IP address of the Ethernet port for which you want to add a route.
2. Click **Add**.
3. Set the parameters listed in **Table 5-11**.

Table 5-11 Route parameters

Parameter	Description
Type	Three types of routes are available: – Default route A route through which data is forwarded by default if no preferred route is available. The destination address and mask (IPv4) or prefix (IPv6) of the default route are automatically set to 0. To use this option, you only need to add a gateway. – Host route A route to a host. The destination mask (IPv4) or prefix (IPv6) of the host route are automatically set to 255.255.255.255 or 128. To use this option, you only need to add the destination address and gateway. – Network segment route A route to a network segment. You must add the destination address, destination mask (IPv4) or prefix (IPv6), and gateway.
Destination Address	IPv4 address, IPv6 address, or network segment of the destination service network port on the application server or destination Ethernet port on another storage system.
Subnet Mask/ Prefix	Subnet mask of the IPv4 address or prefix of the IPv6 address for the destination service network port on the application server or destination Ethernet port on another storage system.
Gateway	Gateway where the local Ethernet port's IP address resides. **NOTE** The IP address of the gateway must be different from all internal heartbeat IP addresses. Otherwise, routing will fail.

4. Click ✓. The route information is added to the list.

NOTE

Click on the right of a desired route to delete it.

Step 7 Click **Close**.

----End

5.2.1.6 Modifying a Bond Port

This section describes how to modify the information about a bond port.

Prerequisites

- A bond port has been created.
- After the MTU is changed to a non-default value, ensure that the MTU is the same as that of the peer device (switch or network adapter).

Procedure

Step 1 Choose **System** > **Hardware** > **Devices**.

Step 2 Click the controller enclosure where the desired Ethernet port resides.

Step 3 Click to switch to the rear view.

Step 4 Click an Ethernet port for which a bond port has been created.

The **Ethernet Port:** *Port location* page is displayed on the right.

Step 5 Click the **Bond Port** tab and click **Modify** in the upper right corner.

The **Modify** page is displayed.

NOTE

Alternatively, you can choose **Services** > **Network** > **Ethernet Network** > **Bond Ports**. Click **More** on the right of the desired bond port and select **Modify**.

Step 6 Set the **MTU (Bytes)** of the bond port. The value ranges from 1280 to 9000.

Step 7 In **Logical Port**, specify **Name**, **IP Address**, and **Subnet Mask/Prefix** of the logical port.

NOTE

You can click + to add more logical ports.

Step 8 Click **OK**.

----End

5.2.1.7 Canceling Ethernet Port Bonding

After canceling Ethernet port bonding, each Ethernet port functions as an independent port.

Prerequisites

All services running on the Ethernet ports for which you want to cancel bonding have been stopped. This is necessary because canceling Ethernet port bonding interrupts ongoing services.

Precautions

After Ethernet port bonding is canceled, the IP addresses of the Ethernet ports are cleared. You must reset IP addresses for the Ethernet ports if needed.

Procedure

Step 1 Choose **System** > **Hardware** > **Devices**.

Step 2 Click the controller enclosure where the desired Ethernet port resides.

Step 3 Click to switch to the rear view.

Step 4 Select the desired Ethernet port.

Step 5 Click **Cancel Bonding**.

Confirm your operation as prompted.

----End

5.2.1.8 Managing VLANs

This section describes how to add Ethernet ports or bond ports in the storage system to multiple independent VLANs. You can configure different services in different VLANs to ensure the security and reliability of service data.

Prerequisites

VLANs cannot be created on the Ethernet ports that are configured with IP addresses or carry services.

Procedure

Step 1 Choose **System** > **Hardware** > **Devices**.

Step 2 Click the controller enclosure where the desired Ethernet port resides.

Step 3 Click to switch to the rear view of the controller enclosure.

Step 4 Select the Ethernet port you want to configure.

Step 5 Click **Manage VLAN**.

The **Manage VLAN** page is displayed.

NOTE

Alternatively, you can choose **Services** > **Network** > **Ethernet Network** > **VLANs**.

Step 6 View the VLAN information.

Table 5-12 describes the parameters.

Table 5-12 VLAN parameters

Parameter	Description
Name	Name of a VLAN.
ID	ID of a VLAN.
Running Status	Running status of a VLAN. • **Unknown**: The system fails to query the VLAN status. • **Link up**: The running status of the home port of a VLAN is link up. • **Link down**: The running status of the home port of a VLAN is link down. • **To be recovered**: When the home port of a VLAN is in the **To be recovered** state, the running status of the VLAN is refreshed to **To be recovered**.
MTU (Bytes)	Maximum transmission unit of a VLAN.

Step 7 Create, modify, or delete a VLAN.

- To create a VLAN:
  a. Click **Create**.
     The **Create VLAN** page is displayed.
  b. Set **Port Type**. In the drop-down list, select the desired port type.
     Possible values are **Ethernet Port** and **Bond Port**.
  c. Select the desired Ethernet port or bond port from the port list in the middle function pane.
  d. In **ID**, specify the ID of a VLAN, and then click **Add**.

     NOTE

     - The VLAN ID ranges from 1 to 4094. You can specify multiple VLAN IDs one by one or in a batch. When creating multiple VLANs and specifying VLAN IDs in a batch, the VLAN IDs are in the following format: Start VLAN ID-End VLAN ID.
     - To delete an ID, click × next to it.

  e. Click **OK**.
- To modify a VLAN:
  a. Click **More** on the right of the desired VLAN and click **Modify**.
     The **Modify VLAN** page is displayed.
  b. Set **MTU (Bytes)**.

NOTE

The size of a packet transmitted between a port and a host cannot exceed the MTU of the Ethernet port.

c. Click **OK**.

- To delete a VLAN:

  Select the desired VLAN and click **Delete**.

  Confirm your operation as prompted.

  NOTE

  You can also click **More** on the right of the desired VLAN and select **Delete**.

----End

5.2.1.9 Viewing RDMA Ports

RDMA ports are used to interconnect controller enclosures as well as controller enclosures and smart disk enclosures.

Prerequisites

An RDMA interface module has been correctly installed on a controller.

Procedure

Step 1 Choose **System** > **Hardware** > **Devices**.

Step 2 Click the controller enclosure where the desired RDMA port resides.

Step 3 Click  to switch to the rear view of the controller enclosure.

Step 4 Click the desired RDMA port.

NOTE

Alternatively, you can choose **Services** > **Network** > **Ethernet Network** > **Ethernet Ports**. In **Logical Type**, select **Expansion port** or **Scale-out interconnect port** to filter out desired ports.

Step 5 View the RDMA port information on the page displayed on the right or in the table in the lower function pane.

Table 5-13 describes the parameters.

Table 5-13 RDMA port information

Parameter	Description
Logical Type	Logical type of the RDMA port. Possible values include: • **Expansion port**: connects a controller enclosure to a smart disk enclosure. • **Scale-out interconnect port**: connects controller enclosures.

Parameter	Description
Health Status	Health status of the RDMA port. • **Unknown**: The system fails to query the port status. • **Normal**: Functions and running performance of the port are normal and without error. • **Bit errors found**: Bit errors occur when the port transmits data. • **Faulty**: The port is functioning improperly and cannot work normally.
Running Status	Working status of the RDMA port. • **Unknown**: The system fails to query the port status. • **Link up**: A cable is connected to the port. • **Link down**: No cable is connected to the port. • **To be recovered**: For a 4 U device, if the owning controller of a port is faulty, the running status of the port is **To be recovered**.
Working Rate (Gbit/s)	Data transmission rate of the RDMA port.
Max. Working Rate (Gbit/s)	Maximum data transmission rate of the RDMA port.
Working Mode	Working mode of the RDMA port. **NOTE** • The forward error correction (FEC) technology is used. With this technology, a sender sends data with a certain redundancy error correction code, and a receiver performs error detection on the received data according to the redundancy error correction code. If an error is detected, the receiver can correct the error. • The working mode varies according to the port type. The value can be **Self-adaptive**, **RSFEC**, **NOFEC**, or **BASEFEC**.
MAC Address	MAC address of the RDMA port.
Port State	State of the RDMA port. A port will be disconnected after it is disabled.
MTU (Bytes)	Maximum size of a data packet that can be transmitted between the RDMA port and a controller enclosure or disk enclosure.

----End

5.2.2 Managing SAS Ports

SAS ports are used to interconnect the storage device with disk enclosures. You can view the parameters of SAS ports as required.

5.2.2.1 Viewing SAS Port Information

This section describes how to view information about a SAS port.

Prerequisites

A SAS interface module has been correctly installed on a controller.

Procedure

Step 1 Choose **System** > **Hardware** > **Devices**.

Step 2 Click  to switch to the rear view of the storage device.

Step 3 Click the desired SAS port.

Step 4 View the SAS port information in the displayed **SAS Port:** *Port location* page on the right or the table in the lower function pane.

Table 5-14 describes the parameters.

Table 5-14 SAS port parameters

Parameter	Description
Name	Name of the SAS port.
Location	Location of the SAS port.
ID	ID of the SAS port.
Health Status	Health status of the SAS port. • **Unknown**: The system fails to query the port status. • **Normal**: Functions and running performance of the port are normal and without error. • **Bit errors found**: Bit errors occur when the port transmits data. • **Faulty**: The port is functioning improperly and cannot work normally.
Running Status	Working status of the SAS port. • **Unknown**: The system fails to query the port status. • **Link up**: A cable is connected to the port. • **Link down**: No cable is connected to the port.
WWPN	WWPN of the SAS port.
Working Rate (Gbit/s)	Data transmission rate of the SAS port.
Max. Working Rate (Gbit/s)	Maximum data transmission rate of the SAS port.

Parameter	Description
Port State	State of the SAS port. A port will be disconnected after it is disabled.
Model	Model of the SAS port.

----End

5.2.2.2 Viewing Bit Error Statistics

A port's bit error statistics reflect the data transfer efficiency of the port. A high bit error rate compromises the read and write performance of the application server using the port.

Procedure

Step 1 Choose **System** > **Hardware** > **Devices**.

Step 2 Click to switch to the rear view.

Step 3 Click the desired SAS port.

Step 4 In the lower function pane, click **Bit Error Statistics**.

The **Bit Error Statistics** page is displayed on the right.

Step 5 Select **SAS Port** from the drop-down list in the upper-right corner.

Step 6 Query the bit error statistics in the port list.

NOTE

You can click **Clear** to clear bit error statistics.

----End

5.2.3 Managing FC Ports

FC ports are used to connect a storage device with application servers, allowing them to communicate with each other over FC links. You can view or modify parameters of FC ports as required.

5.2.3.1 Viewing FC Port Information

This section describes how to view information about an FC port.

Procedure

Step 1 Choose **System** > **Hardware** > **Devices**.

Step 2 Click the controller enclosure where the desired FC port resides.

Step 3 Click to switch to the rear view of the storage device.

Step 4 Click the desired FC port.

NOTE

Alternatively, you can choose **Services** > **Network** > **FC Network**.

Step 5 View the FC port information on the page displayed on the right or in the table in the lower function pane.

Table 5-15 describes the parameters.

Table 5-15 FC port information

Parameter	Description
Name	Name of the FC port.
Location	Location of the FC port.
ID	ID of the FC port.
Health Status	Health status of the FC port. • **Unknown**: The system fails to query the port status. • **Normal**: Functions and running performance of the FC port are normal and without error. • **Bit errors found**: Bit errors occur when the port transmits data. • **Faulty**: The FC port is functioning improperly and cannot work normally.
Running Status	Working status of the FC port. • **Unknown**: The system fails to query the port status. • **Link up**: A cable is connected to the port. • **Link down**: No cable is connected to the port.
WWPN	WWPN of the FC port.
Configured Rate (Gbit/s)	Configured rate of the FC port.
Working Rate (Gbit/s)	Data transmission rate of the FC port.
Max. Working Rate (Gbit/s)	Maximum data transmission rate of the FC port.
Operation Mode	Operation mode of the FC port. • **FC-AL**: arbitrated loop. • **P2P**: point to point. • **auto_adapt**: auto-adaptation.
Port State	Isolation status of the FC port. Possible values are **Enabled** and **Disabled**. If **Port State** is **Disabled**, this port cannot be used.

Parameter	Description
Initiators	Number of initiators connected to the FC port.
Port Protocol	Protocol used by the FC port.
Immediate Data	Indicates whether the immediate data function is enabled for the FC port.

NOTE

You can click the **Initiators** tab on the displayed page to view detailed initiator information.

----End

5.2.3.2 Modifying an FC Port

When the networking mode between a storage device and an application server changes, modify the parameters of the FC port to ensure proper communication between them.

Context

Note the following when modifying the properties of an FC port:

- When a storage system uses an FC port to connect to an application server, ensure that the rate of the FC port on the storage system is the same as that of the HBA port on the application server. Using different rates may cause communication failure between the storage system and application server.
- When two storage systems are interconnected by FC ports, ensure that the rates of the FC ports are the same on the two storage systems. Using different rates may cause communication failure.
- Do not modify the properties of an FC port when services are running because modifying the properties will interrupt the communication on this port.

Procedure

Step 1 Choose **System** > **Hardware** > **Devices**.

Step 2 Click the controller enclosure where the desired FC port resides.

Step 3 Click  to switch to the rear view of the controller enclosure.

Step 4 Click the desired FC port.

The **FC Port** page is displayed.

Step 5 Modify the FC port.

1. Click **Modify** in the upper right corner.

NOTE

Alternatively, you can choose **Services** > **Network** > **FC Network** and click the name of the desired FC port. In the upper right corner of the page that is displayed, click **Modify**.

2. In **Configured Rate (Gbit/s)**, select a data transmission rate for the FC port.

NOTICE

- The FC port must have the same rate and mode as the HBA port on the application server to prevent a communication failure.
- When two storage systems are interconnected by FC ports, ensure that the rates and modes of the FC ports are the same on the two storage systems. Using different rates or modes may cause communication failure.

The rate of an FC port can be 2 Gbit/s, 4 Gbit/s, 8 Gbit/s, 16 Gbit/s, 32 Gbit/s, or self-adaptive. Select a correct value after obtaining necessary information.

NOTE

- If the maximum rate of the port is 4 Gbit/s, you can set the value to 2 Gbit/s or 4 Gbit/s.
- If the maximum rate of the port is 8 Gbit/s, you can set the value to 2 Gbit/s, 4 Gbit/s, or 8 Gbit/s.
- If the maximum rate of the port is 16 Gbit/s, you can set the value to 4 Gbit/s, 8 Gbit/s, or 16 Gbit/s.
- If the maximum rate of the port is 32 Gbit/s, you can set the value to 8 Gbit/s, 16 Gbit/s, or 32 Gbit/s.
- If the value is set to **Self-adaptive**, the interconnected FC ports negotiate the rate automatically. If the negotiated rates do not match, modify the rate manually.

3. In **Port Protocol**, select **FC-SCSI** or **FC-NVMe**.
4. Determine whether to enable **Immediate Data**. In scenarios where FC replication links are used to transmit service data between storage arrays, the **Immediate Data** function can improve the data transmission performance. You are advised to enable this function.

Step 6 Click **OK**.

Confirm your operation as prompted.

----End

5.2.3.3 Viewing Bit Error Statistics

A port's bit error statistics reflect the data transmission efficiency of this port. A high bit error rate compromises the read and write performance of the application server using the port.

Procedure

Step 1 Choose **System** > **Hardware** > **Devices**.

Step 2 Click the controller enclosure where the desired FC port resides.

Step 3 Click to switch to the rear view.

Step 4 Click the desired FC port.

Step 5 In the lower function pane, click **Bit Error Statistics**.

The **Bit Error Statistics** page is displayed on the right.

NOTE

Alternatively, you can choose **Services** > **Network** > **FC Network** and click **Bit Error Statistics**.

Step 6 Query the bit error statistics of the FC ports.

1. Select **FC Port** from the drop-down list in the upper-right corner.
2. Query the bit error statistics in the port list.

NOTE

You can click **Clear** to clear bit error statistics.

----End

5.2.4 Managing RoCE Ports

RoCE ports are used to connect a storage device with application servers, allowing them to communicate with each other over RoCE networks. You can view or modify parameters of RoCE ports as required.

5.2.4.1 Viewing RoCE Ports

This operation enables you to view information about RoCE ports.

Procedure

Step 1 Choose **System** > **Hardware** > **Devices**.

Step 2 Click the controller enclosure where the desired RoCE port resides.

Step 3 Click to switch to the rear view of the storage device.

Step 4 Click the desired RoCE port.

NOTE

Alternatively, you can choose **Services** > **Network** > **RoCE Network** > **RoCE Ports**.

Step 5 View the RoCE port information on the page displayed on the right or in the table in the lower function pane.

Table 5-16 describes the parameters.

Table 5-16 RoCE port information

Parameter	Description
Name	Name of the RoCE port.
Location	Location of the RoCE port.
ID	ID of the RoCE port.
Health Status	Health status of the RoCE port. • **Unknown**: The system fails to query the port status. • **Normal**: Functions and running performance of the RoCE port are normal and without error. • **Bit errors found**: Bit errors occur when the port transmits data. • **Faulty**: The RoCE port is functioning improperly and cannot work normally.
Running Status	Working status of the RoCE port. • **Unknown**: The system fails to query the port status. • **Link up**: A cable is connected to the port. • **Link down**: No cable is connected to the port. • **To be recovered**: For a 4 U device, if the owning controller of a port is faulty, the running status of the port is **To be recovered**.
MAC Address	MAC address of the RoCE port.
Working Rate (Gbit/s)	Data transmission rate of the RoCE port.
Max. Working Rate (Gbit/s)	Maximum data transmission rate of the RoCE port.
MTU (Bytes)	Maximum size of a data packet that can be transferred between the RoCE port and an application server.
Working Mode	Working mode of the RoCE port. **NOTE** • The forward error correction (FEC) technology is used. With this technology, a sender sends data with a certain redundancy error correction code, and a receiver performs error detection on the received data according to the redundancy error correction code. If an error is detected, the receiver can correct the error. • The working mode varies according to the port type. The value can be **Self-adaptive**, **RSFEC**, **NOFEC**, or **BASEFEC**.
Bond Name	Bond name of the RoCE port.

Parameter	Description
Logical Type	Logical type of a RoCE port. Possible values are **Management port**, **Maintenance port**, **Expansion port**, **Scale-out interconnection port**, **Container front-end port**, and **Container back-end port**.
iSCSI Target Name	Target name of the iSCSI network where the RoCE port resides.
Port State	State of the RoCE port. A RoCE port will be disconnected after it is disabled.
Initiators	Number of initiators connected to the RoCE port.
SNSD	State of Storage Network Smart Discovery (SNSD). When **SNSD** of a RoCE port is set to **Enabled**, hosts detect the state changes of all logical ports of the RoCE port and determine whether to automatically establish or cancel connections based on logical port states. **NOTE** • **SNSD** has enterprise or standard modes. When **SNSD** is switched from **Disabled** to **Enabled**, the standard mode is used by default. To use the enterprise mode, run the **change port eth_snsd_switch** command on the CLI. For details about this command, see the command reference specific to your product model. • Only 6.1.5 and later versions support the enterprise mode.
Trust Mode	Trust mode of a RoCE port. Possible values are **PCP** and **DSCP**. **NOTE** Only 6.1.5 and later versions support this parameter.

NOTE

On the page displayed on the right, you can view information about **Initiators**, **Owning Port Groups**, and **VLANs**.

----End

5.2.4.2 Modifying a RoCE Port

When the networking mode between a storage device and an application server changes, modify the parameters of the RoCE port to ensure proper communication between them.

Procedure

Step 1 Choose **System** > **Hardware** > **Devices**.

Step 2 Click the controller enclosure where the desired RoCE port resides.

Step 3 Click  to switch to the rear view.

Step 4 Click the desired RoCE port.

The **RoCE Port** page is displayed.

Step 5 Modify the RoCE port.

1. Click **Modify** in the upper right corner.

   NOTE

   Alternatively, you can choose **Services** > **Network** > **RoCE Network** > **RoCE Ports** and click the name of the desired RoCE port. In the upper right corner of the page that is displayed, click **Modify**.

2. In **Working Mode**, select a working mode for the RoCE port.

   NOTE

   - This parameter may be invalid for some interface modules.
   - The forward error correction (FEC) technology is used. With this technology, a sender sends data with a certain redundancy error correction code, and a receiver performs error detection on the received data according to the redundancy error correction code. If an error is detected, the receiver can correct the error.
   - The working mode varies according to the port type. The value can be **Self-adaptive**, **RSFEC**, **NOFEC**, or **BASEFEC**.
   - When the working mode of a port is set to **Self-adaptive**, it can automatically match the FEC mode of the peer network device (such as a NIC or switch). In this case, if the peer network device also has the self-adaptive capability enabled, the link negotiation time may be prolonged.
   - When the working mode of a port is set to **RSFEC**, **NOFEC**, or **BASEFEC**, ensure that the mode matches the FEC mode of the peer network device. Before setting the working mode, you are advised to confirm it by referring to the product description of the peer network device.
   - Retaining the default value is recommended. After modifying the port, verify that its **Running Status** is **Link up**. If **Running Status** is **Link down**, select another working mode to ensure that **Running Status** is **Link up**.

3. In **MTU (Bytes)**, enter a maximum transmission unit (MTU) for the packets transmitted between the RoCE port and the application server.
4. Determine whether to enable **SNSD**. When **SNSD** of a RoCE port is set to **Enabled**, hosts detect the state changes of all logical ports of the RoCE port and determine whether to automatically establish or cancel connections based on logical port states.

   NOTE

   - **SNSD** has enterprise or standard modes. When **SNSD** is switched from **Disabled** to **Enabled**, the standard mode is used by default. To use the enterprise mode, run the **change port eth_snsd_switch** command on the CLI. For details about this command, see the command reference specific to your product model.
   - Only 6.1.5 and later versions support the enterprise mode.

5. Set **Trust Mode** of the port, which can be **PCP** or **DSCP**.

NOTE

- The default trust mode is **PCP**. If you want to create a logical port directly on the RoCE port, select **DSCP**.
- Only 6.1.5 and later versions can set the trust mode of a port.

Step 6 Click **OK**.

Confirm your operation as prompted.

----End

5.2.4.3 Batch Setting SNSD

This section describes how to enable or disable SNSD for RoCE ports in a batch.

Procedure

Step 1 Choose **Services** > **Network** > **RoCE Network** > **RoCE Ports**.

Step 2 Select desired RoCE ports and click **Batch Set SNSD**. Then select **Batch Enable SNSD** or **Batch Disable SNSD**.

NOTE

- When **SNSD** of a RoCE port is set to **Enabled**, hosts detect the state changes of all logical ports of the RoCE port and determine whether to automatically establish or cancel connections based on logical port states.
- **SNSD** has enterprise or standard modes. When **SNSD** is switched from **Disabled** to **Enabled**, the standard mode is used by default. To use the enterprise mode, run the **change port eth_snsd_switch** command on the CLI. For details about this command, see the command reference specific to your product model.
- Only 6.1.5 and later versions support the enterprise mode.

Confirm your operation as prompted.

----End

5.2.4.4 Viewing Bit Error Statistics

A port's bit error statistics reflect the data transmission efficiency of this port. A high bit error rate compromises the read and write performance of the application server using the port.

Procedure

Step 1 Choose **System** > **Hardware** > **Devices**.

Step 2 Click the controller enclosure where the desired RoCE port resides.

Step 3 Click  to switch to the rear view.

Step 4 Click the desired RoCE port.

Step 5 In the lower function pane, click **Bit Error Statistics**.

The **Bit Error Statistics** page is displayed on the right.

NOTE

Alternatively, you can choose **Services** > **Network** > **RoCE Network** > **RoCE Ports** and click **Bit Error Statistics**.

Step 6 Select **RoCE Port** from the drop-down list in the upper-right corner.

Step 7 Query the bit error statistics in the port list.

NOTE

You can click **Clear** to clear bit error statistics.

----End

5.2.4.5 Managing VLANs

This section describes how to add RoCE ports in the storage system to multiple independent VLANs. You can configure different services in different VLANs to ensure the security and reliability of service data.

Procedure

Step 1 Choose **System** > **Hardware** > **Devices**.

Step 2 Click the controller enclosure where the desired RoCE port resides.

Step 3 Click  to switch to the rear view of the controller enclosure.

Step 4 Click the desired RoCE port.

Step 5 Click **Manage VLAN**.

The **Manage VLAN** page is displayed.

NOTE

Alternatively, you can choose **Services** > **Network** > **RoCE Network** > **VLANs**.

Step 6 View the VLAN information.

Table 5-17 describes the parameters.

Table 5-17 VLAN parameters

Parameter	Description
Name	Name of a VLAN.
ID	ID of a VLAN.

Parameter	Description
Running Status	Running status of a VLAN. • **Unknown**: The system fails to query the VLAN status. • **Link up**: The running status of the home port of a VLAN is link up. • **Link down**: The running status of the home port of a VLAN is link down. • **To be recovered**: When the home port of a VLAN is in the **To be recovered** state, the running status of the VLAN is refreshed to **To be recovered**.
MTU (Bytes)	Maximum transmission unit of a VLAN.

Step 7 Create, modify, or delete a VLAN.

- To create a VLAN:
  a. Click **Create**.
     The **Create VLAN** page is displayed.
  b. In the **Home Port** list, select a home port.
  c. In **ID**, specify the ID of a VLAN, and then click **Add**.

     NOTE

     - The VLAN ID ranges from 1 to 4094. You can specify multiple VLAN IDs one by one or in a batch. When creating multiple VLANs and specifying VLAN IDs in a batch, the VLAN IDs are in the following format: Start VLAN ID-End VLAN ID.
     - To delete an ID, click × next to it.

  d. Click **OK**.
- To modify a VLAN:
  a. Click **More** on the right of the desired VLAN and click **Modify**.
     The **Modify VLAN** page is displayed.
  b. Set **MTU (Bytes)**.

     NOTE

     The size of a packet transmitted between a port and a host cannot exceed the MTU of the RoCE port.

  c. Click **OK**.
- To delete a VLAN:
  Select the desired VLAN and click **Delete**.
  Confirm your operation as prompted.

  NOTE

  You can also click **More** on the right of the desired VLAN and select **Delete**.

----End

5.3 Managing Storage Pools

This section describes how to manage storage pools.

5.3.1 Viewing Storage Pool Information

This section describes how to view basic information about storage pools.

Procedure

Step 1 Choose **System** > **Storage Pools**.

Step 2 View the storage pool information in the function pane. **Table 5-18** describes the parameters.

Table 5-18 Storage pool parameters

Parameter	Description
Name	Name of the storage pool. **NOTE** You can click the name of a storage pool to view its details and manage it.
ID	ID of the storage pool.
Health Status	Health status of the storage pool.
Running Status	Running status of the storage pool.
Total	Usable capacity of a storage pool (Total physical capacity of disks – Capacity consumed by RAID and metadata). **NOTE** If a storage pool is created on the CLI and has been configured with the capacity during the creation, the configured capacity is displayed in **Total**. However, the actual capacity that can be used is the total physical capacity of all disks.
Used	Sum of the allocated capacity and data protection capacity of a storage pool. **NOTE** It is recommended that the used capacity of a storage pool should not exceed 85% of the total capacity. If the usage exceeds 85%, you are advised to expand the storage pool.
Free	Free capacity = Total capacity – Used capacity
Data Protection	Total capacity of all LUNs and file systems for data protection in a storage pool. **NOTE** For example, if snapshots are created for LUNs in the storage pool, the space occupied by the activated snapshots is the data protection capacity.

Parameter	Description
Data Reduction	Total amount of user data written to the storage pool divided by the storage pool's used capacity. **NOTE** This parameter is valid only when SmartDedupe and SmartCompression licenses are imported to the storage system.
Data Reduction Ratio for Block	Total amount of block data written to the storage pool divided by the storage pool's used block capacity. **NOTE** This parameter is valid only when SmartDedupe and SmartCompression licenses are imported to the storage system.
Data Reduction Ratio for File	Total amount of file data written to the storage pool divided by the storage pool's used file capacity. **NOTE** This parameter is valid only when SmartDedupe and SmartCompression licenses are imported to the storage system and the product model supports file systems.
Thin Space Saving	Calculation formula: Thin space saving rate = (Total subscribed capacity – Used subscribed capacity)/Total subscribed capacity **NOTE** This parameter is valid only when SmartDedupe and SmartCompression licenses are imported to the storage system.
Overall Space Saving	Space saving ratio of a storage pool. (Total subscribed capacity/Used subscribed capacity) x Data reduction ratio **NOTE** If the percentage of all LUNs' available capacity to their total configured capacity is lower than 1%, the available capacity is considered as 1% of the configured capacity. This parameter is valid only when SmartDedupe and SmartCompression licenses are imported to the storage system.
Total Subscribed	Total capacity of all LUNs and file systems in a storage pool.
Used Subscribed	Total amount of data that has been written to all LUNs and file systems in a storage pool.
Free Subscribed	Free subscribed capacity = Total subscribed capacity – Used subscribed capacity

Step 3 (Optional) Click the name of a storage pool to query its summary and disk information.

----End

5.3.2 Expanding a Storage Pool

When the capacity of a storage pool is insufficient, you can expand the storage pool to meet capacity requirements.

Capacity Expansion Methods

For details about capacity expansion, see the administrator guide specific to your product model and version.

5.3.3 Updating Keys

For storage pools with data encryption enabled, you are advised to periodically update keys for security purpose.

Key Update Method

For details, see the disk encryption user guide specific to your product model and version.

5.3.4 Exporting Disk Configuration

This section describes how to export disk configuration.

Procedure

Step 1 Choose **System** > **Storage Pools**.

Step 2 Click **More** on the right of the desired storage pool and choose **Export Disk Configuration**.

The **Export Disk Configuration** dialog box is displayed.

NOTE

Alternatively, click the name of the desired storage pool. In the upper right corner of the page that is displayed, select **Export Disk Configuration** from the **Operation** drop-down list.

Step 3 Click **OK**.

----End

5.3.5 Modifying the Properties of a Storage Pool

This section describes how to modify the properties of a storage pool.

Procedure

Step 1 Choose **System** > **Storage Pools**.

Step 2 Click **More** on the right of the desired storage pool and choose **Modify**.

The **Modify Storage Pool** page is displayed on the right.

NOTE

Alternatively, click the name of the desired storage pool. In the upper right corner of the page that is displayed, select **Modify** from the **Operation** drop-down list.

Step 3 Set the properties for the storage pool.

Table 5-19 describes the parameters.

Table 5-19 Storage pool parameters

Parameter	Description
Name	Name of the storage pool. [Value range] ● The name must be unique. ● The name can contain only letters, digits, periods (.), underscores (_), and hyphens (-). ● The name contains 1 to 255 characters.
Description	Description of the storage pool.
Hot Spare Policy	Hot spare policy of the storage pool. [Value range] None, Low (1 disk), High (2 disks), Custom (3 disks), Custom (4 disks), Custom (5 disks), Custom (6 disks), Custom (7 disks), and Custom (8 disks) **NOTE** ● Hot spare capacity is provided by all member disks in each storage pool because the storage system uses RAID 2.0+ virtualization technology. For ease of understanding, the hot spare capacity is expressed in the number of hot spare disks on DeviceManager. ● Even if the hot spare space is used up, the system can use the free space of the storage pool to reconstruct data, ensuring storage system reliability.
Capacity Alarm Threshold (%)	When the percentage of the storage pool's allocated capacity to its total capacity reaches this threshold, the system generates a capacity alarm. A proper capacity alarm threshold helps you monitor the capacity usage of a storage pool. [Value range] 1 to 95
Capacity Used Up Alarm Threshold (%)	When the percentage of the storage pool's allocated capacity to its total capacity reaches this threshold, the system generates an alarm indicating that the capacity is being used up. The severity of this alarm is higher than that of the capacity alarm. [Value range] 2 to 99 **NOTE** The value of **Capacity Used Up Alarm Threshold (%)** must be greater than that of **Capacity Alarm Threshold (%)**.

Parameter	Description
Protection Data Auto Deletion	Indicates whether to automatically delete earliest scheduled HyperCDP objects when the percentage of the protection capacity to the storage pool's total capacity reaches **Protection Capacity Upper Limit (%)**. The automatic deletion stops when the percentage becomes less than **Protection Capacity Lower Limit (%)**.
Protection Capacity Lower Limit (%)	Lower limit for the percentage of the protection capacity to the storage pool's total capacity for the system to stop deleting earliest scheduled HyperCDP objects. **NOTE** This parameter is available only when **Protection Data Auto Deletion** is enabled. [Value range] 1 to 95
Protection Capacity Upper Limit (%)	Maximum allowable percentage of the protection capacity to the storage pool's total capacity. After this threshold is reached, the system automatically deletes earliest scheduled HyperCDP objects. **NOTE** • This parameter is available only when **Protection Data Auto Deletion** is enabled. • The value of **Protection Capacity Upper Limit (%)** must be greater than that of **Protection Capacity Lower Limit (%)**. [Value range] 2 to 99

Step 4 Click **OK**.

Confirm your operation as prompted.

----End

5.3.6 Deleting a Storage Pool

5.3.6.1 Deleting a Storage Pool (Applicable to 6.1.3)

This section describes how to delete a storage pool when it is no longer used.

Prerequisites

- LUNs and file systems in the storage pool have been deleted. LUNs configured for containerized applications and in-band LUNs cannot be viewed on DeviceManager. You can run the **show lun general** command on the CLI to query LUNs and run the **delete lun** command to delete LUNs. For details on this command, refer to the *Command Reference*.

- If the storage pool stores historical monitoring data, **Retain historical monitoring data** has been deselected and historical monitoring data has been deleted from the storage pool.

  NOTICE

  Deleted historical monitoring data cannot be restored. Before deleting historical monitoring data, confirm that you do not need to view or export it.

  NOTE

  - On DeviceManager, choose **Settings** > **Monitoring Settings**. In the **Retention Settings** area, deselect **Retain historical monitoring data**.
  - You can delete historical monitoring data in either of the following ways:
    - On DeviceManager, deselect **Retain historical monitoring data** and click **Save**. In the dialog box that is displayed, select **Delete historical monitoring data**.
    - Run the **change performance retention_strategy is_delete_performance_data=yes** command on the CLI.

Procedure

Step 1 Choose **System** > **Storage Pools**.

Step 2 Click **More** on the right of the desired storage pool and choose **Delete**.

NOTE

Alternatively, click the name of the desired storage pool. In the upper right corner of the page that is displayed, select **Delete** from the **Operation** drop-down list.

Step 3 (Optional) Select **Erase Data**.

NOTICE

- Only data on SSDs and encrypted HDDs can be erased.
- After data is erased from all storage pools associated with the performance layer, the performance layer automatically erases data. The erasure mode of the last storage pool associated with the performance layer is used.
- When data is being erased from a disk, a power cycle is automatically performed for this disk.
- Data erasure takes a long time. The time required with data erasure mechanisms **block_erase** and **cryptographic_erase** used is about 10 minutes, and that with data erasure mechanism **overwrite** used varies according to the configured parameters and disk capacity, which ranges from several hours to more than 10 hours. For details about how to view the data erasure progress, see section **Viewing the Data Erasure Progress of a Disk** in the *Administrator Guide* of the desired version.
- Configurations cannot be cleared during data erasure. The commands for clearing configurations include **ccdb.sh -c clearccdb**, **ccdb.sh -c cleardbfile**, **ccdb.sh -c repairdb**, **ccdb.sh -c clearall**, **ccdb.sh -c deletedb**, **restore system factory_mode**, **change ccdb general**, **change cluster controllers**, **change controllers_expansion cancel**, and **clear configuration_data**.

1. Select **I have read and understand the consequences associated with performing this operation**, and click **OK**.

   The **Erase Data** page is displayed on the right.
2. Set data erasure parameters.

   Table 5-20 describes the parameters.

Table 5-20 Data erasure parameters

Parameter	Description
Data Erasure Mechanism	Disk data erasure method. Possible options are as follows: – **cryptographic_erase**: erases security keys. This parameter is available only when the data encryption feature is enabled for the storage pool. – **block_erase**: erases disk data, user data, and mappings by block. – **overwrite**: overwrites disk data with specific pattern values.
Data Erasure Standard	Standard for overwriting disk data. Possible options are **DoD 5220.22-M (E)**, **DoD 5220.22-M (ECE)**, **VSITR**, and **Custom**. This parameter is available only when **Data Erasure Mechanism** is set to **overwrite**. **NOTE** When **Data Erasure Standard** is set to **Custom**, the system will overwrite disk data according to **Pattern Value** and **Overwrites** specified by users.

Parameter	Description
Pattern Value	Pattern value used to overwrite disk data. A pattern value can be **r** or a one-byte hexadecimal number starting with **0x**. A maximum of three values can be entered. **NOTE** – This parameter is available only when **Data Erasure Standard** is set to **Custom**. – Value **r** indicates a random number.
Overwrites	Number of times the disk data is overwritten using the pattern value.
Verify Data Erasure	Indicates whether to enable the data erasure verification function. If **Verify Data Erasure** is set to **Enable**, the system verifies whether the disk data is erased completely. **NOTE** This parameter is unavailable when **Data Erasure Mechanism** is set to **cryptographic_erase**.
Data to Be Verified (%)	Percentage of the data to be verified to the total disk capacity. **NOTE** This parameter is available only when **Verify Data Erasure** is set to **Enable**.

Step 4 Click **OK**.

Confirm your operation as prompted.

----End

5.3.6.2 Deleting a Storage Pool (Applicable to 6.1.5 and Later Versions)

This section describes how to delete a storage pool when it is no longer used.

Prerequisites

- LUNs and file systems in the storage pool have been deleted. LUNs configured for containerized applications and in-band LUNs cannot be viewed on DeviceManager. You can run the **show lun general** command on the CLI to query LUNs and run the **delete lun** command to delete LUNs. For details on this command, refer to the *Command Reference*.
- If the storage pool stores historical monitoring data, **Retain historical monitoring data** has been deselected and historical monitoring data has been deleted from the storage pool.

NOTICE

Deleted historical monitoring data cannot be restored. Before deleting historical monitoring data, confirm that you do not need to view or export it.

NOTE

- On DeviceManager, choose **Settings** > **Monitoring Settings**. In the **Retention Settings** area, deselect **Retain historical monitoring data**.
- You can delete historical monitoring data in either of the following ways:
  - On DeviceManager, deselect **Retain historical monitoring data** and click **Save**. In the dialog box that is displayed, select **Delete historical monitoring data**.
  - Run the **change performance retention_strategy is_delete_performance_data=yes** command on the CLI.

Procedure

Step 1 Choose **System** > **Storage Pools**.

Step 2 Click **More** on the right of the desired storage pool and choose **Delete**.

NOTE

Alternatively, click the name of the desired storage pool. In the upper right corner of the page that is displayed, select **Delete** from the **Operation** drop-down list.

Step 3 (Optional) Click **Advanced** and select **Erase Data**.

NOTICE

- After data is erased from all storage pools associated with the performance layer, the performance layer automatically erases data. The erasure mode of the last storage pool associated with the performance layer is used.
- When data is being erased from a disk, a power cycle is automatically performed for this disk.
- Data erasure takes a long time. The time required with data erasure mechanisms **block_erase** and **cryptographic_erase** used is about 10 minutes, and that with data erasure mechanism **overwrite** used varies according to the configured parameters and disk capacity, which ranges from several hours to more than 10 hours. For details about how to view the data erasure progress, see section **Viewing the Data Erasure Progress of a Disk** in the *Administrator Guide* of the desired version.
- Configurations cannot be cleared during data erasure. The commands for clearing configurations include **ccdb.sh -c clearccdb**, **ccdb.sh -c cleardbfile**, **ccdb.sh -c repairdb**, **ccdb.sh -c clearall**, **ccdb.sh -c deletedb**, **restore system factory_mode**, **change ccdb general**, **change cluster controllers**, **change controllers_expansion cancel**, and **clear configuration_data**.

1. Select **I have read and understand the consequences associated with performing this operation**, and click **OK**.

   The **Erase Data** page is displayed on the right.

2. Set the parameters.

   Table 5-21 describes the parameters.

Table 5-21 Data erasure parameters

Parameter	Description
Data Erasure Mechanism	Disk data erasure method. Possible options are as follows: – **cryptographic_erase**: erases security keys. This parameter is available only when the data encryption feature is enabled for the storage pool. – **block_erase**: erases disk data, user data, and mappings by block. – **overwrite**: overwrites disk data with specific pattern values.
Data Erasure Standard	Standard for overwriting disk data. Possible options are **DoD 5220.22-M (E)**, **DoD 5220.22-M (ECE)**, **VSITR**, and **Custom**. This parameter is available only when **Data Erasure Mechanism** is set to **overwrite**. **NOTE** When **Data Erasure Standard** is set to **Custom**, the system will overwrite disk data according to **Pattern Value** and **Overwrites** specified by users.
Pattern Value	Pattern value used to overwrite disk data. A pattern value can be **r** or a one-byte hexadecimal number starting with **0x**. A maximum of three values can be entered. **NOTE** – This parameter is available only when **Data Erasure Standard** is set to **Custom**. – Value **r** indicates a random number.
Overwrites	Number of times the disk data is overwritten using the pattern value.
Verify Data Erasure	Indicates whether to enable the data erasure verification function. If **Verify Data Erasure** is set to **Enable**, the system verifies whether the disk data is erased completely. **NOTE** This parameter is unavailable when **Data Erasure Mechanism** is set to **cryptographic_erase**.
Data to Be Verified (%)	Percentage of the data to be verified to the total disk capacity. **NOTE** This parameter is available only when **Verify Data Erasure** is set to **Enable**.

Step 4 Click **OK**.

Confirm your operation as prompted.

----End

5.4 Managing LUNs

This section describes how to manage LUNs.

5.4.1 Viewing LUN Information

This section describes how to view basic information about all LUNs.

Procedure

Step 1 Choose **Services** > **Block Service** > **LUN Groups** > **LUNs**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 View the LUN information in the function pane. **Table 5-22** describes the parameters.

Table 5-22 LUN parameters

Parameter	Description
Name	Name of a LUN. **NOTE** You can click the name of a LUN to view its details and manage it.
ID	ID of a LUN.
Owning vStore	Name of the vStore to which the LUN belongs. **NOTE** This parameter is available only when **vStore** is set to **All vStores** in **Step 2**.
vStore ID	ID of the vStore to which the LUN belongs. **NOTE** This parameter is available only when **vStore** is set to **All vStores** in **Step 2**.
Capacity	LUN capacity information, including the total capacity of a LUN and the ratio of the used capacity (that is, the allocated capacity) to the total capacity of the LUN. **NOTE** Move the cursor to **Capacity** of a LUN to view the total capacity, allocated capacity, and data protection capacity of the LUN.
Total	Capacity configured for a LUN.
Allocated	Amount of user data written to a LUN.
Data Protection Capacity	Capacity used for data protection on a LUN.
Used	Ratio of the used capacity (that is, the allocated capacity) to the total capacity of a LUN.
Health Status	Health status of the LUN.

Parameter	Description
Running Status	Running status of the LUN.
Created	Time when the LUN was created.
Data Protection	Data protection information about the LUN.
Owning Storage Pool	Storage pool to which the LUN belongs.
Local WWN	WWN of the LUN.
NGUID	Unique identifier of the namespace of a LUN.
Function Type	Function type of a LUN. Possible values are **LUN**, **Snapshot**, and **Clone**.
Mapping	Indicates whether the LUN has been mapped.
Use Type	Usage type of the LUN. The possible values are as follows: • **Internal**: common LUN created in a local storage system. • **External**: external device LUN (eDevLUN) created for taking over a LUN from an external storage system.
Application Type	Application type of a LUN.
Takeover Type	Takeover type of the LUN.
Remote WWN	WWN of a remote LUN.
Takeover LUN WWN	WWN of the external LUN after takeover, that is, the eDevLUN WWN.

Step 4 (Optional) Click the name of a LUN to query its summary, topology, mapping, and protection features.

NOTE

- If a LUN has been added to multiple LUN groups, click the **Summary** tab on the details page, and click **More** on the right of **Owning LUN Groups**. On the **Owning LUN Groups** page that is displayed, view the names and IDs of the owning LUN groups.
- On the **Topology** tab page, if the number of ports in a port group is greater than 3, you can click ••• to view details about all ports. When **Port Type** is **Physical port**, the parameters are described in **Table 5-23**. When **Port Type** is **Logical port**, the parameters are described in **Table 5-24**.

Table 5-23 Physical port parameters

Parameter	Description
Type	Type of a physical port.
Location	Location of a physical port.

Parameter	Description
Health Status	Health status of a physical port. • **Unknown**: The system fails to query the port status. • **Normal**: Functions and running performance of the port are normal and without error. • **Bit errors found**: Bit errors occur when the port transmits data. • **Faulty**: The port is functioning improperly and cannot work normally.
Running Status	Working status of a physical port. • **Unknown**: The system fails to query the port status. • **Link up**: A cable is connected to the port. • **Link down**: No cable is connected to the port. • **To be recovered**: For a 4 U device, if the owning controller of a port is faulty, the running status of the port is **To be recovered**.
Usage	Usage of a physical port.

Table 5-24 Logical port parameters

Parameter	Description
Name	Name of a logical port.
Running Status	Running status of a logical port. • **Unknown**: The system fails to query the port status. • **Link up**: The running status of the home port of a logical port is link up. • **Link down**: The running status of the home port of a logical port is link down. • **Standby**: In a HyperMetro scenario, when a logical port works at the owning site of the primary or secondary end, the running status of the logical port at the non-owning site of the peer end is **Standby**. • **To be recovered**: When the home port of a logical port is in the **To be recovered** state or a logical port used for the file service fails to be failed over, the running status of the logical port changes to **To be recovered**.
Activation Status	Indicates whether a logical port is activated.
Data Protocol	Data protocol of a logical port.

----End

5.4.2 Mapping a LUN

This section describes how to create one-to-one or many-to-one mapping relationships between LUNs and hosts.

Procedure

Step 1 Choose **Services** > **Block Service** > **LUN Groups** > **LUNs**.

Step 2 Select the vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Select the desired LUNs and click **Map**.

The **Map LUN** page is displayed on the right.

NOTE

Alternatively, perform either of the following operations to go to the **Map LUN** page:

- Click **More** on the right of the desired LUN and select **Map**.
- Click the name of the desired LUN. In the upper right corner of the page that is displayed, select **Map** from the **Operation** drop-down list.

Step 4 Click ▶ on the right of **Selected LUNs**. In the **Available LUNs** list, select the desired LUNs and add them to **Selected LUNs**.

NOTE

Skip this step if you want to map each LUN separately.

Step 5 Select a host from the **Host** drop-down list.

NOTE

You can click **Create** to create a host on the **Create Host** page that is displayed.

Step 6 Select a port group from the **Port Group** drop-down list.

NOTE

You can click **Create** to create a port group on the **Create Port Group** page that is displayed.

Step 7 Select **Advanced** in the upper right corner and set how to assign host LUN IDs.

- **Automatic**: The system assigns a host LUN ID to each LUN mapped to a host.
- **Start ID**: Set a start ID ranging from 0 to 4095. The system assigns a host LUN ID to each LUN mapped to a host, starting from **Start ID**.
- **Specified ID**: Manually assign a host LUN ID to each LUN mapped to a host.

Step 8 If HyperMetro pairs have been created for the LUNs, determine whether to select **Same Host LUN ID**. If you select it, the system forcibly ensures that the host LUN IDs of the local and remote LUNs in the same HyperMetro pairs are the same. In SAN-based HyperMetro scenarios involving ESX hosts, if the host LUN IDs of the local and remote LUNs in the same HyperMetro pairs are different, data may be inconsistent.

Step 9 Click **OK**.

Confirm your operation as prompted.

----End

5.4.3 Unmapping a LUN

This section describes how to unmap a LUN from a host.

Procedure

Step 1 Choose **Services** > **Block Service** > **LUN Groups** > **LUNs**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Click **More** on the right of the LUN and choose **Unmap**.

The **Unmap LUN** page is displayed on the right.

NOTE

Alternatively, perform either of the following operations to go to the **Unmap LUN** page:

- Click the name of the desired LUN. In the upper right corner of the page that is displayed, select **Unmap** from the **Operation** drop-down list.
- Click the name of the desired LUN. On the page that is displayed, click the **Mapping** tab page, then click **More** on the right of the host, and select **Unmap**.

Step 4 Select one or more objects from **Available Objects**.

NOTE

Skip this step if you unmap a LUN from the **Mapping** tab page.

Step 5 Click **OK**.

Confirm your operation as prompted.

----End

5.4.4 Expanding LUN Capacity

When storage space is insufficient, you need to expand LUNs in time to meet capacity requirements.

Capacity Expansion Methods

For details about capacity expansion, see the administrator guide specific to your product model and version.

5.4.5 Configuring Protection Features

You can configure data protection features for LUNs based on service requirements.

Configuration Guide

For details, see the specific data protection feature guide. For example, to create snapshots for LUNs, refer to the HyperSnap feature guide for block specific to your product model and version.

5.4.6 Adding a Port Group

This section describes how to add a port group for a host.

Procedure

Step 1 Choose **Services** > **Block Service** > **LUN Groups** > **LUNs**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Click the name of the desired LUN. On the page that is displayed, click the **Mapping** tab.

Step 4 Select the desired host and click **Add Port Group**.

The **Add Port Group** page is displayed on the right.

NOTE

Alternatively, choose **Services** > **Block Service** > **VVol** > **PE LUNs** and click the name of the desired PE LUN. On the page that is displayed, click the **Mapping** tab, select the desired host or host group, and click **Add Port Group**.

Step 5 Select a port group.

NOTE

You can click **Create** to create a port group.

Step 6 Click **OK**.

Confirm your operation as prompted.

----End

5.4.7 Removing a Port Group

This section describes how to remove a port group from a host.

Procedure

Step 1 Choose **Services** > **Block Service** > **LUN Groups** > **LUNs**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Click the name of the desired LUN. On the page that is displayed, click the **Mapping** tab.

Step 4 Select the desired host and click **Remove Port Group**.

Confirm your operation as prompted.

----End

5.4.8 Modifying the Properties of a LUN

This section describes how to view or modify the properties of a LUN.

Procedure

Step 1 Choose **Services** > **Block Service** > **LUN Groups** > **LUNs**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Click **More** on the right of the LUN and choose **Modify**.

The **Modify LUN** page is displayed on the right.

NOTE

Alternatively, click the name of the desired LUN. In the upper right corner of the page that is displayed, select **Modify** from the **Operation** drop-down list.

Step 4 Modify the properties of the LUN.

Table 5-25 describes the parameters.

Table 5-25 LUN parameters

Parameter	Description
Name	Name of the LUN. [Value range] • The name must be unique. • The name can contain only letters, digits, periods (.), underscores (_), and hyphens (-). • The name contains 1 to 255 characters.
Description	Description of the LUN. [Value range] The description can be left blank or contain up to 255 characters.
Capacity Alarm Threshold	Indicates whether to enable the capacity alarm threshold function. After the function is enabled, you need to set **Capacity Alarm Threshold (%)**. When **Used** of the LUN reaches the value, the system generates a capacity alarm.
Data Reduction	Indicates whether to enable data reduction. After this function is enabled, the system performs deduplication and compression on LUNs to save storage space. **NOTE** The data reduction switch can be modified only after a SmartDedupe and SmartCompression license is imported to the system.

Step 5 Click **OK**.

----End

5.4.9 Deleting a LUN

This section describes how to delete a LUN to release storage space.

Context

- If the recycle bin is enabled when you delete a LUN, the LUN is moved to the recycle bin. Data on the LUN will be deleted when the retention period elapses. You can restore the LUN in the recycle bin.
- If the recycle bin is disabled when you delete a LUN, the data on the LUN is deleted immediately.

Prerequisites

- The LUN to be deleted is not mapped.
- The child objects of the LUN to be deleted have been deleted or moved to the recycle bin.

Precautions

Before deleting a LUN, verify that the data on it is of no use or has been backed up.

Procedure

Step 1 Choose **Services** > **Block Service** > **LUN Groups** > **LUNs**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Select the desired LUN and click **Delete**.

NOTE

Alternatively, perform either of the following operations to delete LUNs:

- Click **More** on the right of the desired LUN and select **Delete**.
- Click the name of the desired LUN. In the upper right corner of the page that is displayed, select **Delete** from the **Operation** drop-down list.

Step 4 Confirm your operation as prompted.

----End

5.4.10 Managing the Recycle Bin

This section describes how to manage LUNs in the recycle bin.

5.4.10.1 Viewing LUN Information

This section describes how to view information about LUNs in the recycle bin.

Procedure

Step 1 Choose **Services** > **Block Service** > **LUN Groups** > **Recycle Bin**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 View the LUN information in the function pane. **Table 5-26** describes the parameters.

Table 5-26 LUN parameters

Parameter	Description
Name	Name of a LUN. **NOTE** You can click the name of a LUN to view its details and manage it.
ID	ID of a LUN.
Owning vStore	Name of the vStore to which the LUN belongs. **NOTE** This parameter is available only when **vStore** is set to **All vStores** in **Step 2**.
vStore ID	ID of the vStore to which the LUN belongs. **NOTE** This parameter is available only when **vStore** is set to **All vStores** in **Step 2**.
Total	Capacity configured for a LUN.
Allocated	Amount of user data written to a LUN.
WWN	WWN of a LUN.
Deleted	Time when a LUN was moved to the recycle bin.
Parent Object	Name of the parent object of a LUN. **NOTE** This parameter is valid only for snapshot LUNs.
Parent Object ID	ID of the parent object of a LUN. **NOTE** This parameter is valid only for snapshot LUNs.
Child Objects	Number of child objects in a LUN, that is, the number of snapshots and cascading snapshots created using the LUN as the source object.
Deletion Status	Deletion status of a LUN. Possible values are: • **To be deleted**: The LUN is within its retention period. • **Deletion failed**: The LUN has reached its retention period but the system fails to delete it.

Step 4 (Optional) Click the name of a LUN to view its summary and child objects.

NOTE

On the **Child Objects** tab page, you can delete child objects of a LUN.

----End

5.4.10.2 Restoring a LUN

This section describes how to restore a LUN in the recycle bin.

Procedure

Step 1 Choose **Services** > **Block Service** > **LUN Groups** > **Recycle Bin**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Select one or more desired LUNs and click **Restore**.

NOTE

Alternatively, perform either of the following operations to restore a LUN:

- Click **More** on the right of the desired LUN and select **Restore**.
- Click the name of the desired LUN. In the upper right corner of the page that is displayed, select **Restore** from the **Operation** drop-down list.

Step 4 After the LUN is moved to the recycle bin, the name of the newly created LUN can be the same as that of the LUN in the recycle bin. To prevent duplicate names after restoration, you need to set the name of the restored LUN.

NOTE

- The name cannot be the same as that of an existing LUN.
- The name can contain only letters, digits, periods (.), underscores (_), and hyphens (-).
- The name contains 1 to 255 characters.

Step 5 Confirm your operation as prompted.

NOTE

After LUNs are restored, you can choose **Services** > **Block Service** > **LUN Groups** > **LUNs** to manage them.

----End

5.4.10.3 Configuring the Recycle Bin

This section describes how to enable or disable the recycle bin and configure the retention period for LUNs in the recycle bin.

Procedure

Step 1 Choose **Services** > **Block Service** > **LUN Groups** > **Recycle Bin**.

Step 2 Click **Configure Recycle Bin**.

The **Configure Recycle Bin** page is displayed on the right.

NOTE

Step 3 Enable or disable the recycle bin as required:

- Enable

  Set **Retention Period**. The retention period specifies the period of time that a LUN will be retained after being moved to the recycle bin. Data on the LUN will be deleted after the retention period elapses.

  NOTE

  The retention period can be 1 to 168 hours or 1 to 7 days.

- Disable

  NOTE

  After the recycle bin is disabled, the LUNs in the recycle bin will not be deleted. You can manually delete them.

Step 4 Click **OK**.

Confirm your operation as prompted.

----End

5.4.10.4 Deleting a LUN

This section describes how to forcibly delete a LUN from the recycle bin.

Procedure

Step 1 Choose **Services** > **Block Service** > **LUN Groups** > **Recycle Bin**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Select one or more desired LUNs and click **Delete**.

NOTE

Alternatively, perform either of the following operations to delete a LUN:

- Click **More** on the right of the desired LUN and select **Delete**.
- Click the name of the desired LUN. In the upper right corner of the page that is displayed, select **Delete** from the **Operation** drop-down list.

Step 4 Confirm your operation as prompted.

----End

5.5 Managing LUN Groups

This section describes how to manage LUN groups.

5.5.1 Viewing LUN Group Information

This section describes how to view basic information about all LUN groups.

Procedure

Step 1 Choose **Services** > **Block Service** > **LUN Groups** > **LUN Groups**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 View the LUN group information in the function pane. **Table 5-27** describes the parameters.

Table 5-27 LUN group parameters

Parameter	Description
Name	Name of the LUN group. **NOTE** You can click the name of a LUN group to view its details and manage it.
ID	ID of the LUN group.
Owning vStore	Name of the vStore to which the LUN group belongs. **NOTE** This parameter is available only when **vStore** is set to **All vStores** in **Step 2**.
vStore ID	ID of the vStore to which the LUN group belongs. **NOTE** This parameter is available only when **vStore** is set to **All vStores** in **Step 2**.
Capacity	LUN group capacity information, including total capacity of the LUN group and the ratio of used capacity (that is, the allocated capacity) to the total capacity of the LUN group. **NOTE** Move the cursor to **Capacity** of a LUN group to view the total capacity, allocated capacity, and data protection capacity of the LUN group.
Allocated	Amount of user data written to LUNs in the LUN group.
Data Protection	Data protection information about the LUN group.
LUNs	Number of LUNs in the LUN group. **NOTE** You can click the number to view members in the LUN group and manage them.
Mapping	Indicates whether the LUN group has been mapped.

Step 4 (Optional) Click the name of a LUN group to query its summary, member LUNs, topology, mapping, and protection features.

NOTE

- On the **Topology** tab page, if the number of ports in a port group is greater than 3, you can click ••• to view details about all ports. When **Port Type** is **Physical port**, the parameters are described in **Table 5-28**. When **Port Type** is **Logical port**, the parameters are described in **Table 5-29**.
- On the **Topology** tab page, if the number of hosts in a host group is greater than 3, you can click ••• to view details about all hosts. **Table 5-30** describes the parameters.

Table 5-28 Physical port parameters

Parameter	Description
Type	Type of a physical port.
Location	Location of a physical port.
Health Status	Health status of a physical port. • **Unknown**: The system fails to query the port status. • **Normal**: Functions and running performance of the port are normal and without error. • **Bit errors found**: Bit errors occur when the port transmits data. • **Faulty**: The port is functioning improperly and cannot work normally.
Running Status	Working status of a physical port. • **Unknown**: The system fails to query the port status. • **Link up**: A cable is connected to the port. • **Link down**: No cable is connected to the port. • **To be recovered**: For a 4 U device, if the owning controller of a port is faulty, the running status of the port is **To be recovered**.
Usage	Usage of a physical port.

Table 5-29 Logical port parameters

Parameter	Description
Name	Name of a logical port.

Parameter	Description
Running Status	Running status of a logical port. • **Unknown**: The system fails to query the port status. • **Link up**: The running status of the home port of a logical port is link up. • **Link down**: The running status of the home port of a logical port is link down. • **Standby**: In a HyperMetro scenario, when a logical port works at the owning site of the primary or secondary end, the running status of the logical port at the non-owning site of the peer end is **Standby**. • **To be recovered**: When the home port of a logical port is in the **To be recovered** state or a logical port used for the file service fails to be failed over, the running status of the logical port changes to **To be recovered**.
Activation Status	Indicates whether a logical port is activated.
Data Protocol	Data protocol of a logical port.

Table 5-30 Host parameters

Parameter	Description
Name	Member host name.
Health Status	Member host health status.

----End

5.5.2 Adding a Port Group

This section describes how to add a port group for a host or host group that uses the LUN group.

Procedure

Step 1 Choose **Services** > **Block Service** > **LUN Groups** > **LUN Groups**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Click the name of the desired LUN group. On the page that is displayed, click the **Mapping** tab.

Step 4 Select the desired host or host group and click **Add Port Group**.

The **Add Port Group** page is displayed on the right.

Step 5 Select a port group.

NOTE

You can click **Create** to create a port group.

Step 6 Click **OK**.

Confirm your operation as prompted.

----End

5.5.3 Removing a Port Group

This section describes how to remove a port group from a host or host group that uses the LUN group.

Procedure

Step 1 Choose **Services** > **Block Service** > **LUN Groups** > **LUN Groups**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Click the name of the desired LUN group. On the page that is displayed, click the **Mapping** tab.

Step 4 Select the desired host or host group and click **Remove Port Group**.

Confirm your operation as prompted.

----End

5.5.4 Mapping a LUN Group

This section describes how to create a mapping between a LUN group and a host or host group.

Procedure

Step 1 Choose **Services** > **Block Service** > **LUN Groups** > **LUN Groups**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Select the desired LUN group and click **Map**.

The **Map LUN Group** page is displayed on the right.

NOTE

Alternatively, perform either of the following operations to go to the **Map LUN Group** page:

- Click **More** on the right of the desired LUN group and choose **Map**.
- Click the name of the desired LUN group. In the upper right corner of the page that is displayed, select **Map** from the **Operation** drop-down list.

Step 4 Select a host or host group.

NOTE

If no host or host group exists in the system, click **Create** to create one.

Step 5 (Optional) Select a port group.

NOTE

If no port group exists in the system, click **Create**.

Step 6 Set how to assign host LUN IDs.

- **Automatic**: The system assigns a host LUN ID to each LUN mapped to a host.
- **Start ID**: Set a start ID ranging from 0 to 4095. The system assigns a host LUN ID to each LUN mapped to a host, starting from **Start ID**.
- **Specified ID**: Manually assign a host LUN ID to each LUN mapped to a host.

Step 7 Select **Advanced** in the upper right corner and determine whether to select **Same Host LUN ID**. If you select it, the system forcibly ensures that the host LUN IDs of the local and remote LUNs in the same HyperMetro pairs are the same. In SAN-based HyperMetro scenarios involving ESX hosts, if the host LUN IDs of the local and remote LUNs in the same HyperMetro pairs are different, data may be inconsistent.

Step 8 Click **OK**.

Confirm your operation as prompted.

----End

5.5.5 Unmapping a LUN Group

This section describes how to unmap a LUN group from a host or host group.

Procedure

Step 1 Choose **Services** > **Block Service** > **LUN Groups** > **LUN Groups**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Click **More** on the right of the LUN group and choose **Unmap**.

The **Unmap LUN Group** page is displayed on the right.

NOTE

Alternatively, perform either of the following operations to go to the **Unmap LUN Group** page:

- Click the name of the desired LUN group. In the upper right corner of the page that is displayed, select **Unmap** from the **Operation** drop-down list.
- Click the name of the desired LUN group. On the page that is displayed, click the **Mapping** tab page, then click **More** on the right of the host or host group, and select **Unmap**.

Step 4 Select one or more objects from **Available Objects**.

NOTE

Skip this step if you unmap a LUN group from the **Mapping** tab page.

Step 5 Click **OK**.

Confirm your operation as prompted.

----End

5.5.6 Adding a LUN

This section describes how to add a LUN to a LUN group.

Procedure

Step 1 Choose **Services** > **Block Service** > **LUN Groups** > **LUN Groups**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Click **More** on the right of the desired LUN group and choose **Add LUN**.

The **Add LUN** page is displayed on the right.

NOTE

Alternatively, perform any of the following operations to go to the **Add LUN** page:

- Click the name of the desired LUN group. In the upper right corner of the page that is displayed, select **Add LUN** from the **Operation** drop-down list.
- Click the name of the desired LUN group. On the page that is displayed, click the **Member LUNs** tab page, and then click **Add**.
- Click the value in the **LUNs** column of the desired LUN group if the value is not **0**. On the **Member LUNs** tab page, click **Add**.

Step 4 Select one or more LUNs from **Available LUNs** to add them to **Selected LUNs**.

Step 5 If the LUN group has been mapped, select **Advanced** in the upper right corner and set how to assign host LUN IDs.

- **Automatic**: The system assigns a host LUN ID to each LUN mapped to a host.
- **Start ID**: Set a start ID ranging from 0 to 4095. The system assigns a host LUN ID to each LUN mapped to a host, starting from **Start ID**.
- **Specified ID**: Manually assign a host LUN ID to each LUN mapped to a host.

Step 6 If the LUN group has been mapped, determine whether to select **Same Host LUN ID**. If you select it, the system forcibly ensures that the host LUN IDs of the local and remote LUNs in the same HyperMetro pairs are the same. In SAN-based HyperMetro scenarios involving ESX hosts, if the host LUN IDs of the local and remote LUNs in the same HyperMetro pairs are different, data may be inconsistent.

Step 7 If remote replication, HyperMetro, or DR Star is configured for the LUN group, add LUNs by referring to the feature guide of the corresponding version and model.

Step 8 Click **OK**.

Confirm your operation as prompted.

NOTE

After the task is created successfully, the **Execution Result** page is displayed. You can view details about the current task on this page.

----End

5.5.7 Removing a LUN

This section describes how to remove a LUN from a LUN group.

Procedure

Step 1 Choose **Services** > **Block Service** > **LUN Groups** > **LUN Groups**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Click **More** on the right of the desired LUN group and choose **Remove LUN**.

The **Remove LUN** page is displayed on the right.

NOTE

Alternatively, perform any of the following operations to remove LUNs:

- Click the name of the desired LUN group. In the upper right corner of the page that is displayed, select **Remove LUN** from the **Operation** drop-down list.
- Click the name of the desired LUN group. On the page that is displayed, click the **Member LUNs** tab page, select the desired LUNs, and click **Remove**.
- Click the value in the **LUNs** column of the desired LUN group if the value is not **0**. On the **Member LUNs** tab page, select the desired LUNs, and click **Remove**.

Step 4 Select one or more LUNs from **Available LUNs** to add them to **Selected LUNs**.

NOTE

- Skip this step if you remove LUNs from the **Member LUNs** tab page.
- If a HyperMetro or remote replication consistency group (CG) has been created for the LUN group, the related HyperMetro or remote replication pair will be removed from the CG after you remove a LUN.
- If a DR Star trio has been created for the LUN group, when you remove a LUN from the LUN group, the HyperMetro pair and two remote replication pairs corresponding to the LUN are removed from the HyperMetro CG and two remote replication CGs that form the DR Star trio.

Step 5 Click **OK**.

Confirm your operation as prompted.

NOTE

If a HyperMetro or remote replication CG or DR Star trio has been created for the LUN group, after the task is created successfully, the **Execution Result** page is displayed. You can view details about the current task on this page.

----End

5.5.8 Configuring Protection Features

You can configure data protection features for a LUN group based on service requirements.

Configuration Guide

For details, see the specific data protection feature guide. For example, to create snapshots for a LUN group, refer to the HyperSnap feature guide for block specific to your product model and version.

5.5.9 Modifying the Properties of a LUN Group

This section describes how to modify the properties of a LUN group.

Procedure

Step 1 Choose **Services** > **Block Service** > **LUN Groups** > **LUN Groups**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Click **More** on the right of the desired LUN group and choose **Modify**.

The **Modify LUN Group** page is displayed on the right.

NOTE

Alternatively, click the name of the desired LUN group. In the upper right corner of the page that is displayed, select **Modify** from the **Operation** drop-down list.

Step 4 Modify the properties of the LUN group.

1. Modify the **Name** of the LUN group.

   NOTE

   - The name must be unique.
   - The name can contain only letters, digits, periods (.), underscores (_), and hyphens (-).
   - The name contains 1 to 255 characters.

2. Input necessary information about the LUN group in **Description** to help you identify the LUN group.

Step 5 Click **OK**.

----End

5.5.10 Deleting a LUN Group

This section describes how to delete a LUN group to release storage space.

Prerequisites

The LUN group to be deleted has not been mapped.

Procedure

Step 1 Choose **Services** > **Block Service** > **LUN Groups** > **LUN Groups**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Click **More** on the right of the desired LUN group and choose **Delete**.

NOTE

Alternatively, click the name of the desired LUN group. In the upper right corner of the page that is displayed, select **Delete** from the **Operation** drop-down list.

Step 4 Confirm your operation as prompted.

----End

5.6 Managing VVol

This section describes how to manage VVol.

5.6.1 Creating a PE LUN

This section describes how to create a PE LUN.

Context

PE LUNs are only used by virtual volumes (VVols) in VMware software-defined storage. VVols provide storage space for VMs. A PE LUN is used as an I/O distributor to simplify the connection between a VM and a VVol. I/Os from a VM are sent to the VVol through a PE LUN.

Procedure

Step 1 Choose **Services** > **Block Service** > **VVol** > **PE LUNs**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Click **Create**.

The **Create PE LUN** page is displayed on the right.

NOTE

The screenshot is for reference only and the actual GUI may vary.

Step 4 Set the PE LUN parameters.

Table 5-31 describes the parameters.

Table 5-31 PE LUN parameters

Parameter	Description
Name	Name of the PE LUN. [Value range] • The name must be unique. • The name can contain only letters, digits, periods (.), underscores (_), and hyphens (-). • The name contains 1 to 255 characters.
Owning vStore	vStore to which the newly created PE LUN belongs. **NOTE** This parameter is mandatory when **vStore** is set to **All vStores** in Step 2.
Description	Description of the PE LUN. [Value range] The description can be left blank or contain up to 255 characters.
Owning Storage Pool	Storage pool to which the PE LUN belongs.
Quantity	Number of PE LUNs created in a batch. Set this parameter based on site requirements. [Value range] 1 to 64
Start Number	Start number from which the system incrementally adds a suffix number to the name of each PE LUN for distinction. [Value range] 0 to (10000 – Number of PE LUNs created in a batch) **NOTE** • This parameter is displayed only when **Quantity** is greater than **1** and **Advanced** is selected. • For example, if you want to create 300 PE LUNs, the value range of **Start Number** is 0 to 9700.
Map to Host	Host to which the PE LUN you are creating is mapped. **NOTE** • If no host is available in the system, click **Create**. • You can also map the PE LUNs after you have created them. • This parameter is displayed only when **Add to LUN Group** is not selected.
Add to LUN Group	Determines whether to add the PE LUN to a LUN group.

Parameter	Description
LUN Group	After selecting **Add to LUN Group**, you must choose a LUN group. **NOTE** You can click **Create** to create a LUN group.
Map To	Specifies the host or host group to which the LUN group is mapped. **NOTE** You can click **Create** to create a host or host group.
Port Group	Port group you want to use for the mapping. **NOTE** • This option is displayed after you have selected a host or host group. • If no port group exists in the system, click **Create**.
Host LUN ID	Method to assign IDs. • **Automatic** A host LUN ID is allocated by the storage system to a LUN mapped to a host. If you select **Automatic**, the system automatically allocates a unique host LUN ID to each LUN. • **Start ID** The system automatically allocates a unique host LUN ID to each LUN, starting from **Start ID**.
Start ID	Start number for host LUN IDs. [Value range] 0 to 4095 **NOTE** This parameter is displayed only when **Host LUN ID** is **Start ID**.

NOTE

The **Description**, **Start Number**, and **Host LUN ID** are hidden parameters. You can click **Advanced** to display them.

Step 5 Click **OK**.

Confirm your operation as prompted.

----End

5.6.2 Viewing PE LUNs

This section describes how to view the basic information about PE LUNs.

Context

- On the PE LUN management page, click to refresh PE LUN information.

- On the PE LUN management page, click or next to a parameter, and enter a keyword or select a value to search for the desired PE LUNs.
- On the PE LUN management page, click and select the PE LUN parameters you want to view.

Procedure

Step 1 Choose **Services** > **Block Service** > **VVol** > **PE LUNs**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 View the PE LUN information in the function pane. **Table 5-32** describes the parameters.

Table 5-32 PE LUN parameters

Parameter	Description
Name	Name of the PE LUN.
ID	ID of the PE LUN.
Owning vStore	Name of the vStore to which the PE LUN belongs. **NOTE** This parameter is available only when **vStore** is set to **All vStores** in **Step 2**.
vStore ID	ID of the vStore to which the PE LUN belongs. **NOTE** This parameter is available only when **vStore** is set to **All vStores** in **Step 2**.
Capacity	Capacity of the PE LUN.
Health Status	Health status of the PE LUN.
Running Status	Running status of the PE LUN.
Owning Storage Pool	Storage pool to which the PE LUN belongs.
Local WWN	Local WWN of the PE LUN.
NGUID	Unique identifier of the namespace of a PE LUN.
Mapping	Indicates whether the PE LUN has been mapped to a host.
Use Type	Usage type of the LUN. The value is **PE LUNs**.

Step 4 (Optional) Click the name of a PE LUN to view its **Summary**, **Topology**, and **Mapping**.

NOTE

- If a PE LUN has been added to multiple LUN groups, click the **Summary** tab on the details page, and click **More** on the right of **Owning LUN Groups**. On the **Owning LUN Groups** page that is displayed, view the names and IDs of the owning LUN groups.
- On the **Topology** tab page, if the number of ports in a port group is greater than 3, you can click ••• to view details about all ports. When **Port Type** is **Physical port**, the parameters are described in **Table 5-33**. When **Port Type** is **Logical port**, the parameters are described in **Table 5-34**.

Table 5-33 Physical port parameters

Parameter	Description
Type	Type of a physical port.
Location	Location of a physical port.
Health Status	Health status of a physical port. • **Unknown**: The system fails to query the port status. • **Normal**: Functions and running performance of the port are normal and without error. • **Bit errors found**: Bit errors occur when the port transmits data. • **Faulty**: The port is functioning improperly and cannot work normally.
Running Status	Working status of a physical port. • **Unknown**: The system fails to query the port status. • **Link up**: A cable is connected to the port. • **Link down**: No cable is connected to the port. • **To be recovered**: For a 4 U device, if the owning controller of a port is faulty, the running status of the port is **To be recovered**.
Usage	Usage of a physical port.

Table 5-34 Logical port parameters

Parameter	Description
Name	Name of a logical port.

Parameter	Description
Running Status	Running status of a logical port. • **Unknown**: The system fails to query the port status. • **Link up**: The running status of the home port of a logical port is link up. • **Link down**: The running status of the home port of a logical port is link down. • **Standby**: In a HyperMetro scenario, when a logical port works at the owning site of the primary or secondary end, the running status of the logical port at the non-owning site of the peer end is **Standby**. • **To be recovered**: When the home port of a logical port is in the **To be recovered** state or a logical port used for the file service fails to be failed over, the running status of the logical port changes to **To be recovered**.
Activation Status	Indicates whether a logical port is activated.
Data Protocol	Data protocol of a logical port.

----End

5.6.3 Modifying a PE LUN

This section describes how to modify the name and description of a PE LUN.

Procedure

Step 1 Choose **Services** > **Block Service** > **VVol** > **PE LUNs**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 Click **More** on the right of the desired PE LUN and choose **Modify**.

The **Modify PE LUN** page is displayed on the right.

NOTE

Alternatively, click the name of the desired PE LUN. In the upper right corner of the page that is displayed, select **Modify** from the **Operation** drop-down list.

Step 4 Modify the name of the PE LUN.

NOTE

- The name must be unique.
- The name can contain only letters, digits, periods (.), underscores (_), and hyphens (-).
- The name contains 1 to 255 characters.

Step 5 Modify the description of the PE LUN.

NOTE

The description can be left blank or contain up to 255 characters.

Step 6 Click **OK**.

----End

5.6.4 Adding a Port Group

This section describes how to add a port group for a host or host group that uses the PE LUN.

Procedure

Step 1 Choose **Services** > **Block Service** > **VVol** > **PE LUNs**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 Click the name of the desired PE LUN. On the page that is displayed, click the **Mapping** tab.

Step 4 Select the desired host or host group and click **Add Port Group**.

The **Add Port Group** page is displayed on the right.

Step 5 Select a port group.

NOTE

You can click **Create** to create a port group.

Step 6 Click **OK**.

Confirm your operation as prompted.

----End

5.6.5 Removing a Port Group

This section describes how to remove a port group from a host or host group that uses the PE LUN.

Procedure

Step 1 Choose **Services** > **Block Service** > **VVol** > **PE LUNs**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 Click the name of the desired PE LUN. On the page that is displayed, click the **Mapping** tab.

Step 4 Select the desired host or host group and click **Remove Port Group**.

Confirm your operation as prompted.

----End

5.6.6 Modifying Host LUN IDs

This section describes how to modify the LUN ID for a host or host group that uses the PE LUN.

Procedure

Step 1 Choose **Services** > **Block Service** > **VVol** > **PE LUNs**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 Click the name of the desired PE LUN. On the page that is displayed, click the **Mapping** tab.

Step 4 Click **More** on the right of the desired host or host group and choose **Modify Host LUN ID**.

The **Modify Host LUN ID** page is displayed on the right.

Step 5 Set **Host LUN ID**. The value ranges from 0 to 4095.

Step 6 Click **OK**.

----End

5.6.7 Mapping a PE LUN

This section describes how to create one-to-one or many-to-one mapping relationships between PE LUNs and hosts.

Procedure

Step 1 Choose **Services** > **Block Service** > **VVol** > **PE LUNs**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 Select the desired PE LUN and click **Map**.

The **Map PE LUN** page is displayed on the right.

NOTE

Alternatively, perform any of the following operations to go to the **Map PE LUN** page:

- Click **More** on the right of the desired PE LUN and select **Map**.
- Click the name of the desired PE LUN. In the upper right corner of the page that is displayed, select **Map** from the **Operation** drop-down list.

Step 4 Select the PE LUNs you want to map. Click ▶ on the right of **Selected LUNs**. In the **Available LUNs** list, select the desired LUNs and add them to **Selected LUNs**.

NOTE

Skip this step if you want to map each PE LUN separately.

Step 5 Select a host.

NOTE

You can click **Create** to create a host.

Step 6 Select a port group.

NOTE

You can click **Create** to create a port group.

Step 7 Select **Advanced** in the upper right corner and set how to assign host LUN IDs.

- **Automatic**

  A host LUN ID is allocated by the storage system to a LUN mapped to a host. If you select **Automatic**, the system automatically allocates a unique host LUN ID to each LUN.

- **Start ID**

  The system automatically allocates a unique host LUN ID to each LUN, starting from **Start ID**.

Step 8 Click **OK**.

Confirm your operation as prompted.

----End

5.6.8 Unmapping a PE LUN

This section describes how to unmap a PE LUN from a host.

Procedure

Step 1 Choose **Services** > **Block Service** > **VVol** > **PE LUNs**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 Click **More** on the right of the desired PE LUN and choose **Unmap**.

The **Unmap PE LUN** page is displayed on the right.

NOTE

Alternatively, perform either of the following operations to go to the **Unmap PE LUN** page:

- Click the name of the desired PE LUN. In the upper right corner of the page that is displayed, select **Unmap** from the **Operation** drop-down list.
- Click the name of the desired PE LUN. On the page that is displayed, click the **Mapping** tab page, then click **More** on the right of the host, and select **Unmap**.

Step 4 Select one or more objects from **Available Objects**.

NOTE

This step is not needed if you unmap a PE LUN from the **Mapping** tab page.

Step 5 Click **OK**.

Confirm your operation as prompted.

----End

5.6.9 Deleting a PE LUN

This section describes how to delete a PE LUN to release storage space.

Prerequisites

The PE LUN you want to delete has not been mapped.

Precautions

Before deleting a PE LUN, confirm that its data is of no use or has been backed up.

Procedure

Step 1 Choose **Services** > **Block Service** > **VVol** > **PE LUNs**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 Select the desired PE LUN and click **Delete**.

NOTE

Alternatively, perform either of the following operations to delete a PE LUN:

- Click **More** on the right of the desired PE LUN and select **Delete**.
- Click the name of the desired PE LUN. In the upper right corner of the page that is displayed, select **Delete** from the **Operation** drop-down list.

Step 4 Confirm your operation as prompted.

----End

5.6.10 Viewing VVol LUNs

This section describes how to view the basic information about VVol LUNs.

Context

- On the VVol LUN management page, click to refresh VVol LUN information.
- On the VVol LUN management page, click or next to a parameter, and enter a keyword or select a value to search for the desired VVol LUNs.
- On the VVol LUN management page, click and select the VVol LUN parameters you want to view.

Procedure

Step 1 Choose **Services** > **Block Service** > **VVol** > **VVol LUNs**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 View the VVol LUN information in the function pane. **Table 5-35** describes the parameters.

Table 5-35 VVol LUN parameters

Parameter	Description
Name	Name of the VVol LUN.
ID	ID of the VVol LUN.
Owning vStore	Name of the vStore to which the VVol LUN belongs. **NOTE** This parameter is available only when **vStore** is set to **All vStores** in **Step 2**.
vStore ID	ID of the vStore to which the VVol LUN belongs. **NOTE** This parameter is available only when **vStore** is set to **All vStores** in **Step 2**.
Capacity	Capacity of the VVol LUN.
Health Status	Health status of the VVol LUN.
Running Status	Running status of the VVol LUN.
Data Protection	Data protection information about the VVol LUN.
Owning Storage Pool	Storage pool to which the VVol LUN belongs.
Local WWN	Local WWN of the VVol LUN.
NGUID	Unique identifier of the namespace of a VVol LUN.

Parameter	Description
Function Type	Function type of a VVol LUN. Possible values are **LUN** and **Snapshot**.
Use Type	Usage type of the LUN. The value is **VVol LUNs**, indicating that the LUN provides storage space for VMware VMs.

Step 4 (Optional) Click the name of a VVol LUN to view its summary and protection information.

NOTE

The snapshots, remote replication pairs, and HyperCDP objects of VVol LUNs can only be viewed, but cannot be configured and managed on DeviceManager.

----End

5.7 Managing Hosts

This section describes how to manage hosts.

5.7.1 Viewing Host Information

This section describes how to view the information about all hosts.

Procedure

Step 1 Choose **Services** > **Block Service** > **Host Groups** > **Hosts**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 On the **Hosts** tab page, view the host information in the function pane. **Table 5-36** describes the parameters.

Table 5-36 Host parameters

Parameter	Description
Name	Name of the host. **NOTE** You can click the name of a host to view its details and manage it.
ID	ID of the host.

Parameter	Description
Owning vStore	Name of the vStore to which the host belongs. **NOTE** This parameter is available only when **vStore** is set to **All vStores** in **Step 2**.
vStore ID	ID of the vStore to which the host belongs. **NOTE** This parameter is available only when **vStore** is set to **All vStores** in **Step 2**.
Health Status	Health status of the host. [Value range] **Normal**, **Offline**, or **No redundant link** [Example] Normal
OS	Operating system used by the host. [Example] Linux
LUN Capacity Usage	Capacity usage of the LUNs mapped to the host.
Owning Host Group	Indicates whether the host has been added to a host group.
IP Address	IP address of the host.
Initiators	Number of initiators on the host. **NOTE** When the number of initiators is not 0, you can click the number to view details about the initiators.

----End

5.7.2 Viewing Path Details

This section describes how to view the path details of a host.

Procedure

Step 1 Choose **Services** > **Block Service** > **Host Groups** > **Hosts**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 On the **Hosts** tab page, click the name of the desired host. Click the **Path Details** tab.

Step 4 View path details. **Table 5-37** describes the related parameters.

Table 5-37 Path details parameters

Parameter	Description
Health Status	Health status of the path. [Example] Normal
Link Status	Link status of the path. [Example] Online
Initiator Type	Type of the initiator. [Example] iSCSI
Initiator Identifier	Identifier of the initiator
Target Identifier	Identifier of the target
Port	Local port of the path.
Initiator Alias	Alias of the initiator.
Host	Host associated with the path.
Host IP Address	IP address of a host.

NOTE

You can click to refresh the path information.

----End

5.7.3 Viewing Host LUN IDs

A host LUN ID is allocated by the storage system to a LUN mapped to a host. This ID is visible on the host.

Procedure

Step 1 Choose **Services** > **Block Service** > **Host Groups** > **Hosts**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 On the **Hosts** tab page, click the name of the desired host. On the page that is displayed, click the **Mapping** tab page.

Step 4 Click **View Host LUN ID**.

The **View Host LUN ID** page is displayed on the right.

Step 5 View the LUNs mapped to the host and their host LUN IDs.

----End

5.7.4 Modifying Host LUN IDs

This section describes how to modify host LUN IDs.

Prerequisites

Host services on the LUN have been stopped, and the virtual disk created by multipathing software and physical disk corresponding to the LUN have been uninstalled from the host.

Procedure

Step 1 Choose **Services** > **Block Service** > **Host Groups** > **Hosts**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 On the **Hosts** tab page, click the name of the desired host. On the page that is displayed, click the **Mapping** tab.

Step 4 Click **More** on the right of the desired LUN or LUN group and choose **Modify Host LUN ID**.

The **Modify Host LUN ID** page is displayed on the right.

NOTE

Alternatively, perform either of the following operations to go to the **Modify Host LUN ID** page:

- On the **Mapping** tab page, click **View Host LUN ID**. On the **View Host LUN ID** page that is displayed, click **Modify** in the upper right corner.
- Choose **Services** > **Block Service** > **LUN Groups** > **LUNs** and click the name of the desired LUN. On the page that is displayed, click the **Mapping** tab, then click **More** on the right of the host, and choose **Modify Host LUN ID**.
- Choose **Services** > **Block Service** > **LUN Groups** > **LUN Groups** and click the name of the desired LUN group. On the page that is displayed, click the **Mapping** tab, then click **More** on the right of the host or host group, and choose **Modify Host LUN ID**.

Step 5 Set the host LUN ID for each LUN. The value ranges from 0 to 4095.

Step 6 If HyperMetro pairs have been created for the LUNs or a LUN group is selected, select **Advanced** in the upper right corner and determine whether to select **Same Host LUN ID**. If you select it, the system checks whether the host LUN IDs of the local and remote LUNs in the same HyperMetro pairs are the same when you

change the host LUN IDs. In SAN-based HyperMetro scenarios involving ESX hosts, if the host LUN IDs of the local and remote LUNs in the same HyperMetro pairs are different, data may be inconsistent.

Step 7 Click **OK**.

----End

Follow-up Procedure

After a host LUN ID is modified, re-scan for disks on the host.

5.7.5 Adding a Port Group

This section describes how to add a port group for a LUN group.

Procedure

Step 1 Choose **Services** > **Block Service** > **Host Groups** > **Hosts**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 On the **Hosts** tab page, click the name of the desired host. On the page that is displayed, click the **Mapping** tab page.

Step 4 Select the desired LUN group and click **Add Port Group**.

The **Add Port Group** page is displayed on the right.

Step 5 Select a port group.

NOTE

You can click **Create** to create a port group.

Step 6 Click **OK**.

Confirm your operation as prompted.

----End

5.7.6 Removing a Port Group

This section describes how to remove a port group for a LUN group.

Procedure

Step 1 Choose **Services** > **Block Service** > **Host Groups** > **Hosts**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 On the **Hosts** tab page, click the name of the desired host. On the page that is displayed, click the **Mapping** tab page.

Step 4 Select the desired LUN group and click **Remove Port Group**.

Confirm your operation as prompted.

----End

5.7.7 Mapping a LUN Group to a Host

This section describes how to create a mapping between a host and a LUN group.

Procedure

Step 1 Choose **Services** > **Block Service** > **Host Groups** > **Hosts**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 On the **Hosts** tab page, select the desired host and choose **Map** > **Map LUN Group**.

The **Map LUN Group** page is displayed on the right.

NOTE

Alternatively, perform either of the following operations to go to the **Map LUN Group** page:

- Click **More** on the right of the desired host and choose **Map LUN Group**.
- Click the name of the desired host. In the upper right corner of the page that is displayed, select **Map LUN Group** from the **Operation** drop-down list.

Step 4 Select a LUN group.

- If you select **New**:
  a. Set the name of the new LUN group.
  b. Select the storage pool to which the LUN group belongs. Set **Application Type** for LUNs.

     NOTE

     The following preset application types are provided for typical applications: **Default**, **Oracle_OLAP**, **Oracle_OLTP**, **Oracle_OLAP&OLTP**, **SQL_Server_OLAP**, **SQL_Server_OLTP**, **SQL_Server_OLAP&OLTP**, **SAP_HANA**, **Vmware_VDI**, **Hyper-V_VDI**, and **FusionAccess_VDI**.

     - After you have set an application type for a LUN, you are unable to change it in follow-up operations.
     - If the application type configured for a LUN does not match the actual I/O model, the LUN performance may deteriorate.
     - If none of the preset application types matches the actual I/O model, you can run the **create lun_workload_type general** command to create one. For details on this command, refer to the *Command Reference*.

c. Specify the LUN name prefix, capacity per LUN, and quantity. **Table 5-38** describes the parameters.

Table 5-38 LUN parameters

Parameter	Description
Name Prefix	Name prefix of the LUN. The names of the new LUNs are numbered in sequence based on the name prefix.
Capacity per LUN	Capacity of the LUN in the LUN group. **NOTE** ■ The maximum capacity of the LUN must not exceed the system specifications. ■ You can set the capacity unit to **Blocks** to create LUNs by block. A block is equal to 512 bytes. The LUN capacity must not be smaller than 1024 blocks (that is, 512 KB). ■ The storage system uses the following capacity algorithms defined by Windows: 1 PB = 1,024 TB, 1 TB = 1,024 GB, 1 GB = 1,024 MB, 1 MB = 1,024 KB, and 1 KB = 1,024 bytes.
Quantity	Number of LUNs created in a batch. Set this parameter based on site requirements. [Value range] 1 to 500 **NOTE** ■ LUNs created in a batch have the same capacity. ■ When LUNs are created in a batch, the system automatically adds suffixes to the names based on the number of LUNs for distinction. You can click ⚙ to manually specify the start number for the suffixes.

d. (Optional) When creating LUNs in a batch, click ⚙ and set the suffixes of the LUNs. Related parameters include **Suffix Digits** and **Suffix** (start number of the suffixes). The system adds a suffix to the end of each LUN name in ascending order based on the specified start suffix number.

NOTE

■ The value range of **Suffix** is 0 to (10000 – **Quantity**).

■ For example, if you want to create 300 LUNs, the value range of **Suffix** is 0 to 9700.

e. (Optional) Click + to add more LUNs.

f. (Optional) Click — to remove LUNs.

- If you select **Existing**:

  Select a LUN group from the list.

NOTE

You can select **Include mapped LUN groups** to query the LUN groups that have been mapped to the current host. For these LUN groups, mapping cannot be created repeatedly.

Step 5 (Optional) Select a port group.

NOTE

If no port group exists in the system, click **Create**.

Step 6 Set how to assign host LUN IDs.

- **Automatic**: The system assigns a host LUN ID to each LUN mapped to a host.
- **Start ID**: Set a start ID ranging from 0 to 4095. The system assigns a host LUN ID to each LUN mapped to a host, starting from **Start ID**.
- **Specified ID**: Manually assign a host LUN ID to each LUN mapped to a host.

Step 7 If you select an existing LUN group, select **Advanced** in the upper right corner and determine whether to select **Same Host LUN ID**. If you select it, the system forcibly ensures that the host LUN IDs of the local and remote LUNs in the same HyperMetro pairs are the same. In SAN-based HyperMetro scenarios involving ESX hosts, if the host LUN IDs of the local and remote LUNs in the same HyperMetro pairs are different, data may be inconsistent.

Step 8 Click **OK**.

Confirm your operation as prompted.

NOTE

After the task is created successfully, the **Execution Result** page is displayed. You can view details about the current task on this page.

----End

5.7.8 Mapping LUNs to a Host

This section describes how to create a mapping between a host and LUNs.

Procedure

Step 1 Choose **Services** > **Block Service** > **Host Groups** > **Hosts**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 On the **Hosts** tab page, select the desired host and choose **Map** > **Map LUN**.

The **Map LUN** page is displayed on the right.

NOTE

Alternatively, perform either of the following operations to go to the **Map LUN** page:

- Click **More** on the right of the desired host and choose **Map LUN**.
- Click the name of the desired host. In the upper right corner of the page that is displayed, select **Map LUN** from the **Operation** drop-down list.

Step 4 Select LUNs.

- If you select **New**:
  a. Set the LUN parameters.
  Table 5-39 describes the parameters.

Table 5-39 LUN parameters

Parameter	Description
Name	Name of the LUN. **NOTE** [Value range] ■ The name must be unique. ■ The name can contain only letters, digits, periods (.), underscores (_), and hyphens (-). ■ The name contains 1 to 255 characters.
Owning Storage Pool	Storage pool to which the LUN you are creating belongs.
Capacity	Capacity of the LUN. **NOTE** ■ The maximum capacity of the LUN must not exceed the system specifications. ■ You can set the capacity unit to **Blocks** to create LUNs by block. A block is equal to 512 bytes. The LUN capacity must not be smaller than 1024 blocks (that is, 512 KB). ■ The storage system uses the following capacity algorithms defined by Windows: 1 PB = 1,024 TB, 1 TB = 1,024 GB, 1 GB = 1,024 MB, 1 MB = 1,024 KB, and 1 KB = 1,024 bytes.
Quantity	Number of LUNs created in a batch. Set this parameter based on site requirements. [Value range] 1 to 500 **NOTE** LUNs created in a batch have the same capacity.

Parameter	Description
Suffix Digits	Number of digits in the suffixes of the LUNs to be created in a batch. **NOTE** This parameter is displayed only when **Quantity** is greater than **1**.
Suffix	Set the start number of the suffixes of the LUNs to be created in a batch. The system adds a suffix to the end of each LUN name in ascending order based on the specified start suffix number. **NOTE** ■ This parameter is displayed only when **Quantity** is greater than **1**. ■ The value range of **Suffix** is 0 to (10000 – **Quantity**). ■ For example, if you want to create 300 LUNs, the value range of **Suffix** is 0 to 9700.
Application Type	Application type of the LUN. The following preset application types are provided for typical applications: **Default**, **Oracle_OLAP**, **Oracle_OLTP**, **Oracle_OLAP&OLTP**, **SQL_Server_OLAP**, **SQL_Server_OLTP**, **SQL_Server_OLAP&OLTP**, **SAP_HANA**, **Vmware_VDI**, **Hyper-V_VDI**, and **FusionAccess_VDI**. **NOTE** ■ After you have set an application type for a LUN, you are unable to change it in follow-up operations. ■ If the application type configured for a LUN does not match the actual I/O model, the LUN performance may deteriorate. ■ If none of the preset application types matches the actual I/O model, you can run the **create lun_workload_type general** command to create one. For details on this command, refer to the *Command Reference*.

- If you select **Existing**:

  Select one or more LUNs from **Available LUNs** to add them to **Selected LUNs**.

  NOTE

  You can select **Include mapped LUNs** to query the LUNs that have been mapped to the current host. For these LUNs, mapping cannot be created repeatedly.

Step 5 (Optional) Select a port group.

NOTE

- If no port group exists in the system, click **Create**.
- After a port group is selected, LUNs use the ports of the port group to communicate with hosts in the host group. If no port group is selected, available ports are randomly used.

Step 6 Set how to assign host LUN IDs.

- **Automatic**: The system assigns a host LUN ID to each LUN mapped to a host.
- **Start ID**: Set a start ID ranging from 0 to 4095. The system assigns a host LUN ID to each LUN mapped to a host, starting from **Start ID**.
- **Specified ID**: Manually assign a host LUN ID to each LUN mapped to a host.

Step 7 If HyperMetro pairs have been created for the selected LUNs, select **Advanced** in the upper right corner and determine whether to select **Same Host LUN ID**. If you select it, the system forcibly ensures that the host LUN IDs of the local and remote LUNs in the same HyperMetro pairs are the same. In SAN-based HyperMetro scenarios involving ESX hosts, if the host LUN IDs of the local and remote LUNs in the same HyperMetro pairs are different, data may be inconsistent.

Step 8 Click **OK**.

Confirm your operation as prompted.

NOTE

After the task is created successfully, the **Execution Result** page is displayed. You can view details about the current task on this page.

----End

5.7.9 Unmapping a Host

This section describes how to cancel the mapping between a host and LUNs or a LUN group.

Procedure

Step 1 Choose **Services** > **Block Service** > **Host Groups** > **Hosts**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 On the **Hosts** tab page, click **More** on the right of the desired host and choose **Unmap**.

The **Unmap Object** page is displayed on the right.

NOTE

Alternatively, perform either of the following operations to go to the **Unmap Object** page:

- Click the name of the desired host. In the upper right corner of the page that is displayed, select **Unmap** from the **Operation** drop-down list.
- Click the name of the desired host. On the page that is displayed, click the **Mapping** tab page, then click **More** on the right of the LUN or LUN group, and select **Unmap**.

Step 4 Select one or more objects from **Available Objects**.

NOTE

Skip this step if you cancel the mapping between a host and LUNs or a LUN group from the **Mapping** tab page.

Step 5 Click **OK**.

Confirm your operation as prompted.

----End

5.7.10 Scanning for Hosts

This section describes how to scan for hosts to add detected hosts to the host list.

Prerequisites

The host scanning function has been enabled on the **Block Service** page (**Settings** > **Block Service**).

Procedure

Step 1 Choose **Services** > **Block Service** > **Host Groups** > **Hosts**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 On the **Hosts** tab page, click **Scan for Host**.

----End

5.7.11 Adding an Initiator

This section describes how to add an initiator to a host.

Procedure

Step 1 Choose **Services** > **Block Service** > **Host Groups** > **Hosts**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 On the **Hosts** tab page, click **More** on the right of the desired host and choose **Add Initiator**.

The **Add Initiator** page is displayed on the right.

NOTE

Alternatively, perform either of the following operations to go to the **Add Initiator** page:

- Click the name of the desired host. In the upper right corner of the page that is displayed, select **Add Initiator** from the **Operation** drop-down list.
- Click the name of the desired host. On the page that is displayed, click the **Initiators** tab page, and then click **Add**.

Step 4 Select initiators.

1. Select an initiator type (FC, iSCSI, or NVMe over RoCE) based on service requirements.
2. For an FC initiator, you need to select the vStore to which the initiator belongs. An FC initiator whose owning vStore is the same as that of the created host or whose owning vStore is **--** can be added to the host.

   For iSCSI and NVMe over RoCE initiators, you can only add initiators whose owning vStore is the same as that of the created host to the host.
3. Select one or more initiators from **Available Initiators**.

Step 5 (Optional) Click **Create Initiator**. On the **Create Initiator** page that is displayed, set the related parameters.

NOTE

- If initiators have been configured on an application server:
  - When initiators can be automatically discovered on DeviceManager, skip this step.
  - When initiators cannot be automatically discovered on DeviceManager, create initiators using the IQNs or WWPNs of initiators configured on the application server.
- If no initiator has been configured on an application server, configure initiators by following instructions in **Configuring Connectivity** in the corresponding *Host Connectivity Guide* and then add initiators on DeviceManager.
- On DeviceManager, set parameters of initiators manually created or automatically discovered based on the multipathing software and host operating system version. For details about recommended parameter settings in different scenarios, see **Configuring Multipathing** in the corresponding *Host Connectivity Guide*. For iSCSI initiators, you need to set CHAP authentication parameters based on the security authentication plan.

Table 5-40 describes the FC initiator parameters.

Table 5-40 FC initiator parameters

Parameter	Description
WWPN	World Wide Port Name (WWPN) of the initiator. [Value range] A WWPN is a hexadecimal value that contains 16 characters. It can contain letters A to F (uppercase and lowercase) and digits 0 to 9. It cannot be all 0, all F, or all f.

Parameter	Description
Alias	Alias of the initiator. [Value range] • An alias can be left blank or contain up to 31 characters. • The name can contain only letters, digits, periods (.), underscores (_), and hyphens (-).

Table 5-41 describes the iSCSI initiator parameters.

Table 5-41 iSCSI initiator parameters

Parameter	Description
IQN	iSCSI Qualified Name (IQN) of the iSCSI initiator. **NOTE** The IQN of an initiator must be the same as the one on the application server. The IQN of an initiator must be unique. Do not configure the initiators of multiple application servers with the same IQN. [Value range] An IQN must contain 1 to 223 visible ASCII characters and start with a digit or letter.
Alias	Alias of the iSCSI initiator. [Value range] • An alias can be left blank or contain up to 31 characters. • The name can contain only letters, digits, periods (.), underscores (_), and hyphens (-).
CHAP	CHAP authentication includes **Normal Authentication** and **Discovery Authentication** options. • If you enable CHAP, you must configure a CHAP name and password for the storage system and the same CHAP name and password on the application server. • If you do not enable CHAP, you do not need to configure a CHAP name or password. **NOTE** After changing the CHAP authentication password on the storage system, you must use the new password to configure the CHAP authentication again on the application server.

Parameter	Description
Normal Authentication	The normal session is the process during which the target and initiator transmit data between each other after connections have been set up. Authentication modes include: • No authentication • Unidirectional authentication The target authenticates the initiator. • Bidirectional authentication The target and initiator authenticate each other.
Discovery Authentication	The discovery session is the process during which the target and initiator are setting up connections. Authentication modes include: • No authentication • Unidirectional authentication The target authenticates the initiator. • Bidirectional authentication The target and initiator authenticate each other. **NOTE** When **Normal Authentication** or **Discovery Authentication** is set to **Bidirectional authentication**, you need to specify the **CHAP Name** and **Password**, and confirm the password in both the **Target Authenticates Initiator** and **Initiator Authenticates Target** areas.
CHAP Name	User name for CHAP authentication. **NOTE** • The name must contain 4 to 223 characters. • The name can contain only letters, digits, and special characters (!"#$&%'()*+,-./:;<=>?@[\]^_`{|}~). • The first character must be a letter or digit.
Password	Password for CHAP authentication. **NOTE** • The password can contain 12 to 16 characters. • The password must contain at least three types of characters among uppercase letters, lowercase letters, digits, and special characters (`~!@#$%^&*()-_=+|[{}];:<,.\>/? and spaces). • The password must not be the same as the user name or the user name spelled backwards.
Confirm Password	Password for CHAP authentication. [Value range] The value of **Confirm Password** must be consistent with that of **Password**.

Table 5-42 describes the NVMe over RoCE initiator parameters.

Table 5-42 NVMe over RoCE initiator parameters

Parameter	Description
NQN	World Wide Port Name (WWPN) of the initiator. [Value range] • The value contains 1 to 223 characters. • The value must start with a digit or letter. • The value must be visible ASCII characters.
Alias	Alias of the initiator. [Value range] • An alias can be left blank or contain up to 31 characters. • The value can contain only letters, digits, underscores (_), hyphens (-), and periods (.).

NOTE

After you click **OK**, the new initiator is automatically added to the list on the right.

Step 6 Click **OK**.

Confirm your operation as prompted.

----End

5.7.12 Modifying an Initiator

This section describes how to modify the parameters of an initiator.

Procedure

Step 1 Choose **Services** > **Block Service** > **Host Groups** > **Hosts**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 On the **Hosts** tab page, click the name of the desired host.

The host details page is displayed.

Step 4 Click the **Initiators** tab page.

Step 5 Click **More** on the right of the desired initiator and choose **Modify**.

The **Modify Initiator** page is displayed on the right.

Step 6 (Optional) Set an alias for the initiator.

Step 7 Click **OK**.

----End

5.7.13 Removing an Initiator

This section describes how to remove an initiator from a host.

Procedure

Step 1 Choose **Services** > **Block Service** > **Host Groups** > **Hosts**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 On the **Hosts** tab page, click **More** on the right of the desired host and choose **Remove Initiator**.

The **Remove Initiator** page is displayed on the right.

NOTE

Alternatively, perform any of the following operations to remove initiators:

- Click the name of the desired host. In the upper right corner of the page that is displayed, select **Remove Initiator** from the **Operation** drop-down list.
- Click the name of the desired host. On the page that is displayed, click the **Initiators** tab page, select the desired initiators, and click **Remove**.
- Click the name of the desired host. On the page that is displayed, click the **Initiators** tab page, click **More** on the right of the desired initiator, and select **Remove**.

Step 4 Select initiators.

Select one or more initiators from **Available Initiators**.

NOTE

Skip this step if you remove initiators from the **Initiators** tab page.

Step 5 Click **OK**.

Confirm your operation as prompted.

----End

5.7.14 Modifying the Properties of a Host

This section describes how to modify the properties of a host.

Procedure

Step 1 Choose **Services** > **Block Service** > **Host Groups** > **Hosts**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 On the **Hosts** tab page, click **More** on the right of the desired host and choose **Modify**.

The **Modify Host** page is displayed on the right.

NOTE

Alternatively, click the name of the desired host. In the upper right corner of the page that is displayed, select **Modify** from the **Operation** drop-down list.

Step 4 Modify the general properties of the host.

1. Modify the **Name** for the host.

   NOTE

   - The name must be unique.
   - The name can contain only letters, digits, underscores (_), hyphens (-), and periods (.).
   - The name contains 1 to 255 characters.

2. Select the vStore to which the host belongs from the **Owning vStore** drop-down list.

   NOTE

   After the vStore to which the host belongs is modified, the vStore to which the initiator of the host belongs changes accordingly.

3. (Optional) Modify the **Description** of the host.
4. Modify the **OS** of the host.
5. (Optional) Modify the **IP Address** of the host.
6. (Optional) Modify the **Location** of the host.
7. Select a **Host Access Mode**. The possible values are **Load balancing** and **Asymmetric**.

   NOTE

   The host access mode indicates that a host accesses local and remote storage systems in a HyperMetro pair.

   - **Load balancing**: Hosts access local and remote devices with equal priority.
   - **Asymmetric**: Hosts preferentially access the specified device.

   If a LUN has been mapped to a host, restart the host for the modification to take effect after you modify the host access mode. You do not need to restart the system when configuring the mapping for the first time.

   For details about how to configure the host access mode in different operating systems, see the corresponding *Host Connectivity Guide*.

8. When **Host Access Mode** is **Asymmetric**, set **Preferred Path for HyperMetro**.

Step 5 Click **OK**.

Confirm your operation as prompted.

----End

5.7.15 Deleting a Host

Deleting a host interrupts the communication between the corresponding application server and the LUNs mapped to the host.

Prerequisites

The host to be deleted is not a member of any host group.

Procedure

Step 1 Choose **Services** > **Block Service** > **Host Groups** > **Hosts**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 On the **Hosts** tab page, select the desired host and click **Delete**.

NOTE

Alternatively, perform either of the following operations to delete hosts:

- Click **More** on the right of the host and choose **Delete**.
- Click the name of the desired host. In the upper right corner of the page that is displayed, select **Delete** from the **Operation** drop-down list.

Confirm your operation as prompted.

----End

5.8 Managing Initiators

An initiator is a system component that initiates I/Os on an I/O bus or network.

5.8.1 Creating an Initiator

This section describes how to create an initiator for a storage system.

Procedure

Step 1 Choose **Services** > **Block Service** > **Host Groups** > **Initiators**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 On the **Initiators** tab page, select an initiator type and click **Create**.

The **Create Initiator** page is displayed.

Step 4 Set the initiator parameters.

- FC initiator

  Table 5-43 describes the parameters.

Table 5-43 FC initiator parameters

Parameter	Description
WWPN	World Wide Port Name (WWPN) of the initiator. [Value range] A WWPN consists of 16 hexadecimal numbers (0 to 9 and A to F or a to f). It cannot be all 0s or all Fs (both uppercase and lowercase).
Owning vStore	vStore to which the newly created host belongs. **NOTE** This parameter is mandatory when **vStore** is set to **All vStores** in Step 2.
Alias	Alias of the initiator. [Value range] – An alias can be left blank or contain up to 31 characters. – It contains only letters, digits, periods (.), underscores (_), and hyphens (-).

- iSCSI initiator

  Table 5-44 describes the parameters.

Table 5-44 iSCSI initiator parameters

Parameter	Description
IQN	iSCSI Qualified Name (IQN) of the iSCSI initiator. **NOTE** The IQN of an initiator must be the same as the one on the application server. The IQN of an initiator must be unique. Do not use the same IQN for the initiators from multiple application servers. [Value range] An IQN contains 1 to 223 characters.
Owning vStore	vStore to which the newly created host belongs. **NOTE** This parameter is mandatory when **vStore** is set to **All vStores** in Step 2.
Alias	Alias of the iSCSI initiator. [Value range] – An alias can be left blank or contain up to 31 characters. – It contains only letters, digits, periods (.), underscores (_), and hyphens (-).

Parameter	Description
CHAP	Specifies whether to enable CHAP authentication. CHAP authentication includes **Normal Authentication** and **Discovery Authentication** options. – If you enable CHAP, you must configure the same CHAP name and password for the storage system and the application server. – If you do not enable CHAP, you do not need to configure a CHAP name or password.
Normal Authentication	The normal session is the process during which the target and initiator transmit data between each other after connections have been set up. Authentication modes include: – No authentication – Unidirectional authentication The target authenticates the initiator. – Bidirectional authentication The target and initiator authenticate each other.
Discovery Authentication	The discovery session is the process during which the target and initiator are setting up connections. Authentication modes include: – No authentication – Unidirectional authentication The target authenticates the initiator. – Bidirectional authentication The target and initiator authenticate each other.
CHAP Name	User name for CHAP authentication. [Value range] – The name must contain 4 to 223 characters. – The name can contain only letters, digits, and the following special characters: !"#$&%'()*+,-./:;<=>?@[\]^_`{|}~ – The first character must be a letter or digit.

Parameter	Description
Password	Password for CHAP authentication. [Value range] – The password must contain 12 to 16 characters. – The password must contain at least three of the following types of characters: ■ Uppercase letters ■ Lowercase letters ■ Digits ■ Special characters (including spaces) !"#$&%'()*+,-./:;<=>?@[\]^_`{|}~ – The password must not be the same as the user name or the user name spelt backwards.
Confirm Password	Enter the password again for confirmation.

NOTE

If you choose **Bidirectional authentication**, you must configure the CHAP name and password for **Target Authenticates Initiator** and **Initiator Authenticates Target**.

- NVMe over RoCE initiator

  Table 5-45 describes the parameters.

Table 5-45 NVMe over RoCE initiator parameters

Parameter	Description
NQN	World Wide Port Name (WWPN) of the initiator. [Value range] – The value contains 1 to 223 characters. – The value must start with a digit or letter. – The value must be visible ASCII characters.
Owning vStore	vStore to which the newly created initiator belongs. **NOTE** This parameter is mandatory when **vStore** is set to **All vStores** in **Step 2**.

Parameter	Description
Alias	Alias of the initiator. [Value range] – An alias can be left blank or contain up to 31 characters. – The value can contain only letters, digits, underscores (_), hyphens (-), and periods (.).

Step 5 Click **OK**.

Confirm your operation as prompted.

----End

5.8.2 Viewing Initiator Information

This section describes how to view initiator information.

Procedure

Step 1 Choose **Services** > **Block Service** > **Host Groups** > **Initiators**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 On the **Initiators** tab page, select an initiator type. In the function pane, view information about initiators. **Table 5-46** describes the parameters.

Table 5-46 Initiator parameters

Parameter	Description
WWPN/IQN/NQN	• **WWPN**: unique identifier of the FC initiator. • **IQN**: iSCSI Qualified Name (IQN) of the iSCSI initiator. • **NQN**: unique identifier of the NVMe over RoCE initiator.
Owning vStore	Name of the vStore to which the initiator belongs. **NOTE** This parameter is available only when **vStore** is set to **All vStores** in **Step 2**.
vStore ID	ID of the vStore to which the initiator belongs. **NOTE** This parameter is available only when **vStore** is set to **All vStores** in **Step 2**.
Alias	Alias of the initiator.
Status	Indicates whether an initiator is online.

Parameter	Description
Associated with Host	Indicates whether the initiator has been associated with a host.
Associated Host Name	Name of the host with which the initiator is associated.
Associated Host IP Address	IP address of the host with which the initiator is associated. **NOTE** This parameter is displayed only when the initiator type is iSCSI or NVMe over RoCE.

----End

5.8.3 Modifying an Initiator

This section describes how to modify the parameters of an initiator.

Procedure

Step 1 Choose **Services** > **Block Service** > **Host Groups** > **Initiators**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 On the **Initiators** tab page, select an initiator type.

Step 4 Click **More** on the right of the desired initiator and select **Modify**.

The **Modify Initiator** page is displayed on the right.

Step 5 Modify the initiator information.

- FC initiator
  a. Select the vStore to which the initiator belongs from the **Owning vStore** drop-down list.

     NOTE

     If an initiator has been added to a host, the owning vStore of the initiator can be modified only on the host.

  b. Set an alias for an FC initiator.

     NOTE

     - An alias can be left blank or contain up to 31 characters.
     - The name can contain only letters, digits, underscores (_), hyphens (-), and periods (.).
- iSCSI initiator

  Table 5-47 describes the parameters.

Table 5-47 iSCSI initiator parameters

Parameter	Description
Owning vStore	vStore to which the initiator belongs. **NOTE** If an initiator has been added to a host, the owning vStore of the initiator can be modified only on the host.
Alias	Alias of the iSCSI initiator. [Value range] – An alias can be left blank or contain up to 31 characters. – The name can contain only letters, digits, underscores (_), hyphens (-), and periods (.).
CHAP	Specifies whether to enable CHAP authentication. CHAP authentication includes **Normal Authentication** and **Discovery Authentication** options. – If you enable CHAP, you must configure the same CHAP name and password for the storage system and the application server. – If you do not enable CHAP, you do not need to configure a CHAP name or password.
Normal Authentication	The normal session is the process during which the target and initiator transmit data between each other after connections have been set up. Authentication modes include: – No authentication – Unidirectional authentication The target authenticates the initiator. – Bidirectional authentication The target and initiator authenticate each other.
Discovery Authentication	The discovery session is the process during which the target and initiator are setting up connections. Authentication modes include: – No authentication – Unidirectional authentication The target authenticates the initiator. – Bidirectional authentication The target and initiator authenticate each other.

Parameter	Description
CHAP Name	User name for CHAP authentication. [Value range] – The name must contain 4 to 223 characters. – The name can contain only letters, digits, and the following special characters: !"#$&%'()*+,-./:;<=>?@[\]^_`{|}~ – The first character must be a letter or digit.
Password	Password for CHAP authentication. [Value range] – The password must contain 12 to 16 characters. – The password must contain at least three of the following types of characters: ■ Uppercase letters ■ Lowercase letters ■ Digits ■ Special characters (including spaces) !"#$&%'()*+,-./:;<=>?@[\]^_`{|}~ – The password must not be the same as the user name or the user name spelt backwards.
Confirm Password	Enter the password again for confirmation.

NOTE

If you choose **Bidirectional authentication**, you must configure the CHAP name and password for **Target Authenticates Initiator** and **Initiator Authenticates Target**.

- NVMe over RoCE initiator
  a. Select the vStore to which the initiator belongs from the **Owning vStore** drop-down list.

     NOTE

     If an initiator has been added to a host, the owning vStore of the initiator can be modified only on the host.

  b. Set an alias for the NVMe over RoCE initiator.

     NOTE

     ■ An alias can be left blank or contain up to 31 characters.

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

Step 6 Click **OK**.

Confirm your operation as prompted.

----End

5.8.4 Associating an Initiator with a Host

This section describes how to associate an initiator with a host.

Prerequisites

- An FC initiator whose owning vStore is the same as that of the created host or whose owning vStore is **--** can be added to the host.
- For iSCSI and NVMe over RoCE initiators, you can only add initiators whose owning vStore is the same as that of the created host to the host.

Procedure

Step 1 Choose **Services** > **Block Service** > **Host Groups** > **Initiators**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 On the **Initiators** tab page, select an initiator type.

Step 4 Select an initiator and click **Associate with Host**.

NOTE

Alternatively, click **More** on the right of the initiator and select **Associate with Host**.

Step 5 Select a host.

Step 6 Click **OK**.

Confirm your operation as prompted.

----End

5.8.5 Dissociating an Initiator from a Host

This section describes how to dissociate an initiator from a host.

Precautions

Removing an initiator will interrupt services on the host. Stop host services before performing this operation.

Procedure

Step 1 Choose **Services** > **Block Service** > **Host Groups** > **Initiators**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 On the **Initiators** tab page, select an initiator type.

Step 4 Select an initiator and click **Dissociate from Host**.

Confirm your operation as prompted.

NOTE

Alternatively, click **More** on the right of the initiator and select **Dissociate from Host**.

----End

5.8.6 Deleting an Initiator

This section describes how to delete an initiator.

Prerequisites

- **Status** of the initiator is **Offline**.
- The initiator is not associated with any host.

Procedure

Step 1 Choose **Services** > **Block Service** > **Host Groups** > **Initiators**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 On the **Initiators** tab page, select an initiator type.

Step 4 Select the desired initiator and click **Delete**.

NOTE

Alternatively, click **More** on the right of the initiator and select **Delete** to delete the desired initiator.

Step 5 Confirm your operation as prompted.

----End

5.9 Managing Host Groups

This section describes how to manage host groups.

5.9.1 Viewing Host Group Information

This section describes how to view basic information about all host groups.

Prerequisites

At least one host group has been created.

Procedure

Step 1 Choose **Services** > **Block Service** > **Host Groups** > **Host Groups**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 On the **Host Groups** tab page, view the host group information in the function pane. **Table 5-48** describes the parameters.

Table 5-48 Host group parameters

Parameter	Description
Name	Name of the host group. **NOTE** You can click the name of a host group to view its details and manage it.
ID	ID of the host group.
Owning vStore	Name of the vStore to which the host group belongs. **NOTE** This parameter is available only when **vStore** is set to **All vStores** in **Step 2**.
vStore ID	ID of the vStore to which the host group belongs. **NOTE** This parameter is available only when **vStore** is set to **All vStores** in **Step 2**.
LUN Capacity Usage	Capacity usage of LUNs in the LUN group mapped to the host group.
Hosts	Number of hosts in a host group.

Step 4 (Optional) Click the name of the host group to query its summary, member hosts, and mapping.

----End

5.9.2 Viewing Host LUN IDs

A host LUN ID is allocated by the storage system to a LUN mapped to a host. This ID is visible on the host.

Procedure

Step 1 Choose **Services** > **Block Service** > **Host Groups** > **Host Groups**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 On the **Host Groups** tab page, click the name of the desired host group. On the page that is displayed, click the **Mapping** tab page.

Step 4 Click **View Host LUN ID**.

The **View Host LUN ID** page is displayed on the right.

Step 5 View the LUNs mapped to hosts in the host group and their host LUN IDs.

----End

5.9.3 Modifying Host LUN IDs

This section describes how to modify host LUN IDs.

Prerequisites

Host services on the LUN have been stopped, and the virtual disk created by multipathing software and physical disk corresponding to the LUN have been uninstalled from the host.

Procedure

Step 1 Choose **Services** > **Block Service** > **Host Groups** > **Host Groups**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 On the **Host Groups** tab page, click the name of the desired host group. On the page that is displayed, click the **Mapping** tab.

Step 4 Click **More** on the right of the desired LUN or LUN group and choose **Modify Host LUN ID**.

The **Modify Host LUN ID** page is displayed on the right.

NOTE

Alternatively, perform either of the following operations to go to the **Modify Host LUN ID** page:

- On the **Mapping** tab page, click **View Host LUN ID**. On the **View Host LUN ID** page that is displayed, click **Modify** in the upper right corner.
- Choose **Services** > **Block Service** > **LUN Groups** > **LUN Groups** and click the name of the desired LUN group. On the page that is displayed, click the **Mapping** tab, then click **More** on the right of the host or host group, and choose **Modify Host LUN ID**.

Step 5 Set the host LUN ID for each LUN. The value ranges from 0 to 4095.

Step 6 Select **Advanced** in the upper right corner and determine whether to select **Same Host LUN ID**. If you select it, the system checks whether the host LUN IDs of the local and remote LUNs in the same HyperMetro pairs are the same when you change the host LUN IDs. In SAN-based HyperMetro scenarios involving ESX hosts, if the host LUN IDs of the local and remote LUNs in the same HyperMetro pairs are different, data may be inconsistent.

Step 7 Click **OK**.

----End

Follow-up Procedure

After a host LUN ID is modified, re-scan for disks on the host.

5.9.4 Adding a Port Group

This section describes how to add a port group for a LUN group.

Procedure

Step 1 Choose **Services** > **Block Service** > **Host Groups** > **Host Groups**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 On the **Host Groups** tab page, click the name of the desired host group. On the page that is displayed, click the **Mapping** tab page.

Step 4 Select the desired LUN group and click **Add Port Group**.

The **Add Port Group** page is displayed on the right.

Step 5 Select a port group.

NOTE

You can click **Create** to create a port group.

Step 6 Click **OK**.

Confirm your operation as prompted.

----End

5.9.5 Removing a Port Group

This section describes how to remove a port group for a LUN group.

Procedure

Step 1 Choose **Services** > **Block Service** > **Host Groups** > **Host Groups**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 On the **Host Groups** tab page, click the name of the desired host group. On the page that is displayed, click the **Mapping** tab page.

Step 4 Select the desired LUN group and click **Remove Port Group**.

Confirm your operation as prompted.

----End

5.9.6 Mapping a LUN Group to a Host Group

This section describes how to create a mapping between a host group and a LUN group.

Procedure

Step 1 Choose **Services** > **Block Service** > **Host Groups** > **Host Groups**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 On the **Host Groups** tab page, choose **Map** > **Map LUN Group**.

The **Map LUN Group** page is displayed on the right.

NOTE

Alternatively, perform either of the following operations to go to the **Map LUN Group** page:

- Click **More** on the right of the desired host group and choose **Map LUN Group**.
- Click the name of the desired host group. In the upper right corner of the page that is displayed, select **Map LUN Group** from the **Operation** drop-down list.

Step 4 Select a LUN group.

- If you select **New**:
  a. Set the name of the new LUN group.
  b. Select the storage pool to which the LUN group belongs. Set **Application Type** for LUNs.

NOTE

The following preset application types are provided for typical applications: **Default**, **Oracle_OLAP**, **Oracle_OLTP**, **Oracle_OLAP&OLTP**, **SQL_Server_OLAP**, **SQL_Server_OLTP**, **SQL_Server_OLAP&OLTP**, **SAP_HANA**, **Vmware_VDI**, **Hyper-V_VDI**, and **FusionAccess_VDI**.

- After you have set an application type for a LUN, you are unable to change it in follow-up operations.
- If the application type configured for a LUN does not match the actual I/O model, the LUN performance may deteriorate.
- If none of the preset application types matches the actual I/O model, you can run the **create lun_workload_type general** command to create one. For details on this command, refer to the *Command Reference*.

c. Specify the LUN name prefix, capacity per LUN, and quantity. **Table 5-49** describes the parameters.

Table 5-49 LUN parameters

Parameter	Description
Name Prefix	Name prefix of the LUN. The names of the new LUNs are numbered in sequence based on the name prefix.
Capacity per LUN	Capacity of the LUN in the LUN group. **NOTE** ■ The maximum capacity of the LUN must not exceed the system specifications. ■ You can set the capacity unit to **Blocks** to create LUNs by block. A block is equal to 512 bytes. The LUN capacity must not be smaller than 1024 blocks (that is, 512 KB). ■ The storage system uses the following capacity algorithms defined by Windows: 1 PB = 1,024 TB, 1 TB = 1,024 GB, 1 GB = 1,024 MB, 1 MB = 1,024 KB, and 1 KB = 1,024 bytes.
Quantity	Number of LUNs created in a batch. Set this parameter based on site requirements. [Value range] 1 to 500 **NOTE** ■ LUNs created in a batch have the same capacity. ■ When LUNs are created in a batch, the system automatically adds suffixes to the names based on the number of LUNs for distinction. You can click to manually specify the start number for the suffixes.

d. (Optional) When creating LUNs in a batch, click and set the suffixes of the LUNs. Related parameters include **Suffix Digits** and **Suffix** (start

number of the suffixes). The system adds a suffix to the end of each LUN name in ascending order based on the specified start suffix number.

NOTE

- The value range of **Suffix** is 0 to (10000 – **Quantity**).
- For example, if you want to create 300 LUNs, the value range of **Suffix** is 0 to 9700.

e. (Optional) Click + to add more LUNs.

f. (Optional) Click — to remove LUNs.

- If you select **Existing**:

  Select a LUN group from the list.

  NOTE

  You can select **Include mapped LUN groups** to query the LUN groups that have been mapped to the current host group. For these LUN groups, mapping cannot be created repeatedly.

Step 5 (Optional) Select a port group.

NOTE

If no port group exists in the system, click **Create**.

Step 6 Set how to assign host LUN IDs.

- **Automatic**: The system assigns a host LUN ID to each LUN mapped to a host.
- **Start ID**: Set a start ID ranging from 0 to 4095. The system assigns a host LUN ID to each LUN mapped to a host, starting from **Start ID**.
- **Specified ID**: Manually assign a host LUN ID to each LUN mapped to a host.

Step 7 If you select an existing LUN group, select **Advanced** in the upper right corner and determine whether to select **Same Host LUN ID**. If you select it, the system forcibly ensures that the host LUN IDs of the local and remote LUNs in the same HyperMetro pairs are the same. In SAN-based HyperMetro scenarios involving ESX hosts, if the host LUN IDs of the local and remote LUNs in the same HyperMetro pairs are different, data may be inconsistent.

Step 8 Click **OK**.

Confirm your operation as prompted.

NOTE

After the task is created successfully, the **Execution Result** page is displayed. You can view details about the current task on this page.

----End

5.9.7 Unmapping a Host Group

This section describes how to cancel the mapping between a host group and a LUN group.

Procedure

Step 1 Choose **Services** > **Block Service** > **Host Groups** > **Host Groups**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 On the **Host Groups** tab page, click **More** on the right of the desired host group and choose **Unmap**.

The **Unmap Object** page is displayed on the right.

NOTE

Alternatively, perform either of the following operations to go to the **Unmap Object** page:

- Click the name of the desired host group. In the upper right corner of the page that is displayed, select **Unmap** from the **Operation** drop-down list.
- Click the name of the desired host group. On the page that is displayed, click the **Mapping** tab page, then click **More** on the right of the LUN group, and select **Unmap**.

Step 4 Select one or more objects from **Available Objects**.

NOTE

Skip this step if you cancel the mapping between a host group and a LUN group from the **Mapping** tab page.

Step 5 Click **OK**.

Confirm your operation as prompted.

----End

5.9.8 Adding a Host

This section describes how to add a host to a host group.

Procedure

Step 1 Choose **Services** > **Block Service** > **Host Groups** > **Host Groups**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 On the **Host Groups** tab page, click **More** on the right of the desired host group and choose **Add Host**.

The **Add Host** page is displayed on the right.

NOTE

Alternatively, perform any of the following operations to go to the **Add Host** page:

- Click the name of the desired host group. In the upper right corner of the page that is displayed, select **Add Host** from the **Operation** drop-down list.
- Click the name of the desired host group. On the page that is displayed, click the **Member Hosts** tab page, and then click **Add**.
- Click the value in the **Hosts** column of the desired host group if the value is not **0**. On the **Member Hosts** tab page, click **Add**.

Step 4 Select one or more hosts from **Available Hosts** and add them to **Selected Hosts**.

NOTE

You can select **Only show the hosts that have not been added to any host group** below the host list, which helps you find the desired hosts.

Step 5 Click **OK**.

Confirm your operation as prompted.

----End

5.9.9 Removing a Host

This section describes how to remove a host from a host group.

Procedure

Step 1 Choose **Services** > **Block Service** > **Host Groups** > **Host Groups**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 On the **Host Groups** tab page, click **More** on the right of the desired host group and choose **Remove Host**.

The **Remove Host** page is displayed on the right.

NOTE

Alternatively, perform any of the following operations to remove hosts:

- Click the name of the desired host group. In the upper right corner of the page that is displayed, select **Remove Host** from the **Operation** drop-down list.
- Click the name of the desired host group. On the page that is displayed, click the **Member Hosts** tab page, select the desired hosts, and click **Remove**.
- Click the name of the desired host group. On the page that is displayed, click the **Member Hosts** tab page, click **More** on the right of the desired host, and select **Remove**.
- Click the value in the **Hosts** column of the desired host group. On the **Member Hosts** tab page, select the desired hosts and click **Remove**.
- Click the value in the **Hosts** column of the desired host group. On the **Member Hosts** tab page, click **More** on the right of the desired host and select **Remove**.

Step 4 Select one or more hosts from **Available Hosts** and add them to **Selected Hosts**.

NOTE

Skip this step if you remove hosts from the **Member Hosts** tab page.

Step 5 Click **OK**.

Confirm your operation as prompted.

----End

5.9.10 Modifying the Properties of a Host Group

This section describes how to modify the name and description of a host group.

Procedure

Step 1 Choose **Services** > **Block Service** > **Host Groups** > **Host Groups**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 On the **Host Groups** tab page, click **More** on the right of the desired host group and choose **Modify**.

The **Modify Host Group** page is displayed on the right.

NOTE

Alternatively, click the name of the desired host group. In the upper right corner of the page that is displayed, select **Modify** from the **Operation** drop-down list.

Step 4 Modify the properties of the host group.

1. Modify the **Name** for the host group.

   NOTE

   - The name must be unique.
   - The name can contain only letters, digits, periods (.), underscores (_), and hyphens (-).
   - The name contains 1 to 255 characters.

2. Modify **Description** for the host group.

Step 5 Click **OK**.

----End

5.9.11 Deleting a Host Group

This section describes how to delete a host group when it is no longer needed.

Prerequisites

The host group to be deleted is not mapped.

Procedure

Step 1 Choose **Services** > **Block Service** > **Host Groups** > **Host Groups**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 On the **Host Groups** tab page, click **More** on the right of the desired host group and choose **Delete**.

NOTE

Alternatively, click the name of the desired host group. In the upper right corner of the page that is displayed, select **Delete** from the **Operation** drop-down list.

Confirm your operation as prompted.

----End

5.10 Managing Port Groups

This chapter describes how to configure and manage port groups.

5.10.1 Viewing Port Group Information

This operation enables you to view information about port groups.

Procedure

Step 1 Choose **Services** > **Block Service** > **Port Groups**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 View information about port groups in the function pane. **Table 5-50** describes the parameters.

Table 5-50 Port group parameters

Parameter	Description
Name	Name of a port group. **NOTE** You can click the name of a port group to view its details and manage it.
Owning vStore	Name of the vStore to which the port group belongs. **NOTE** This parameter is available only when **vStore** is set to **All vStores** in **Step 2**.

Parameter	Description
vStore ID	ID of the vStore to which the port group belongs. **NOTE** This parameter is available only when **vStore** is set to **All vStores** in **Step 2**.
ID	ID of a port group.
Ports	Number of ports in a port group.
Port Type	Type of ports in a port group.
Mapping	Indicates whether a port group has been mapped.

Step 4 (Optional) Click the name of a port group to query its summary and member ports.

----End

5.10.2 Adding a Port

This operation enables you to add a port to a port group.

Procedure

Step 1 Choose **Services** > **Block Service** > **Port Groups**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 Click **More** on the right of the desired port group and select **Add Port**.

The **Add Port** page is displayed on the right.

NOTE

Alternatively, perform any of the following operations to go to the **Add Port** page:

- Click the name of the desired port group. In the upper right corner of the page that is displayed, select **Add Port** from the **Operation** drop-down list.
- Click the name of the desired port group. On the page that is displayed, click the **Member Ports** tab page, and then click **Add**.
- Click the value in the **Ports** column of the desired port group if the value is not **0**. On the **Member Ports** tab page, click **Add**.

Step 4 In **Available Ports**, select one or more desired ports and they are added to **Selected Ports** automatically.

NOTE

- A port can be added to multiple port groups.
- You can select **Include the ports that are link down** below the port list, which helps you find the desired ports.

Step 5 Click **OK**.

----End

5.10.3 Removing a Port

This operation enables you to remove a port from a port group.

Procedure

Step 1 Choose **Services** > **Block Service** > **Port Groups**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 Click **More** on the right of the desired port group and select **Remove Port**.

The **Remove Port** page is displayed on the right.

NOTE

Alternatively, perform any of the following operations to remove ports:

- Click the name of the desired port group. In the upper right corner of the page that is displayed, select **Remove Port** from the **Operation** drop-down list.
- Click the name of the desired port group. On the page that is displayed, click the **Member Ports** tab page, select the desired ports, and click **Remove**.
- Click the name of the desired port group. On the page that is displayed, click the **Member Ports** tab page, click **More** on the right of the desired port, and select **Remove**.
- Click the value in the **Ports** column of the desired port group. On the **Member Ports** tab page, select the desired ports and click **Remove**.
- Click the value in the **Ports** column of the desired port group. On the **Member Ports** tab page, click **More** on the right of the desired port and select **Remove**.

Step 4 In **Available Ports**, select one or more desired ports and they are added to **Selected Ports** automatically.

NOTE

Skip this step if you remove ports from the **Member Ports** tab page.

Step 5 Click **OK**.

Confirm your operation as prompted.

----End

5.10.4 Modifying a Port Group

This operation enables you to change the name and modify the description of a port group.

Procedure

Step 1 Choose **Services** > **Block Service** > **Port Groups**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 Click **More** on the right of the desired port group and select **Modify**.

The **Modify Port Group** page is displayed on the right.

NOTE

Alternatively, click the name of the desired port group. In the upper right corner of the page that is displayed, select **Modify** from the **Operation** drop-down list.

Step 4 Modify the name of the port group.

NOTE

- The name must be unique.
- The name can contain only letters, digits, periods (.), underscores (_), and hyphens (-).
- The name contains 1 to 255 characters.

Step 5 Modify the description of the port group.

Step 6 Click **OK**.

----End

5.10.5 Deleting a Port Group

This operation enables you to delete a port group.

Prerequisites

The port group to be deleted has not been mapped.

Procedure

Step 1 Choose **Services** > **Block Service** > **Port Groups**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 Click **More** on the right of the desired port group and select **Delete**.

NOTE

Alternatively, click the name of the desired port group. In the upper right corner of the page that is displayed, select **Delete** from the **Operation** drop-down list.

Step 4 Confirm your operation as prompted.

----End

5.11 Viewing a Mapping View

This section describes how to view the mapping between LUNs or LUN groups and hosts or host groups.

Procedure

Step 1 Choose **Services** > **Block Service** > **Mapping Views**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

NOTE

Only 6.1.3 and later versions support multiple vStores.

Step 3 View the mapping view information in the function pane. **Table 5-51** describes the parameters.

Table 5-51 Mapping view parameters

Parameter	Description
Name	Name of a mapping view. **NOTE** You can click a name to view the brief information about a mapping view, as well as LUNs, LUN group, host, host group, and port group in the mapping view.
ID	ID of a mapping view.
Owning vStore	Name of the vStore to which the mapping view belongs. **NOTE** This parameter is available only when **vStore** is set to **All vStores** in **Step 2**.
vStore ID	ID of the vStore to which the mapping view belongs. **NOTE** This parameter is available only when **vStore** is set to **All vStores** in **Step 2**.
LUN Group	Name of the LUN group in a mapping view.
Host	Name of the host in a mapping view.
Host Group	Name of the host group in a mapping view.
Port Group	Name of the port group in a mapping view.

NOTE

Mapping views include mapping LUNs to hosts, mapping LUN groups to hosts, and mapping LUN groups to host groups.

- In a mapping view where LUNs are mapped to a host, **LUN Group** and **Host Group** are displayed as **--**. You can click the name of the mapping view and click the **LUNs** tab to view the LUNs mapped to the host.
- In a mapping view where a LUN group is mapped to a host, **Host Group** is displayed as **--**.
- In a mapping view where a LUN group is mapped to a host group, **Host** is displayed as **--**.
- In a mapping view that does not contain a port group, **Port Group** is displayed as **--**.

----End

6 FAQs

This chapter describes the FAQs related to the basic storage service configuration guide. You can also refer to this chapter to handle faults encountered during configuration or maintenance.

6.1 How Can I Enable Mapping Cancellation Fool-Proofing?

To prevent users from falsely deleting a mapping in use, the storage system provides the mapping cancellation fool-proofing function. This function is disabled by default and can be enabled using the **change tgt_switch map_foolproof switch=on** command.

After this function is enabled, the system checks whether there are I/O operations when a user tries to remove a LUN or host during mapping cancellation. If there are I/O operations, the system does not allow mapping cancellation.

NOTE

- Mapping cancellation operations include: unmap a LUN and a host, unmap a host and a LUN group, unmap a host group and a LUN group, remove a LUN from a LUN group, remove a host from a host group, and remove an initiator.
- After this function is enabled, the system checks whether there are I/O operations at the point in time when an operation is performed. The system may incorrectly determine the status of periodical or routine test services. Therefore, this function provides only reference for you to determine the service status. You need to manually confirm whether there are running services. If you confirm the involved LUN but the system still displays a message indicating that I/O operations exist, disable this function and try again.
- You can run the **show tgt_switch map_foolproof** command to check whether the function is enabled. For more details, refer to the command reference specific to your product version.

6.2 How Can I Query the iSCSI Target Name of an Ethernet Port on a Storage System?

After an IP address is configured for an Ethernet port on a storage system, an iSCSI target name is automatically generated on the Ethernet port.

Using the CLI

Log in to the CLI of the storage system and run the **show iscsi target_name eth_port_id=?** command to query the iSCSI target name of the Ethernet port.

```
admin:/>show iscsi target_name eth_port_id=CTE0.B.IOM2.P0
  iSCSI Target Name : iqn.2006-08.com.huawei:oceanstor:2100ac8d34eea90a::1020200:192.168.1.8
admin:/>
```

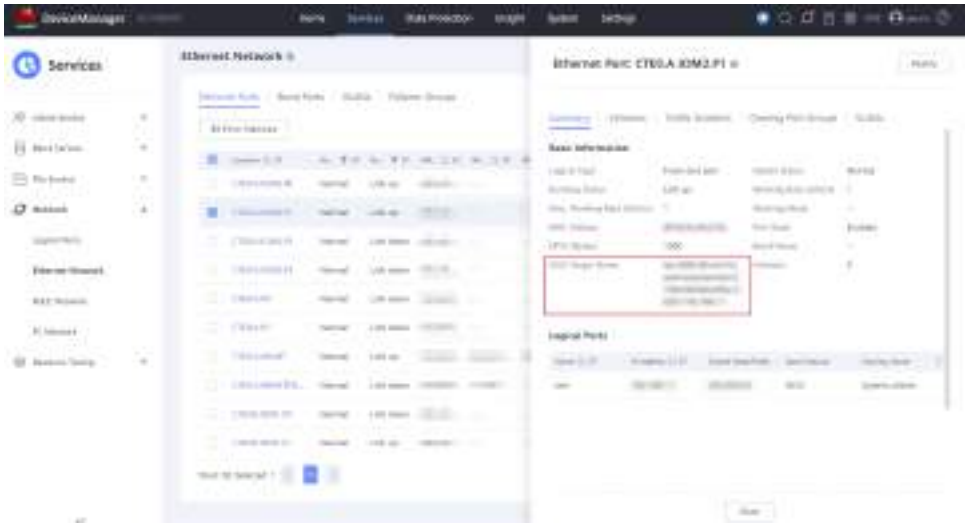
NOTE

- You can run the **show port general physical_type=ETH logic_type=Host_Port** command to query the value of **eth_port_id**.
- For details on this command, refer to the Command Reference.

Using DeviceManager

Method 1:

Choose **Services** > **Network** > **Ethernet Network** > **Ethernet Ports**. Click the desired Ethernet port and view its **iSCSI Target Name** on the page that is displayed.



Method 2:

Step 1 Choose **System** > **Hardware** > **Devices**.

Step 2 Click the controller enclosure where the desired Ethernet port resides.

Step 3 Click to switch to the rear view of the controller enclosure.

Step 4 Click the desired Ethernet port.

View the **iSCSI Target Name** on the page that is displayed.

----End

6.3 How Can I Replace the In-band Management Certificate with Self-signed Certificates?

In specific scenarios, you can import self-signed certificates to replace the in-band management certificate. The configuration procedure is as follows:

Procedure

Step 1 Prepare the OpenSSL environment.

1. Prepare a Linux-based device where the OpenSSL tool is installed (generally, the OpenSSL tool has been pre-installed in a CentOS or Ubuntu system). Run the **openssl version** command to verify that the OpenSSL tool version is **1.0.2a** or later.

```
# openssl version
OpenSSL 1.0.2k-fips 26 Jan 2017
```

2. Create a temporary directory, for example, **/tmp/cert**, and go to the directory.

```
# mkdir -p /tmp/cert
# cd /tmp/cert
```

3. Create and edit the **ssl.conf** file.

```
# vi ssl.conf
```

Copy the following content to the **ssl.conf** file:

```
[ req ]
default_bits = 4096
distinguished_name = req_distinguished_name

[ req_distinguished_name ]
countryName = Country Name (2 letter code)
countryName_default = CN
stateOrProvinceName = State or Province Name (full name)
stateOrProvinceName_default = SC
localityName = Locality Name (eg, city)
localityName_default = CD
```



```
organizationName = Organization Name (eg, company)
organizationName_default = Huawei
organizationalUnitName = Organizational Unit Name (eg, section)
organizationalUnitName_default = Storage
commonName = Common Name (e.g. server FQDN or YOUR name)
commonName_max = 64
commonName_default = xxxx

[ x509_ext ]
subjectKeyIdentifier        = hash
authorityKeyIdentifier    = keyid,issuer

[ v3_ca ]
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid:always,issuer
basicConstraints = CA:true
```

In the preceding content, *xxxx* indicates the ESN of the storage system.

Step 2 Use the OpenSSL tool to generate CA private key and CA certificate files.

1. Create directories and files related to certificate files.
   ```
   # mkdir -p /etc/pki/CA
   # touch /etc/pki/CA/index.txt
   # touch /etc/pki/CA/serial
   # echo 00 > /etc/pki/CA/serial
   # mkdir -p /tmp/cert/demoCA
   # touch /tmp/cert/demoCA/index.txt
   # touch /tmp/cert/demoCA/serial
   # echo 00 > /tmp/cert/demoCA/serial
   ```
2. Generate a CA private key file.
   ```
   openssl genrsa -out in_band_ca.key 2048
   ```
3. Generate a CA certificate request.
   ```
   openssl req -new -key in_band_ca.key -out in_band_ca.csr -config ssl.conf -subj "/C=cn/ST=sc/L=cd/
   O=huawei/OU=storage/CN=xxxx"
   ```
   In the preceding content, *xxxx* indicates the ESN of the storage system.
4. Generate a CA certificate file.
   ```
   openssl x509 -req -days 3650 -in in_band_ca.csr -signkey in_band_ca.key -out in_band_ca.crt -
   extensions v3_ca  -extfile ssl.conf
   ```

Step 3 Generate an in-band management certificate file.

1. Generate an in-band management private key file.
   ```
   openssl genrsa -out in_band_plain.key 2048
   ```
2. Generate an in-band management certificate request file.
   ```
   openssl req -new -key in_band_plain.key -out in_band.csr -config ssl.conf -subj "/C=cn/ST=sc/L=cd/
   O=huawei/OU=storage/CN=xxxx"
   ```
   In the preceding content, *xxxx* indicates the ESN of the storage system.
3. Use the CA certificate to sign the certificate request file.
   ```
   mkdir /etc/pki/CA/newcerts
   mkdir /tmp/cert/demoCA/newcerts
   openssl ca -in in_band.csr -out in_band.crt -cert in_band_ca.crt -keyfile in_band_ca.key -extfile ssl.conf
   ```
   Run the preceding commands and enter **y** as prompted. The following is an example of the command output:
   ```
   linux110232:/tmp/cert # mkdir /etc/pki/CA/newcerts
   linux110232:/tmp/cert # mkdir /tmp/cert/demoCA/newcerts
   linux110232:/tmp/cert # openssl ca -in in_band.csr -out in_band.crt -cert in_band_ca.crt -keyfile
   in_band_ca.key -extfile ssl.conf
   Using configuration from /etc/ssl/openssl.cnf
   Check that the request matches the signature
   Signature ok
   Certificate Details:
         Serial Number: 0 (0x0)
         Validity
   ```



```
            Not Before: May  5 12:19:38 2022 GMT
            Not After : May  5 12:19:38 2023 GMT
        Subject:
            countryName               = cn
            stateOrProvinceName       = sc
            organizationName          = huawei
            organizationalUnitName    = storage
            commonName                = 2102352UMS10K6000006
Certificate is to be certified until May  5 12:19:38 2023 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
linux110232:/tmp/cert #
```

Step 4 Replace the certificates.

1. Use an FTP tool (such as FileZilla) to connect to the Linux environment where the OpenSSL tool is installed and transfer the generated certificates and key file to the local PC.

   In this example, the certificates and key files generated in the **/tmp/cert/** directory are as follows:

   ```
   linux110232:/tmp/cert # ll
   total 28
   drwxr-xr-x 1 root root  120 May  5 20:19 demoCA
   -rw-r--r-- 1 root root 3804 May  5 20:19 in_band.crt
   -rw-r--r-- 1 root root  985 May  5 20:19 in_band.csr
   -rw-r--r-- 1 root root 1281 May  5 20:18 in_band_ca.crt
   -rw-r--r-- 1 root root  985 May  5 20:18 in_band_ca.csr
   -rw-r--r-- 1 root root 1675 May  5 20:18 in_band_ca.key
   -rw-r--r-- 1 root root 1679 May  5 20:18 in_band_plain.key
   -rw-r--r-- 1 root root  817 May  5 20:17 ssl.conf
   linux110232:/tmp/cert #
   ```

   In this example, you must transfer the following files:

   in_band.crt

   in_band_ca.crt

   in_band_plain.key

2. Import the generated self-signed certificates to the storage system.

   a. Log in to DeviceManager.

   b. Choose **Settings** > **Certificates** > **Certificate Management**.

   c. Select **In-band management certificate** and click **Import Certificate**.

      The **Import Certificate** page is displayed.

d. Import **in_band.crt** in **Certificate File** (mandatory), **in_band_ca.crt** in **CA Certificate File** (optional) and **in_band_plain.key** in **Private Key File** (mandatory).

e. Click **OK**.

----End

A Configuring Basic Storage Services Using the CLI

This section provides some CLI commands for configuring basic block storage services.

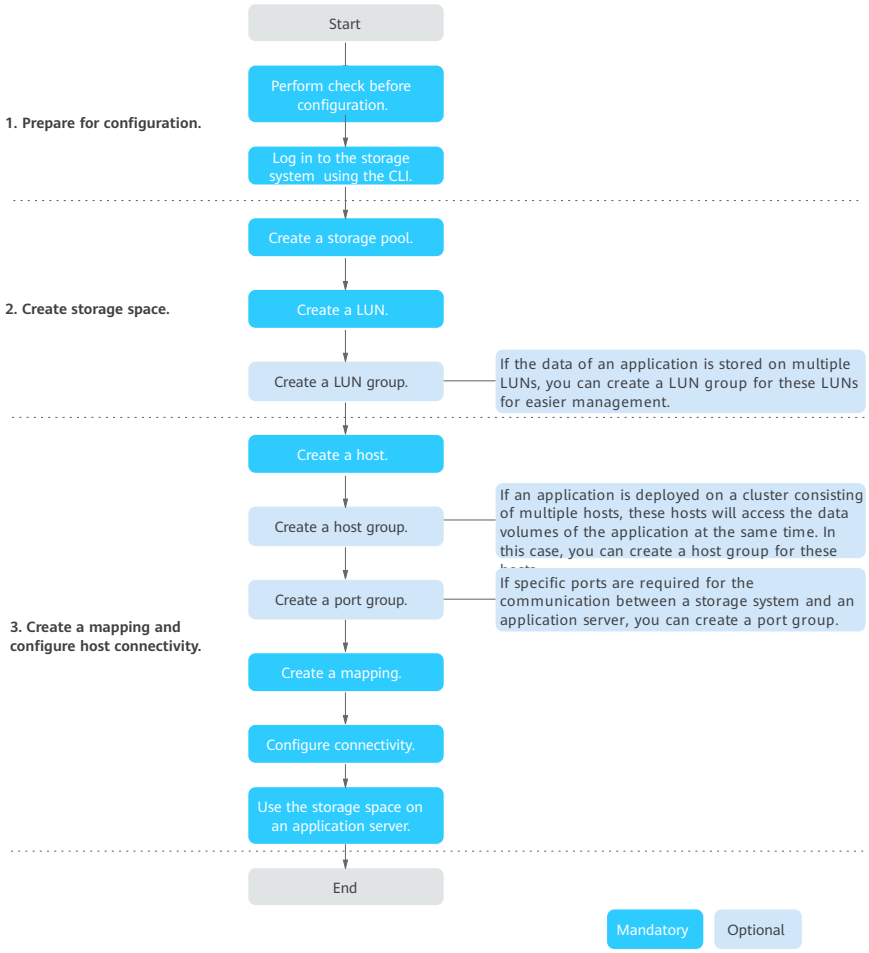
NOTE

- The CLI commands supported by different models may vary.
- For more CLI commands and their description, see the Command Reference specific to your product model and version.

Configuration Process

The following flowchart shows the common configuration process.

Figure A-1 Process for configuring the block storage service



Preparing for the Configuration

Table A-1 Preparations

Item	Reference
Pre-check (software installation check, security check, and network connection status check)	For details, see **4.2 Check Before Configuration**.
Logging in to the storage system using the CLI	For details, see "Logging In to the CLI" in the *Initialization Guide*.

Creating Storage Space

Table A-2 Commands for creating storage space

Procedure	Command
Creating a performance layer	create performance_layer
Creating a storage pool	create storage_pool **NOTE** • When you run the **create storage_pool** command to create a storage pool, the system automatically creates a disk domain in the background. • You can also run the **create disk_domain** and **create storage_pool** commands to create a disk domain and a storage pool, respectively.
Creating LUNs	create lun
(Optional) Creating a LUN group	create lun_group

Creating Mappings and Configuring Host Connectivity

Table A-3 Commands for creating mappings and configuring host connectivity

Procedure	Command
Creating a host	create host
(Optional) Creating a host group	create host_group
(Optional) Creating a port group	create port_group
Creating a mapping	create mapping_view

Procedure	Command

Configuring host connectivity	Host configuration:
	For details, see "Preparing for Configuration" and "Configuring Connectivity" in the *Host Connectivity Guide*.
	Storage configuration:
	● Configuring storage service ports (iSCSI connection)
	Storage systems use logical ports to establish iSCSI connections with hosts. The home ports of logical ports can be physical Ethernet ports, bond ports, or VLANs.
	– (Optional) Creating a bond port:
	`create bond_port`
	– (Optional) Creating a VLAN:
	`create vlan general`
	– Creating a logical port
	(Optional) Creating a logical port based on a bond port:
	`create logical_port bond`
	(Optional) Creating a VLAN-based logical port:
	`create logical_port vlan`
	Creating a logical port based on an Ethernet port:
	`create logical_port eth`
	● Creating an initiator
	– iSCSI connection:
	`create initiator iscsi`
	– Fibre Channel connection:
	`create initiator fc`
	– NVMe over RoCE connection:
	`create nvme_over_roce_initiator general`
	● Adding an initiator for a host
	– iSCSI or Fibre Channel connection:
	`add host initiator`
	– NVMe over RoCE connection:
	`add host nvme_over_roce_initiator`

Using storage space	For details, see "Scanning LUNs on the Host" in the *Host Connectivity Guide*.

B Managing Basic Storage Services Using the CLI

This section provides some CLI commands for managing basic block storage services.

NOTE

- The CLI commands supported by different models may vary.
- For more CLI commands and their description, see the Command Reference specific to your product model and version.

Managing Storage Pools

Table B-1 Commands for managing storage pools

Operation	Command
Creating a performance layer	create performance_layer
Creating a storage pool	create storage_pool
Querying storage pools	show storage_pool general
Modifying a storage pool	change storage_pool general
Deleting a storage pool	delete storage_pool

Managing LUNs

Table B-2 Commands for managing LUNs

Operation	Command
Creating a LUN	create lun
Querying LUNs	show lun general

Operation	Command
Modifying a LUN	change lun
Deleting a LUN	delete lun
Creating an application type for a LUN	create lun_workload_type general
Querying the application type of a LUN	show lun_workload_type general
Changing the application type of a LUN	change lun_workload_type general
Deleting the application type of a LUN	delete lun_workload_type general
Querying information about the mapping related to a specified LUN	show lun mapping_view

Managing LUN Groups

Table B-3 Commands for managing LUN groups

Operation	Command
Creating a LUN group	create lun_group
Querying LUN groups	show lun_group general
Modifying a LUN group	change lun_group
Deleting a LUN group	delete lun_group
Adding LUNs to a LUN group	add lun_group lun
Removing LUNs from a LUN group	remove lun_group lun
Querying LUNs in a LUN group	show lun_group lun
Querying information about the mapping related to a specified LUN group	show lun_group mapping_view

Managing Hosts

Table B-4 Commands for managing hosts

Operation	Command
Creating a host	create host
Querying hosts	show host general
Modifying a host	change host
Deleting a host	delete host
Adding an initiator for a host	add host initiator
Removing an initiator	remove host initiator
Scanning for hosts where UltraPath is installed	scan host
Enabling or disabling the automatic host discovery function	change host_auto_scan
Checking whether the automatic host discovery function is enabled	show host_auto_scan
Querying the host group to which a host is added	show host host_group
Querying all LUNs mapped to a host	show host lun
Querying the host to which a LUN is mapped	show lun host
Querying host link information in a storage system	show host link
Querying information about the mapping related to a specified host	show host mapping_view

Managing Initiators

Table B-5 Commands for managing initiators

Operation	Command
Creating an initiator	create initiator iscsi create initiator fc create nvme_over_roce_initiator general

Operation	Command
Querying initiators	show initiator show nvme_over_roce_initiator general
Modifying an initiator	change initiator change nvme_over_roce_initiator general
Deleting an initiator	delete initiator iscsi delete initiator fc delete nvme_over_roce_initiator general

Managing Host Groups

Table B-6 Commands for managing host groups

Operation	Command
Creating a host group	create host_group
Querying host groups	show host_group general
Modifying a host group	change host_group general
Deleting a host group	delete host_group
Adding hosts to a host group	add host_group host
Removing hosts from a host group	remove host_group host
Querying hosts in a host group	show host_group host
Querying information about the mapping related to a specified host group	show host_group mapping_view

Managing Port Groups

Table B-7 Commands for managing port groups

Operation	Command
Creating a port group	create port_group
Querying port groups	show port_group general
Modify a port group	change port_group general
Deleting a port group	delete port_group
Adding ports to a port group	add port_group port

Operation	Command
Removing ports from a port group	remove port_group port
Querying ports in a port group	show port_group port
Querying information about the mapping related to a specified port group	show port_group mapping_view

Managing Mappings

Table B-8 Commands for managing mappings

Operation	Command
Creating a mapping	create mapping_view
Querying mappings	show mapping_view general
Modifying a mapping	change mapping_view
Deleting a mapping	delete mapping_view
Adding a host group to a mapping	add mapping_view host_group
Removing a host group from a mapping	remove mapping_view host_group
Adding a LUN group to a mapping	add mapping_view lun_group
Removing a LUN group from a mapping	remove mapping_view lun_group
Adding a port group to a mapping	add mapping_view port_group
Removing a port group from a mapping	remove mapping_view port_group
Querying host groups in a mapping	show mapping_view host_group
Querying LUN groups in a mapping	show mapping_view lun_group
Querying port groups in a mapping	show mapping_view port_group

Managing the Service Network

Table B-9 Commands for managing Ethernet ports

Operation	Command
Querying Ethernet ports	show port general physical_type=ETH logic_type=Host_Port
Modifying an Ethernet port	change port eth
Querying bit errors	show port bit_error **NOTE** You can also run this command to query bit errors on other types of ports.

Table B-10 Commands for managing bond ports

Operation	Command
Creating a bond port	create bond_port
Querying bond ports	show bond_port
Modifying a bond port	change bond_port general
Deleting a bond port	delete bond_port

Table B-11 Commands for managing VLANs

Operation	Command
Creating a VLAN	create vlan general
Querying VLANs	show vlan general
Modifying a VLAN	change vlan general
Deleting a VLAN	delete vlan general

Table B-12 Commands for managing logical ports

Operation	Command
Creating a logical port	• Creating a logical port based on a bond port: create logical_port bond • Creating a VLAN-based logical port: create logical_port vlan • Creating a logical port based on an Ethernet port: create logical_port eth

Operation	Command
Querying logical ports	show logical_port general
Modifying a logical port	change logical_port general
Deleting a logical port	delete logical_port general
Adding a route for a logical port	• IPv4 network: add logical_port ipv4_route • IPv6 network: add logical_port ipv6_route
Querying routes of a logical port	show logical_port route
Deleting routes of a logical port	• IPv4 network: remove logical_port ipv4_route • IPv6 network: remove logical_port ipv6_route

Table B-13 Commands for managing the RoCE network

Operation	Command
Querying RoCE ports	show port general physical_type=RoCE
Modifying a RoCE port	change port roce

Table B-14 Commands for managing the Fibre Channel network

Operation	Command
Querying Fibre Channel ports	show port general physical_type=FC
Modifying a Fibre Channel port	change port fc

C How to Obtain Help

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

C.1 Preparations for Contacting Huawei

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

C.1.1 Collecting Troubleshooting Information

You need to collect troubleshooting information before troubleshooting.

You need to collect the following information:

- Name and address of the customer
- Contact person and telephone number
- Time when the fault occurred
- Description of the fault phenomena
- Device type and software version
- Measures taken after the fault occurs and the related results
- Troubleshooting level and required solution deadline

C.1.2 Making Debugging Preparations

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

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

C.2 How to Use the Document

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

To better solve the problems, use the documents before you contact Huawei for technical support.

C.3 How to Obtain Help from Website

Huawei provides users with timely and efficient technical support through the regional offices, secondary technical support system, telephone technical support, remote technical support, and onsite technical support.

Huawei technical support system includes:

- Huawei headquarters technical support department
- Regional office technical support center
- Customer service center
- Technical support website: **https://support.huawei.com/enterprise/**

You can query how to contact the regional offices at **https://support.huawei.com/enterprise/**.

C.4 Ways to Contact Huawei

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

Huawei Technologies Co., Ltd.

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

Website: **https://e.huawei.com/en/**

D 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) on the network. Application programs of data services run on the application server.

Asynchronous remote replication A kind of remote replication. When the data at the primary site is updated, the data does not need to be updated synchronously at the mirroring site to finish the update. In this way, performance is not reduced due to data mirroring.

Air baffle It optimizes the ventilation channels and improves the heat dissipation capability of the system.

Audit log guarantee mode A mode for recording audit logs. This mode preferentially ensures that the audit log function is normal and no audit log is missing.

Audit log non-guarantee mode A mode for recording audit logs. In this mode, services are running properly. Audit logs may be missing.

B

Backup A collection of data stored on (usually removable) non-volatile storage media for purposes of recovery in case the original copy of data is lost or becomes inaccessible; also called a backup copy. To be useful for recovery, a backup must be made by copying the source data image when it is in a consistent state. The act of creating a backup.

Backup window	An interval of time during which a set of data can be backed up without seriously affecting applications that use the data.
Bandwidth	The numerical difference between the upper and lower frequencies of a band of electromagnetic radiation. A deprecated synonym for data transfer capacity that is often incorrectly used to refer to throughput.
Baud rate	The maximum rate of signal state changes per second on a communications circuit. If each signal state change corresponds to a code bit, then the baud rate and the bit rate are the same. It is also possible for signal state changes to correspond to more than one code bit, so the baud rate may be lower than the code 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	The probability that a transmitted bit will be erroneously received. The bit error rate (BER) is measured by counting the number of bits in error at the output of a receiver and dividing by the total number of bits in the transmission. BER is typically expressed as a negative power of 10.
Bonding	Bonding of multiple independent physical network ports into a logical port, which ensures the high availability of server network connections and improves network performance.
Boundary scan	A test methodology that uses shift registers in the output connections of integrated circuits (ICs). One IC is often connected to the next IC. 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 known as Joint Test Action Group (JTAG).
Browser/Server	Architecture that defines the roles of the browser and server. The browser is the service request party and the server is the service provider.
Built-in FRU Alarm indicator	It indicates errors on the built-in FRUs of a controller, such as errors on fans or memory modules.

C

Cache hit ratio	The ratio of the number of cache hits to the number of all I/Os during a read task, usually expressed as a percentage.
Captive screw	Specially designed to lock into place on a parent board or motherboard, allowing for easy installation and removal of attached pieces without release of the screw.
Challenge Handshake Authentication Protocol	A password-based authentication protocol that uses a challenge to verify that a user has access rights to a system. A hash of the supplied password with the challenge is sent for comparison so the cleartext password is never sent over the connection.
Compliance mode	A protection mode of WORM. In compliance mode, files within their protection period cannot be changed or deleted by either the file user or by the system administrator. Files with expired protection periods can be deleted but not changed by the file user or the system administrator.
Controller	The control logic in a disk or tape that performs command decoding and execution, host data transfer, serialization and deserialization of data, error detection and correction, and overall management of device operations. The control logic in a storage subsystem that performs command transformation and routing, aggregation (RAID, mirroring, striping, or other), high-level error recovery, and performance optimization for multiple storage devices.
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.
Copying	A pair state. The state indicates that the source LUN data is being synchronized to the target LUN.
Container root directory	Space used to store the metadata for running container images and container instances.
Container image	An image is a special file system, which provides the programs, libraries, resources, and configuration files required for running containers. It also contains configuration parameters, for example, for anonymous disks, environment variables, and users. The image does not contain dynamic data, and its content will not be modified after construction.
Containerized application	An image can start multiple containers, and an application can contain one or a group of containers.

Container node	Controller that runs the container service.
Configuration item list	A series of modifiable configuration items defined in the Helm chart of the container.
Container service	Containerized application management service, which manages the lifecycle of containerized applications.

D

Data compression	The process of encoding data to reduce its size. Lossy compression (i.e., compression using a technique in which a portion of the original information is lost) is acceptable for some forms of data (e.g., digital images) in some applications, but for most IT applications, lossless compression (i.e., compression using a technique that preserves the entire content of the original data, and from which the original data can be reconstructed exactly) is required.
Data flow	A process that involves processing data extracted from the source system. These processes include: 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	A movement of data or information between information systems, formats, or media. Migration is performed for reasons such as possible decay of storage media, obsolete hardware or software (including obsolete data formats), changing performance requirements, the need for cost efficiencies etc.
Data source	A system, database (database user; database instance), or file that can make BOs persistent.
Dirty data	Data that is stored temporarily on the cache and has not been written onto disks.
Disaster recovery	The recovery of data, access to data and associated processing through a comprehensive process of setting up a redundant site (equipment and work space) with recovery of operational data to continue business operations after a loss of use of all or part of a data center. This involves not only an essential set of data but also an essential set of all the hardware and software to continue processing of that data and business. Any disaster recovery may involve some amount of down time.

Disk array	A set of disks from one or more commonly accessible disk subsystems, combined with a body of control software. The control software presents the disks' storage capacity to hosts as one or more virtual disks. Control software is often called firmware or microcode when it runs in a disk controller. Control software that runs in a host computer is usually called a volume manager.
Disk domain	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 enclosure	Consists of the following parts in redundancy: expansion module, disk, power module, and fan module. System capacity can be expanded by cascading multiple disk enclosures.
Disk location	The process of locating a disk in the storage system by determining the enclosure ID and slot ID of the disk.
Disk utilization	The percentage of used capacity in the total available capacity.

E

eDevLUN	Logical storage array space created by a third-party storage array.
Expansion module	A component used for expansion.
Expansion	Connects a storage system to more disk enclosures through connection cables, expanding the capacity of the storage system.

F

Field replaceable unit	A unit or component of a system that is designed to be replaced in the field, i.e., without returning the system to a factory or repair depot. Field replaceable units may either be customer-replaceable or their replacement may require trained service personnel.
Firmware	Low-level software for booting and operating an intelligent device. Firmware generally resides in read-only memory (ROM) on the device.

Flash Translation Layer	Flash Translation Layer (FTL) organizes and manages host data, enables host data to be allocated to NAND flash chips of SSDs in an orderly manner, maintains the mapping relationship between logical block addresses (LBAs) and physical block addresses (PBAs), and implements garbage collection, wear leveling, and bad block management.
Front-end port	The port that connects the controller enclosure to the service side and transfers service data. Front-end port types are Fibre Channel and iSCSI.
Front-end interconnect I/O module (FIM)	On a storage device, all controllers share the front-end interface modules.

G

Garbage collection	The process of reclaiming resources that are no longer in use. Garbage collection has uses in many aspects of computing and storage. For example, in flash storage, background garbage collection can improve write performance by reducing the need to perform whole block erasures prior to a write.
Gateway	A device that receives data via one protocol and transmits it via another.
Global garbage collection	With a view to defragmentation of storage arrays and garbage collection of disks, global garbage collection reduces garbage of disks by enabling storage arrays to inform disks of not implementing invalid data relocation and of controlling space release so that disks and controllers consume less space, reducing costs and prolonging the useful life of storage arrays.
Global system for mobile communications	The second-generation mobile networking standard defined by the European Telecommunications Standards Institute (ETSI). It is aimed at designing a standard for global mobile phone networks. GSM consists of three main parts: mobile switching subsystem (MSS), base station subsystem (BSS), and mobile station (MS).
Global wear leveling	With a view to individual characteristics of a single disk, global wear leveling uses space allocation and write algorithms to achieve wear leveling among disks, preventing a disk from losing efficacy due to excessive writes and prolonging the useful life of the disk.

H

Hard disk tray	The tray that bears the hard disk.
Heartbeat	Heartbeat supports node communication, fault diagnosis, and event triggering. Heartbeats are protocols that require no acknowledgement. They are transmitted between two devices. The device can judge the validity status of the peer device.
Hit ratio	The ratio of directly accessed I/Os from the cache to all I/Os.
Hot swap	The substitution of a replacement unit (RU) in a system for a defective unit, where the substitution can be performed while the system is performing its normal functioning normally. Hot swaps are physical operations typically performed by humans.
HyperMetro	A value-added service of storage systems. HyperMetro means 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 generally; made up of two storage arrays and one quorum server. HyperMetro services can be created on a HyperMetro domain.
HyperMetro vStore pair	A HyperMetro vStore pair consists of two vStores, that is, two tenants. After a HyperMetro relationship is set up for a pair of vStores, the datasets in the two vStores work in redundancy mode and provide storage services in one dataset view, achieving hitless service failover.
HyperMetro-Inner	On an eight-controller network, with HyperMetro-Inner, continuous mirroring, back-end global sharing, and three-copy technologies, a storage system can tolerate one-by-one failures of seven controllers among eight controllers, concurrent failures of two controllers, and failure of a controller enclosure.
HyperDetect	HyperDetect is a feature that provides ransomware detection.
Handle	A handle resides on the structural part of a module. It is used to insert or remove a module into or from a chassis, not helpful in saving efforts.
Helm chart	A Helm chart is in TAR format. It is similar to the deb package of APT or the rpm package of Yum. It contains a group of yaml files that define Kubernetes resources.

I

In-band management	The management control information of the network and the carrier service information of the user network are transferred through the same logical channel. In-band management enables users to manage storage arrays through commands. Management commands are sent through service channels, such as I/O write and read channels. The advantages of in-band management include high speed, stable transfer, and no additional management network ports required.
Initiator	The system component that originates an I/O command over an I/O interconnect. The endpoint that originates a SCSI I/O command sequence. I/O adapters, network interface cards, and intelligent I/O interconnect control ASICs are typical initiators.
I/O	Shorthand for input/output. I/O is the process of moving data between a computer system's main memory and an external device or interface such as a storage device, display, printer, or network connected to other computer systems. This encompasses reading, or moving data into a computer system's memory, and writing, or moving data from a computer system's memory to another location.
Intelligent ransomware detection	The system detects known ransomware features to identify whether the file systems are attacked by ransomware. If no ransomware attack is identified, the system analyzes and compares the changes in file system snapshots, and uses machine learning algorithms to further check whether the file systems are infected by ransomware.
Interface module	A replaceable field 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/Os or computing requests to physical resources of the system.
Logical unit	The addressable entity within a SCSI target that executes I/O commands.
Logical unit number	The SCSI identifier of a logical unit within a target. Industry shorthand, when phrased as "LUN", for the logical unit indicated by the logical unit number.

LUN formatting	The process of writing 0 bits in the data area of the logical drive and generating related parity bits so that the logical drive can be in the ready state.
LUN mapping	A storage system maps LUNs to application servers so that application servers can access storage resources.
LUN migration	A method for the LUN data to migrate between different physical storage spaces while ensuring data integrity and uninterrupted operation of host services.
LUN snapshot	A type of snapshot created for a LUN. This snapshot is both readable and writable and is mainly used to provide a snapshot LUN from point-in-time LUN data.
Lever	A lever resides on the structural part of a module. It is used to insert or remove a module into or from a chassis, saving efforts.
Local image repository	A private repository used to store the container images and Helm charts imported by users. It is different from the standard image repository. The imported images and Helm charts must meet the compatibility requirements of the system.

M

Maintenance terminal	A computer connected through a serial port or management network port. It maintains the storage system.
Management interface module	The module that integrates one or more management network ports.
Management network	An entity that provides means to transmit and process network management information.
Management network port	The network port on the controller enclosure connected to the maintenance terminal. It is provided for the remote maintenance terminal. Its IP address can be modified with the change of the customer's environment.

N

NVM Express	A host controller interface with a register interface and command set designed for PCI Express-based SSDs.

NVMe SSD	A solid state disk (SSD) with a non-volatile memory express (NVMe) interface. Compared with other SSDs, such SSDs can deliver higher performance and shorter latency.

O

Out-of-band management	A management mode used during out-of-band networking. The management and control information of the network and the bearer service information of the user network are transmitted through different logical channels.

P

Power failure protection	When an external power failure occurs, the AC PEM depends on the battery for power supply. This ensures the integrity of the dirty data in the cache.
Pre-copy	When the system monitors a failing member disk in a RAID group, the system copies the data from the disk to a hot spare disk in advance.
Palm-sized NVMe SSD	A palm-sized NVMe SSD is a type of NVMe SSD of which the dimensions (H x W x D) are 160 mm x 79.8 mm x 9.5 mm (neither 3.5-inch nor 2.5-inch).

Q

Quorum server	A server that can provide arbitration services for clusters or HyperMetro to prevent the resource access conflicts of 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 redundancy 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.

Ransomware file interception	When launching attacks, ransomware usually generates encrypted files with special file name extensions. In light of this, the system intercepts the write to files with specific file name extensions to block the extortion from known ransomware and protect file systems in the storage system.
Real-time ransomware detection	Ransomware has similar I/O behavior characteristics. By analyzing file I/O behavior characteristics, the system quickly filters out abnormal files and performs deep content analysis on the abnormal files to detect files attacked by ransomware. Then, secure snapshots are created for file systems where files have been attacked, and alarms are reported to notify the data protection administrator, limiting the impact of ransomware and reducing losses.
Reconstruction	The regeneration and writing onto one or more replacement disks of all of the user data and check data from a failed disk in a mirrored or RAID array. In most arrays, a rebuild can occur while applications are accessing data on the array's virtual disks.
Redundancy	The inclusion of extra components of a given type in a system (beyond those required by the system to carry out its function) for the purpose of enabling continued operation in the event of a component failure.
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 mirrors 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.
Reverse synchronization	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. On a TCP/IP network, each IP packet is routed independently. Routes can change dynamically.

S

Script	A parameterized list of primitive I/O interconnect operations intended to be executed in sequence. Often used with respect to ports, most of which are able to execute scripts of I/O commands autonomously (without policy processor assistance). A sequence of instructions intended to be parsed and carried out by a command line interpreter or other scripting language. Perl, VBScript, JavaScript and Tcl are all scripting languages.
Serial port	An input/output location (channel) that sends and receives data (one bit at a time) to and from the CPU of a computer or a communications device. Serial ports are used for serial data communication and as interfaces for some peripheral devices, such as mouse devices 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.
Simple network management protocol	An IETF protocol for monitoring and managing systems and devices in a network. The data being monitored and managed is defined by an MIB. The functions supported by the protocol are the request and retrieval of data, the setting or writing of data, and traps that signal the occurrence of events.
Single point of failure	One component or path in a system, the failure of which would make the system inoperable.
Slot	A position defined by an upper guide rail and the corresponding lower guide rail in a frame. A slot houses a board.
Small computer system interface	A collection of ANSI standards and proposed standards that define I/O interconnects primarily intended for connecting storage subsystems or devices to hosts through host bus adapters. Originally intended primarily for use with small (desktop and desk-side workstation) computers, SCSI has been extended to serve most computing needs, and is arguably the most widely implemented I/O interconnect in use today.
Snapshot	A point in time copy of a defined collection of data. Clones and snapshots are full copies. Depending on the system, snapshots may be of files, LUNs, file systems, or any other type of container supported by the system.
Snapshot copy	A copy of a snapshot LUN.

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 system	An integrated system that 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 to the actual storage media used to back up data.
Streaming media	Streaming media is media continuously streamed over the network. Combining technologies concerning streaming media data collection, compression, encoding, storage, transmission, playback, and network communications, streaming media can provide high-quality playback effects in real time at low bandwidth.
Subnet	A type of smaller network that forms a larger network according to a rule, such as, forming a network according to different districts. This facilitates the management of a large network.
Smart disk enclosure	Being compared with traditional disk enclosures, the smart disk enclosures are equipped with Arm chips and DDR memories or other computing modules to achieve powerful computing capabilities. With such capabilities, the smart disk enclosures can help controllers to share some computing loads, accelerating data processing.
Share authentication	During vStore configuration synchronization, the share authentication information (including the share information and domain controller configuration) is synchronized to the secondary end.

T

Target	The endpoint that receives a SCSI I/O command sequence.
Target LUN	The LUN on which target data resides.
Thin LUN	A logic disk that can be accessed by hosts. It dynamically allocates storage resources from the thin pool according to the actual capacity requirements of users.

Topology	The logical layout of the components of a computer system or network and their interconnections. Topology deals with questions of what components are directly connected to other components from the standpoint of being able to communicate. It does not deal with questions of physical location of components or interconnecting cables. The communication infrastructure that provides Fibre Channel communication among a set of PN_Ports (e.g., a Fabric, an Arbitrated Loop, or a combination of the two).
Trim	A method by which the host operating system may inform a storage device of data blocks that are no longer in use and can be reclaimed. Many storage protocols support this functionality via various names, e.g., ATA TRIM and SCSI UNMAP.

U

User interface	The space where users interact with a machine.
U-shaped bracket	It is an optional structural part like letter "U". It is located between the mounting ear of a chassis and the mounting bar of a cabinet or bay and is used to adjust the locations of the chassis and mounting bar of the cabinet or bay.

W

Wear leveling	A set of algorithms utilized by a flash controller to distribute writes and erases across the cells in a flash device. Cells in flash devices have a limited ability to survive write cycles. The purpose of wear leveling is to delay cell wear out and prolong the useful life of the overall flash device.
Write amplification	Increase in the number of write operations by the device beyond the number of write operations requested by hosts.
Write amplification factor	The ratio of the number of write operations on the device to the number of write operations requested by the host.

Write back	A caching technology in which the completion of a write request is signaled as soon as the data is in the cache. Actual writing to non-volatile media occurs at a later time. Write back includes inherent risks: an application will take 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 these reasons, sufficient write back implementations include mechanisms to preserve cache contents across system failures (including power failures) and a flushed cache at system restart time.
Write Once Read Many	A type of storage, designed for fixed content, that preserves what is written to it in an immutable fashion. Optical disks are an example of WORM storage.
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 equipped with the write through technology is approximately that of a non-cached system. However, if the written data is also held in a cache, subsequent read performance may be dramatically improved.

Z

Zone	A collection of Fibre Channel N_Ports and/or NL_Ports (i.e., device ports) that are permitted to communicate with each other via the fabric. Any two N_Ports and/or NL_Ports that are not members of at least one common zone are not permitted to communicate via the fabric. Zone membership may be specified by: 1) port location on a switch, (i.e., Domain_ID and port number); or, 2) the device's N_Port_Name; or, 3) the device's address identifier; or, 4) the device's Node_Name. Well-known addresses are implicitly included in every zone.

E Acronyms and Abbreviations

C	
CHAP	Challenge Handshake Authentication Protocol
CLI	Command Line Interface
F	
FC	Fiber Channel
G	
GUI	Graphical User Interface
H	
HBA	Host Bus Adapter
I	
IE	Internet Explorer
IP	Internet Protocol
IQN	iSCSI Qualified Name
iSCSI	Internet Small Computer Systems Interface
L	
LDAP	Lightweight Directory Access Protocol
LUN	Logical Unit Number
S	
SAS	Serial Attached SCSI
SCSI	Small Computer System Interface

SSD	Solid-State Drive
W	
WWN	World Wide Name
WWPN	World Wide Port Name

OceanStor
6.1.x

Basic Storage Service Configuration Guide for File

Issue 03
Date 2022-08-25

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: https://e.huawei.com

About This Document

Purpose

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

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

Product Model	Product Version
OceanStor 5310	6.1.3 6.1.5
OceanStor 5510	
OceanStor 5610	
OceanStor 6810	
OceanStor 18510	
OceanStor 18810	

NOTICE

This document is updated periodically with the software version. The operations described in this document use the latest version as an example. Note that the supported functions and features vary according to the software version. The content in this document is for reference only.

Intended Audience

This document is intended for:

- Technical support engineers
- Maintenance engineers

Symbol Conventions

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

Symbol	Description
DANGER	Indicates a hazard with a high level of risk which, if not avoided, will result in death or serious injury.
WARNING	Indicates a hazard with a medium level of risk which, if not avoided, could result in death or serious injury.
CAUTION	Indicates a hazard with a low level of risk which, if not avoided, could result in minor or moderate injury.
NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. **NOTICE** is used to address practices not related to personal injury.
NOTE	Supplements the important information in the main text. 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 03 (2022-08-25)

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

- Optimized descriptions about some operations.
- Added accessible IP addresses or IP address segments.

Issue 02 (2022-04-15)

This issue is the second official release.

Issue 01 (2022-01-25)

This issue is the first official release.

Contents

1 Basic Storage Service Overview

This chapter describes the basic storage principles, features, and application scenarios related to file storage services.

1.1 Introduction

A storage system allows application servers to access shared files using different protocols, such as Common Internet File System (CIFS) and Network File System (NFS).

Tips

- A storage system supports two file access protocol management modes: graphical user interface (GUI) and command-line interface (CLI). This document explains how to manage file access protocols using GUI. For details about how to manage file access protocols using the CLI, see the command reference specific to your product model.
- GUIs may vary with product versions and models. The actual GUIs prevail.

1.2 Basic Storage Principles

This section describes basic concepts and working principles of a storage system.

1.2.1 Basic Concepts

Get yourself started with basic concepts.

- Disk domain

  A disk domain consists of multiple disks. When a storage pool is created on DeviceManager, a disk domain is automatically created within the storage

system but is not displayed on DeviceManager. By default, the capacity of a storage pool is equal to the available capacity of the corresponding disk domain.

NOTE

You can create disk domains and storage pools on the CLI. For details, see the command reference specific to your product model and version.

- Storage pool

  A storage resource container, which is created under a disk domain. The storage resources used by application servers are called up from storage pools.

- Chunk (CK)

  A set of consecutive physical spaces of a fixed size on a disk.

- Chunk group (CKG)

  A logical set of CKs on different disks. A CKG has the properties of a redundant array of independent disks (RAID) group.

- Block virtualization

  A new type of RAID technology. Block virtualization divides disks into multiple CKs of a fixed size and organizes them into multiple CKGs. When a disk fails, the disks of the CKG where the CKs in the faulty disk reside also participate in reconstruction. This significantly increases the disks involved in the reconstruction, improving the data reconstruction speed. In addition, block virtualization distributes data to all the disks in a storage system and leverages the I/O processing capability of the storage system.

- Grain

  CKGs are further divided into grains. The size of grains ranges from 4 KB to 64 KB (16 KB by default). Grains are basic units that constitute a file system.

- Hot spare space

  Space used for faulty block data reconstruction in block virtualization. When a CK is faulty, the system lets a CK of the hot spare space take over and instructs the other CKs in the CKG to perform data reconstruction using the hot spare space. This ensures data integrity and read/write performance.

- Reconstruction

  A process of restoring the data saved on a faulty disk to hot spare CKs and replacing the CKs on the faulty disk with the hot spare CKs. During data reconstruction, valid data and parity data must be read and processed to restore the data saved on a faulty disk to hot spare space, thereby ensuring data security and reliability. Traditional reconstruction technologies allow only all disks in the same RAID group as the faulty disk to participate in reconstruction. RAID 2.0+ technology enables all disks in the same storage pool as the faulty disk to participate in reconstruction, boosting data reconstruction speed and shortening data recovery duration.

- Thin file system

  A logical space accessible to a host. A thin file system is configured with an initial capacity when being created and dynamically allocated required storage resources when its initial capacity is insufficient.

- Dtree

A dtree is a subdirectory of a file system. You can manage file quantity or storage space under a dtree.

- Quota, which restricts resource usage.

  There are three types of quotas:

  – Directory quota: restricts the maximum available space or number of files in a dtree.

  – User quota: restricts the space or number of files that can be used by a user.

  – User group quota: restricts the space or number of files that can be used by a user group.

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

  – Space quota: maximum capacity of a quota object

  – File quantity quota: maximum number of files under a quota object

  A quota can be soft or hard.

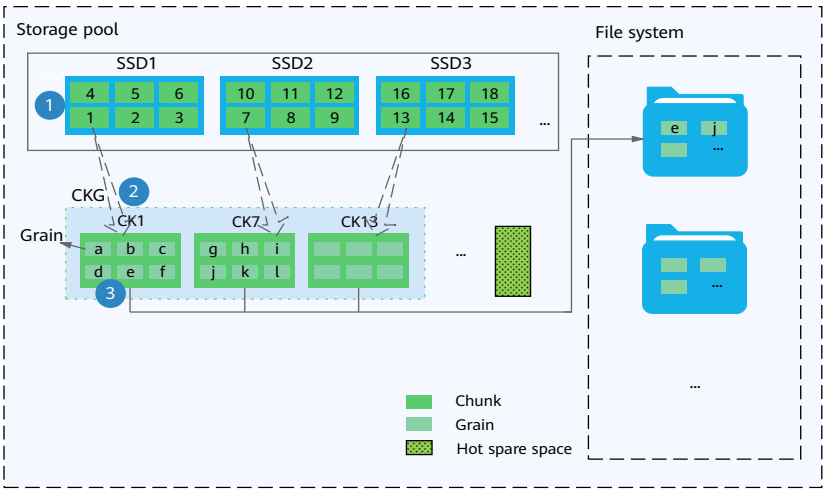
  – For storage space, a hard quota specifies the maximum capacity of the storage space for a quota object. If the space occupied by files exceeds the hard quota, the system immediately forbids writes. A soft quota is the alarm threshold of the storage space for a quota object. If the space occupied by files exceeds the soft quota, the system generates an alarm but allows writes.

  – For file quantity, a hard quota specifies the maximum number of files that can be created under a quota object. If the number of files exceeds the hard quota, the system immediately forbids file creation. The soft quota indicates the alarm threshold of the number of files under a quota object. If the number of files exceeds the soft quota, the system generates an alarm but allows file creation.

1.2.2 Block Virtualization Process

Block virtualization technology enables dynamic allocation and expansion of storage resources in storage pools. Using this technology shortens the response time for data reads/writes in the storage pools and the time needed to reconstruct data on failed disks.

Figure 1-1 Block virtualization process

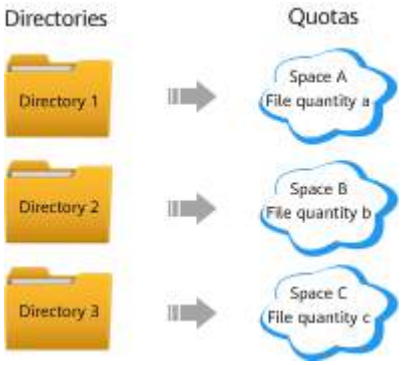


1. The storage system divides each SSD in the storage pool into fixed-size CKs for logical space management.
2. CKs are grouped into CKGs and hot spare space based on the RAID policy and hot spare policy specified on DeviceManager.
3. The storage system divides CKGs into grains based on the application request size configured on DeviceManager. The file systems used by application servers are composed of grains.

1.2.3 Working Principles of Quotas

You can configure different space sizes and file quantities for various quota objects (including directory, user, and user group) for efficient storage resource utilization. **Figure 1-2** shows quotas for directories.

Figure 1-2 Quotas for directories



The storage system uses SmartQuota for quota control. SmartQuota uses the space and file quantity hard quotas to restrict the maximum available resources for each quota object. The process is as follows:

1. For each write I/O, SmartQuota checks whether the new resources (including the space and file quantity) requested by the I/O plus the used resources exceed the hard quota.
   a. If the sum of resources is within the hard quotas, the system permits the write I/O.
   b. If the sum of resources exceeds the hard quotas, the write I/O fails.
2. After the write I/O is allowed, SmartQuota adds the incremental resources (including the space and file quantity) to the previously used resources, updates the quota (latest space + latest file quantity), and enables the quota and I/O data to be written into the file system.

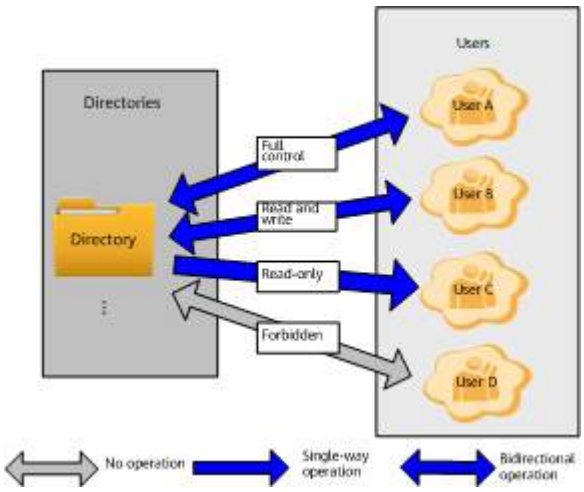
I/O writes and quota update succeed or fail at the same time, ensuring that the used capacity is correct in each I/O check.

If a directory quota, user quota, and group quota are concurrently configured for a shared directory, all of the three quotas take effect for the write I/Os to the directory. If the resources requested by an I/O exceed any of the directory, user, or group hard quota, the I/O will be rejected.

1.2.4 User Permission Control

You can assign different user permissions for the same directory, so that users can only access the directory allowed by their specified permissions.

Figure 1-3 User Permission Control



- Users with the full control permission can:
  Read and write directories.
  Modify directories.
  Obtain all permissions of directories.
- Users with the forbidden permission can view shared directories but cannot perform operations in any directory.

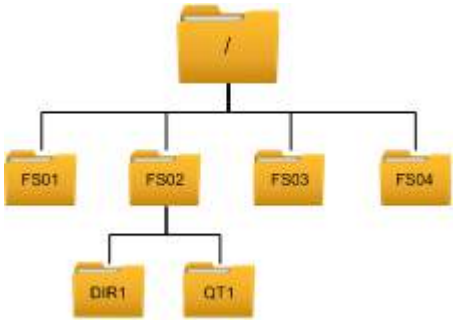
1.2.5 Global Namespace

File virtualization technology based on global namespaces (GNSs) is used to solve problems encountered by file management.

What Is a GNS?

A GNS converges scattered file systems to a virtual root directory /, providing a unified logical view and simplifying file access and management. **Figure 1-4** shows the typical structure of a GNS. The top of a GNS is a virtual root directory, which is represented by a slash (/).

Figure 1-4 Typical structure of a GNS



What Are the Benefits of GNSs?

GNS is the core of file virtualization technology. Similar to Domain Name System (DNS) which enables users to visit websites without memorizing IP addresses, a GNS enables clients to directly access files without knowing their locations. A GNS adopts a unified logical view for file management. Users can create their own file folders or access authorized file folders.

1.2.6 DNS Load Balancing

A host can use a domain name to access NAS services on a storage system. A domain name system (DNS) can balance the loads of multiple IP addresses for a domain name. The following describes how DNS load balancing works:

1. A host sends a DNS request to the storage system's built-in DNS server to obtain an IP address based on the domain name.
2. The built-in DNS server checks the CPU utilization, port bandwidth usage, and NAS connections of all controllers where IP addresses reside, selects an IP address with a relatively light load, and returns it to the host as a DNS response.
3. After receiving the DNS response, the host sends a service request to the target IP address.

DNS load balancing involves domain name resolution and IP address load balancing.

Domain Name Resolution

Storage systems provide the domain name resolution service by enabling logical interfaces (LIFs) to listen to DNS query requests. IP addresses assigned to LIFs can serve as DNS server IP addresses. The following table describes some terms related to domain name resolution.

Table 1-1 Terms related to domain name resolution

Term	Description
LIF	Logical interfaces, running file services. They are created on physical Ethernet ports, bond ports, or VLANs.
Listen to DNS Query Request	An attribute that enables or disables a LIF to listen to DNS query request. After it is enabled for a LIF, the IP address assigned to the LIF can act as a DNS server IP address. Clients can use this IP address to initiate domain name resolution requests.
DNS Zone	DNS employs a tree structure, on which each node is a domain. Typically, each domain is managed by a dedicated DNS server. Each domain can be further divided into subdomains, and a subdomain's resolution tasks are delegated to its server. Traditionally, DNS zone is a concept used in the scenario of configuring DNS servers, and it describes the configuration of a DNS domain. A node located at the end of a DNS tree can also be called a DNS zone. The DNS zone mentioned in this document is essentially a domain name at the end of a DNS tree. The domain name's services are distributed on a storage system. The domain name contains a group of IP addresses. When hosts use the domain name to access a share service on the storage system, it is expected that the loads are evenly distributed on the storage system.

Load Balancing

The following DNS load balancing policies are supported:

- Weighted round robin

  IP addresses which process loads and are under the same domain name are randomly selected for processing.
- CPU usage

  The CPU usage of each node determines the weight. The storage system uses the weight to select a node to process client services.
- Port bandwidth usage

  The total bandwidth usage of each node determines the weight. The storage system uses the weight to select a node to process client services.
- NAS connections

  The NAS connections of each node determine the weight. The storage system uses the weight to select a node to process client services.
- Overall load

  The overall load of CPU usage, bandwidth usage, and number of NAS connections determines node selection. Less loaded nodes are more likely to be selected.

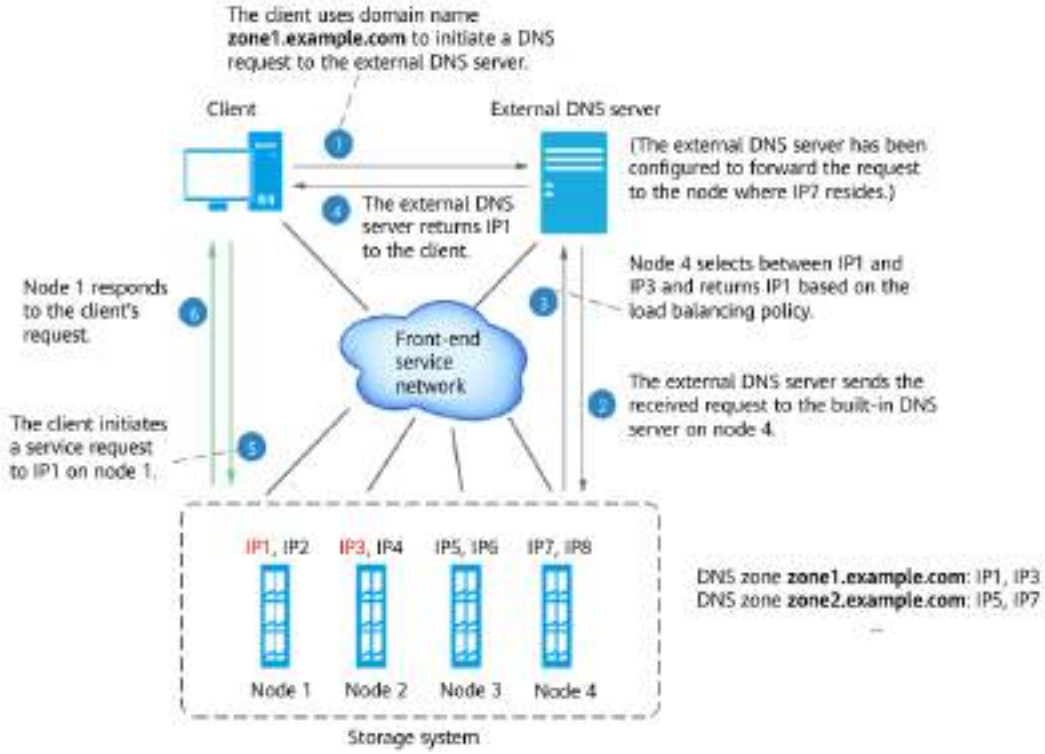
NOTE

- **Weighted round robin** applies to scenarios where the load of storage devices is light or unknown, for example, in the scenario where shares are initially mounted to a large number of NAS clients.
- Other policies apply to scenarios where users want to balance loads based on a certain indicator (such as CPU usage, port bandwidth, number of connections, and overall loads) of running services, for example, in the scenario where shares are mounted to NAS clients in batches during capacity expansion of client applications.

Application Scenarios

DNS load balancing applies to the following scenarios:

Figure 1-5 Scenario 1: Clients are connected to an external DNS server



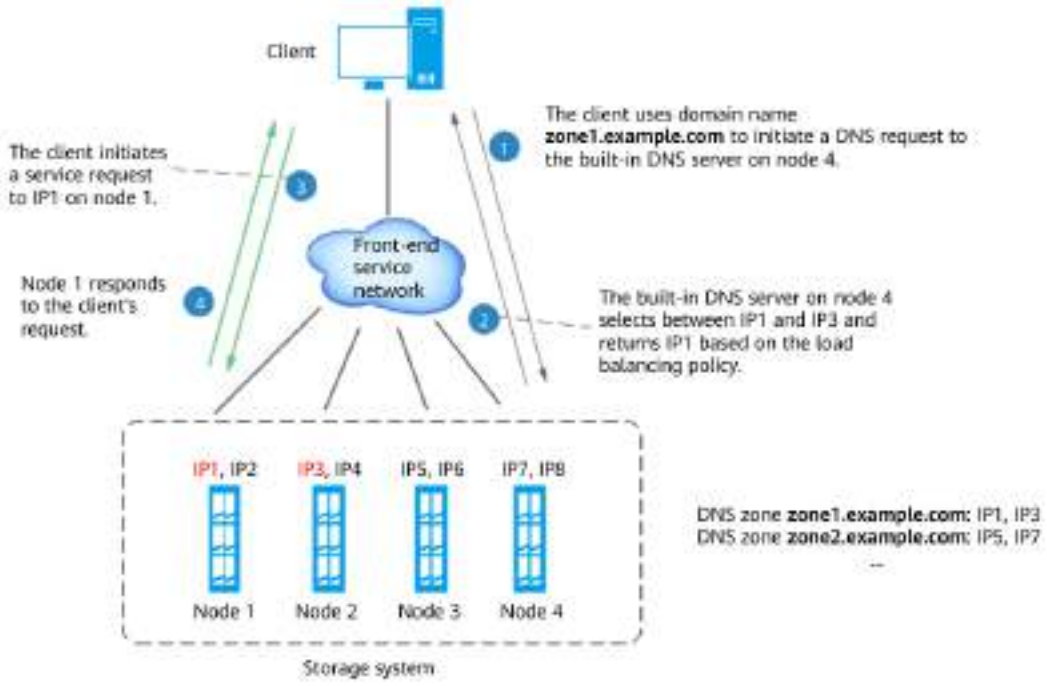
1. A client uses domain name **zone1.example.com** to initiate a DNS request to the external DNS server that has been configured to forward requests to the node where IP7 resides.
2. Upon receiving the DNS request, the external DNS server forwards it to node 4.
3. Upon receiving the **zone1.example.com** domain name resolution request, node 4 queries the DNS zone (**zone1.example.com**), finds that the zone contains two IP addresses (IP1 and IP3), and then returns IP1 based on the calculation result obtained using the current load balancing policy to the external DNS server.

   NOTE

   A built-in DNS server is deployed on each node of the storage system and can independently provide domain name resolution and load balancing services.

4. The external DNS server returns IP1 to the client.
5. After receiving IP1, the client sends the NAS service request to node 1 where IP1 resides.
6. Node 1 responds to the client access request.

Figure 1-6 Scenario 2: Clients are directly connected to a storage system



In scenario 2, no external DNS server is used, and the process is as following:

1. A client uses the domain name (**zone1.example.com**) to initiate a DNS request to the node where IP7 resides.

   NOTE

   IP7 acts as a LIF and is allowed to listen to DNS requests.
2. Upon receiving the DNS request, node 4 where IP7 resides queries the DNS zone (**zone1.example.com**), finds that the zone contains two IP addresses (IP1 and IP3), and then returns IP1 based on the calculation result obtained using the current load balancing policy.
3. After receiving IP1, the client sends the NAS service request to node 1 where IP1 resides.
4. Node 1 responds to the service access request.

DNS load balancing can detect the CPU utilization of the node and the bandwidth usage of the port where each IP address resides, implementing more intelligent load balancing and providing higher storage service performance and reliability as compared with conventional external DNS servers which only provide round-robin load balancing policies.

1.2.7 File System Write Protection

- Write back: A caching technique 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 protection: Data writing to storage systems is prohibited.

In normal cases, the default write mode of a file system is write back. However, the write mode changes to write protection if any of the following faults occurs.

Table 1-2 File system write protection situations and recommended actions

Fault Symptom	Write Protection Situation	Impact and Recommended Action
The backup battery unit (BBU) of a controller enclosure is faulty.	• On a dual-controller storage system, if two BBUs are faulty, an alarm is generated and file systems change to write protection mode. • On a four-controller storage system, if four BBUs are faulty, an alarm is generated and file systems change to write protection mode.	• Impact The write mode of all service objects on the controller enclosure changes to write protection. • Recommended action – Check whether BBUs are properly connected. – Check whether the BBUs break down. Replace the faulty BBUs if any. – If the power of the BBUs is insufficient, wait until the BBUs are fully charged.
The built-in coffer disk of a controller is faulty.	• On a dual-controller storage system, if all coffer disks of the two controllers are faulty, file systems change to write protection mode. • On a four-controller storage system, if all built-in coffer disks of controllers A and B or those of controllers C and D are faulty, file systems change to write protection mode.	• Impact The write mode of all service objects on the controller enclosure changes to write protection. • Recommended action Check whether the built-in coffer disks of the controllers are faulty. Replace the faulty coffer disks if any.

Fault Symptom	Write Protection Situation	Impact and Recommended Action
A controller is faulty.	File systems stay in write back mode for the write back hold time (192 hours by default) if only one controller on a storage system is properly working. If faults are not rectified within this period, the file systems change to write protection mode.	• Impact The write mode of all service objects on the controller enclosure changes to write protection after the specified period of time. • Recommended action – Replace the faulty controller at off-peak hours within the write back hold time. – If a spare part is unavailable during the write back hold time, you can extend the hold time properly after assessing risks to prevent write protection from adversely affecting services.
The storage pool capacity is used up.	An alarm is generated indicating that the storage pool capacity is used up.	• Impact The file systems in the storage pool change to write protection mode. • Recommended action Expand the capacity of the storage pool.
The file system space is used up.	An alarm is generated indicating that the file system space is used up.	• Impact The file system changes to write protection mode. • Recommended action Expand the capacity of the file system.

1.3 Feature Description

This section describes the NFS feature and CIFS feature.

1.3.1 NFS Feature

This section describes the overview, license requirements, impact and restrictions, and application scenarios of the NFS feature.

1.3.1.1 Overview

NFS is a protocol developed by Sun. IETF is in charge of developing its new versions. This protocol is designed for file sharing between Linux and UNIX operating systems.

NFS works based on the client/server architecture. A server provides clients with file system access, whereas clients access shared file systems. NFS enables clients running different operating systems to share files over a network.

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

NFS Lock Policy

By default, NFSv3 supports mandatory locks.

NFS Protocol Version Comparison

The storage systems support NFSv3, NFSv4.0, and NFSv4.1.

The differences between the performance of the NFS protocol versions are as follows:

Table 1-3 Performance of NFS protocol versions

NFS Protocol Version	Performance
NFSv3	NFSv3 does not maintain persistent sessions between hosts and storage devices. Concurrent stateless short connections are established for I/O interactions. Its performance is better than that of NFSv4.0 and NFSv4.1.
NFSv4.0	NFSv4.0 enhances the connection security and maintains persistent session connections. Its performance is only about 30% of that of NFSv3 in small file scenarios, and is basically the same in large file scenarios.
NFSv4.1	NFSv4.1 optimizes the performance in small file scenarios and supports concurrent I/O processing with persistent connections. Its performance is better than that of NFSv4.0 in small file scenarios.

NOTE

The performance may vary with different test conditions. The actual test result in the user environment prevails.

In conclusion, NFSv4.0 delivers higher security but lower performance than NFSv3. NFSv4.1 is recommended if fine-grained NFSv4 ACL permission control and higher performance are required. NFSv3 is also a mainstream option if the NAS network is highly secure and security can be guaranteed through network isolation.

1.3.1.2 License Requirements

This section describes the license requirements and specifications of NFS.

License Requirements

The NFS feature is license-controlled. Ensure that the license file imported to the system contains the **NAS Foundation** feature.

Specifications

Specifications vary with product models. For details about the specifications, visit **Specifications Query**.

1.3.1.3 Impact and 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, NFSv4.0, and NFSv4.1.

Item	Document
RFC1813	NFS Version 3 Protocol Specification
RFC3530	Network File System (NFS) Version 4 Protocol
RFC5661	Network File System (NFS) Version 4 Minor Version 1 Protocol

Network Requirements

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

Interaction with Other Features

Table 1-4 describes the relationship between the NFS feature and other features.

Table 1-4 Relationship between the NFS feature and other features

Feature	Relationship
File system snapshot	Before accessing snapshots of a file system, you must create an NFS share for the file system.
CIFS share	In multi-protocol sharing mode, you are advised to use the byte range lock on an application to exclusively access a file in a file system to prevent file data overwriting or loss and ensure shared data consistency.

Compatibility

Verify that clients' operating systems are compatible with the storage system. You can query the compatibility using the **Huawei Storage Interoperability Navigator**.

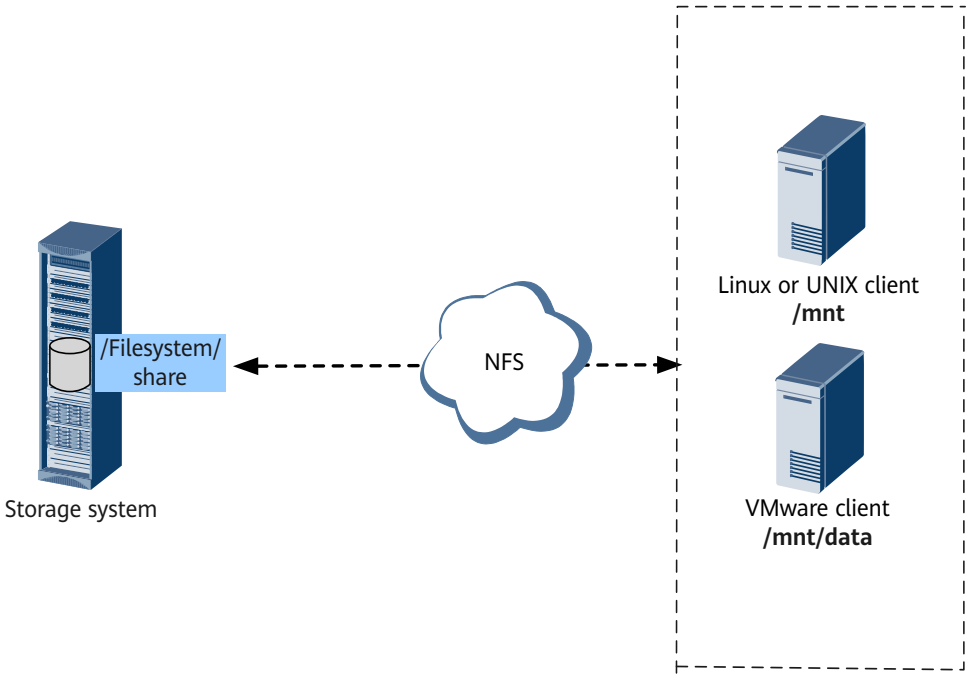
1.3.1.4 Application Scenarios

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, Lightweight Directory Access Protocol (LDAP) domain environment, and network information service (NIS) domain environment.

NFS Share in a Non-Domain Environment

NFS shares in a non-domain environment are commonly used for small- and medium-sized enterprises. **Figure 1-7** shows the networking. On the network, the storage system serves as an 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 as if they are accessing local files. Clients whose IP addresses are configured in the storage system are allowed to access the shared file system.

Figure 1-7 NFS share in a non-domain environment



NFS Share in a Domain Environment

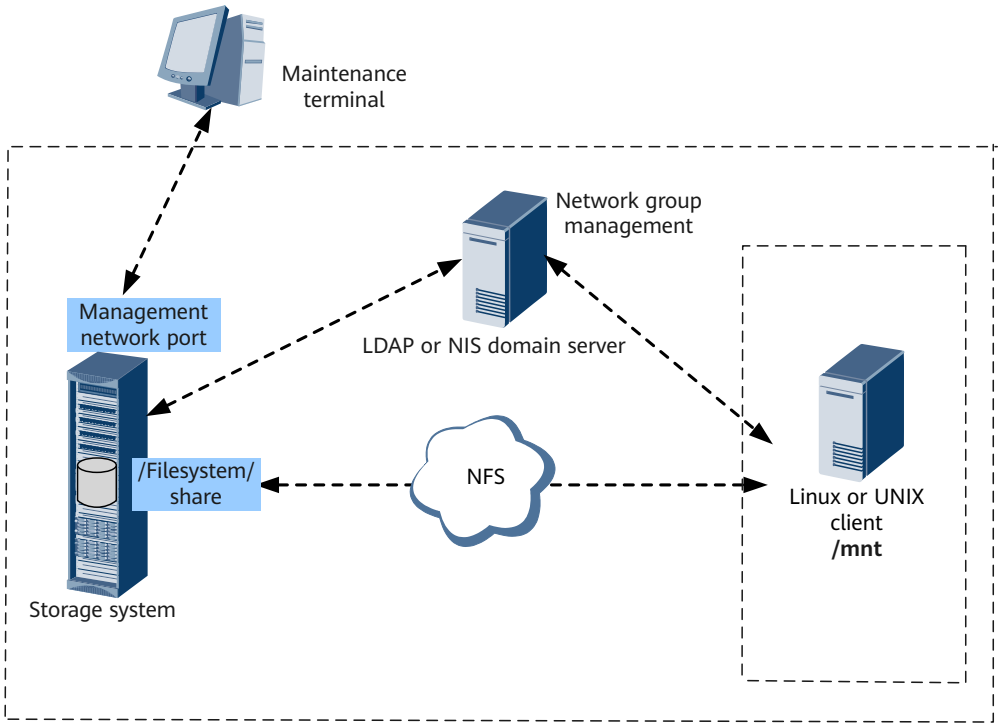
Domains enable accounts, applications, and networks to be centrally managed. In Linux, LDAP and NIS domains are available.

LDAP is an open, extendable network protocol. 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 an LDAP domain, 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 central management of system databases. It provides a yellow page function to support the centralized management of network information. NIS works based on the client/server architecture. When the user name and password of a user are saved in the NIS server database, the user can log in to an NIS client and maintain the database to centrally manage the network information on the LAN.

As shown in **Figure 1-8**, when a client needs to access an NFS share provided by a storage system in a domain environment, the storage system uses the domain server network group to authenticate the accessible IP address, ensuring the reliability of file system data.

Figure 1-8 NFS share in a domain environment



1.3.2 CIFS Feature

This section describes the overview, license requirements, impact and restrictions, and application scenarios of the CIFS feature.

1.3.2.1 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.

Introduction to CIFS

Server Message Block (SMB) is a protocol used for network file access and CIFS is a public version of SMB. SMB allows a local PC to access files and request services on PCs over the local area network (LAN).

Storage systems support SMB 2.0, SMB 2.1, and SMB 3.0. Storage systems are adaptive to protocol versions according to Windows OSs running on clients.

- If a client runs Windows Server 2008 or Windows Vista, SMB 2.0 is used.
- If a client runs Windows Server 2008 R2 or Windows 7, SMB 2.1 is used.
- If a client runs Windows Server 2012 or Windows 8, SMB 3.0 is used.

NOTE

If a client supports multiple versions of SMB, it is recommended that you select a higher version to ensure higher security.

The CIFS feature allows Windows clients to identify and access shared resources provided by a storage system. With CIFS, clients can quickly read, write, and create files in a storage system as on local PCs.

Basic Concepts

Homedir: one of CIFS share modes. Homedir shares a file system to a specific user as a private directory. Different from common CIFS shares, when accessing a Homedir share, a user accesses a private directory. Homedir shares can be created (including share permission setting and feature enabling/disabling), queried, modified, and deleted like common CIFS shares.

Homedir has the following benefits:

- Allows a customer to map Homedir directories of various users to different file system paths based on service requirements.
- Allows a user to access multiple Homedir shares using Homedir share names.
- Allows all share-related features to be enabled/disabled like common CIFS shares.
- Offers **Auto Create Path** for mapping rules, preventing administrators from creating Homedir directories separately for each CIFS user and thereby simplifying O&M.

1.3.2.2 License Requirements

This section describes the license requirements and specifications of CIFS.

License Requirements

The CIFS feature is license-controlled. Ensure that the license file imported to the system contains the **NAS Foundation** feature.

Specifications

Specifications vary with product models. For details about the specifications, visit **Specifications Query**.

1.3.2.3 Impact and 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

Storage systems support SMB 2.0, SMB 2.1, and SMB 3.0.

Network Requirements

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

Interaction with Other Features

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

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

Feature	Relationship
File system snapshot	Before accessing snapshots of a file system, you must create a CIFS share for the file system.
NFS share	In multi-protocol sharing mode, you are advised to use the byte range lock on an application to exclusively access a file in a file system to prevent file data overwriting or loss and ensure shared data consistency.

Compatibility

Verify that clients' operating systems are compatible with the storage system. You can query the compatibility using the **Huawei Storage Interoperability Navigator**.

Restrictions

- The failover function is enabled by default.
- If this function is enabled, the read and write performance for small files will be affected. To ensure the performance, you can run the **change share cifs share_id=? continue_available_enabled=no smb2_ca_enabled=no** command to disable the function. To ensure reliability, you are advised to enable the failover function.
- For details about this command, see the command reference specific to your product model.

NOTE

After the failover function is enabled, the storage system retains persistent handles for 60 seconds when the SMB session between the client and the storage system is disconnected.

1.3.2.4 Application Scenarios

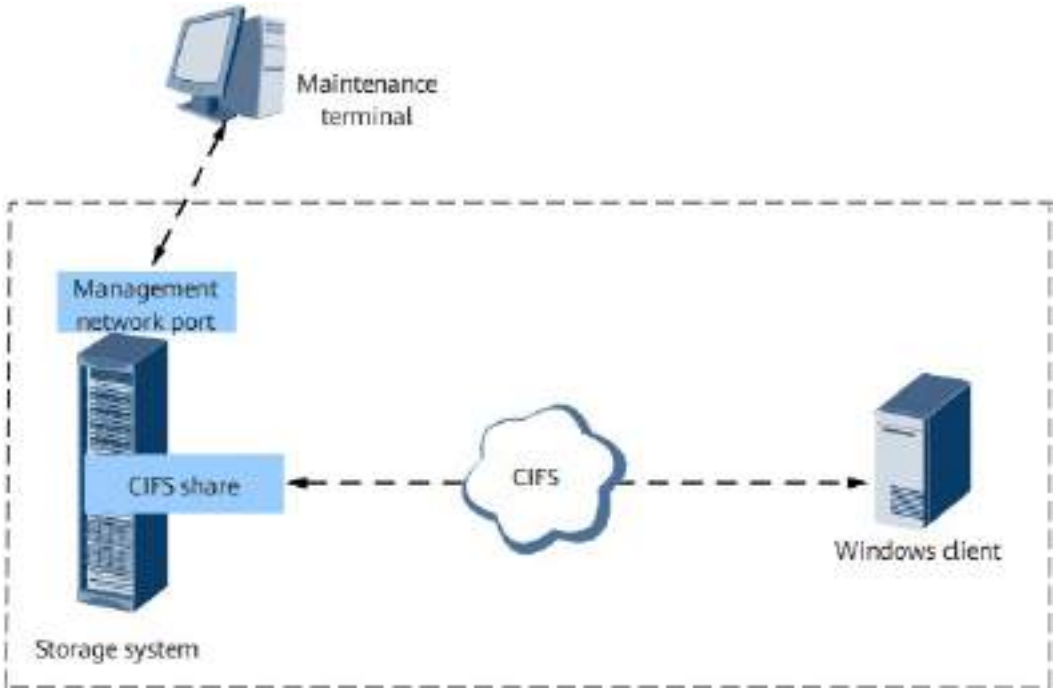
The CIFS share feature is primarily used by Windows clients to share files in a non-domain or AD domain environment.

CIFS Share in a Non-Domain Environment

A storage system can employ CIFS shares to share file systems as directories to users. Users can only view or access their own shared directories.

As shown in **Figure 1-9**, a storage system serves as a CIFS server and employs the CIFS 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 as if they are accessing local files. You can set locally authenticated user names and passwords in the storage system to determine the local authentication information that can be used for accessing the file system.

Figure 1-9 CIFS share in a non-domain environment

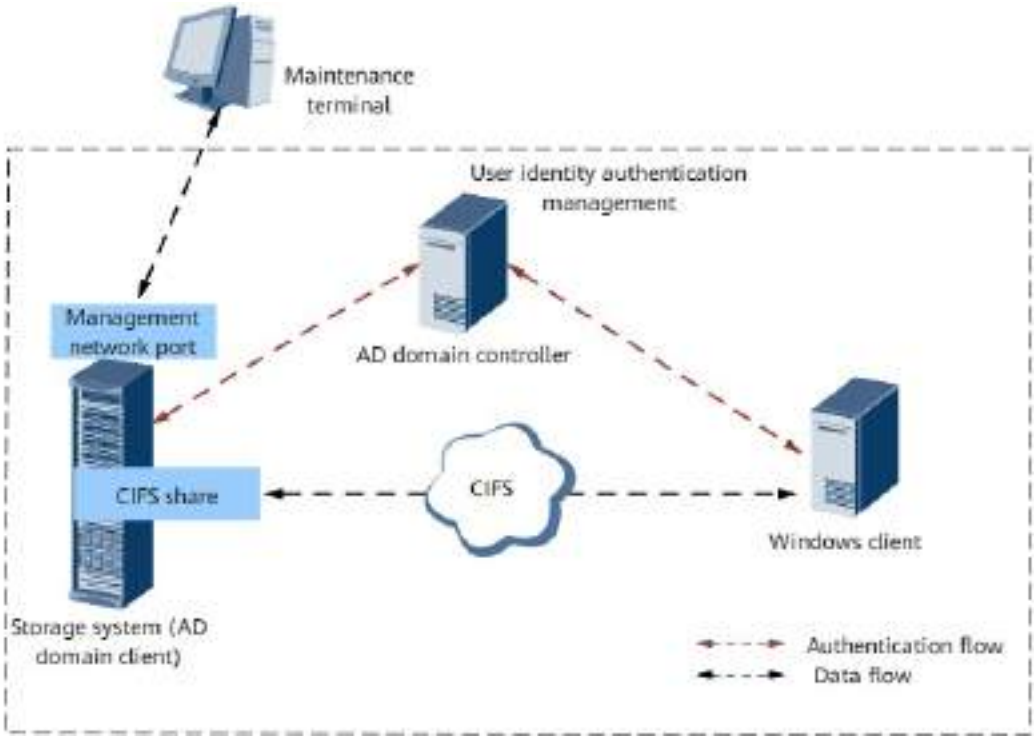


CIFS Share in an AD Domain Environment

With the expansion of LANs and WANs, many enterprises use AD domains to manage Windows-based networks, simplifying network management and improving network scalability.

A storage system can be added to an AD domain as a client, thereby being seamlessly integrated with the AD domain. An AD domain controller saves information about all the clients and groups in the domain. The AD domain controller authenticates clients which request access to CIFS shares provided by the storage system. AD domain users can implement file-specific permission management. Different clients have different permissions for each shared directory. A client in an AD domain can only access the shared directory with the same name as the client.

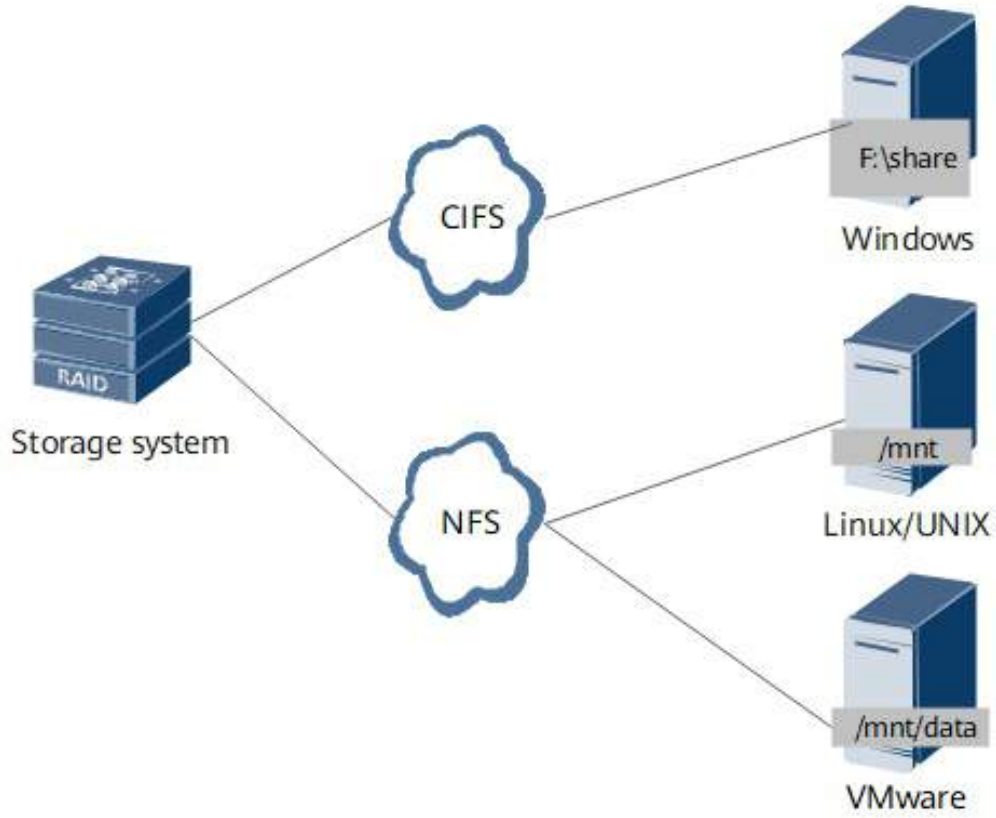
Figure 1-10 CIFS share in an AD domain environment



1.4 Application Scenarios

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

Figure 1-11 Scenario in which application servers access a storage system



2 Planning Basic Storage Services

This chapter describes how to make appropriate plans to facilitate subsequent configuration and maintenance before configuring basic storage services.

2.1 Planning Storage Resources

This section describes how to properly plan storage resources to better meet the service needs.

2.1.1 Planning the Available Capacity

The available capacity of a storage system must be properly planned to ensure sufficient capacity for service data.

For details about the available capacity and purchased capacity, contact your local Huawei representative office or Huawei authorized distributor.

When planning the available capacity, you must consider the nominal disk capacity, hot spare capacity, and RAID usage.

- Nominal disk capacity

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

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

- Hot spare capacity

  The storage system provides hot spare space to take over data from any failed disk.

- RAID usage

  The capacity used by parity data varies with the RAID level.

2.1.2 Planning Storage Pools

Storage pools of a storage system can be used for both block services and file services. For details about how to plan and configure storage pools, see the *Basic Storage Service Configuration Guide for Block*.

This document focuses on the configuration and management of the file system sharing service.

2.1.3 Planning File Systems

Properly plan file systems to ensure optimal storage system performance. The following table describes major file system parameters.

Table 2-1 File system parameter planning

Parameter	Description
Capacity	Plan the capacity and quantity of file systems based on service requirements.
Quantity	

Parameter	Description
Application Type	Application type of the file system. Preset application types are provided for typical applications. In file service scenarios, possible options are **NAS_Default**, **NAS_Virtual_Machine**, **NAS_Database**, **NAS_Large_File**, **Office_Automation**, **NAS_EDA**, and **NAS_Others**. **NOTE** • The **Application Request Size** and **File System Distribution Algorithm** parameters are set for preset application types. The value of **Application Request Size** is **16 KB** for **NAS_Default**, **NAS_Virtual_Machine**, **Office_Automation**, **NAS_EDA**, and **NAS_Others**, **8 KB** for **NAS_Database**, and **32 KB** for **NAS_Large_File**. If **Application Type** is set to **NAS_Default**, **NAS_Large_File**, **Office_Automation**, **NAS_EDA**, or **NAS_Others**, **File System Distribution Algorithm** is **Directory balance mode**. In this mode, directories are evenly allocated to each controller by quantity. If **Application Type** is set to **NAS_Virtual_Machine**, or **NAS_Database**, **File System Distribution Algorithm** is **Performance mode**. In this mode, directories and files are allocated to the access controller preferentially to improve access performance of directories and files. • When SmartCompression and SmartDedupe licenses are imported to the system, the preset application types also display whether SmartCompression and SmartDedupe are enabled. For details, see *SmartDedupe and SmartCompression Feature Guide for File* specific to your product model and version. • **Application Type** cannot be changed once being configured. You are advised to set the value based on the service I/O model. • To create an application type, run the **create workload_type general name=? io_size=?** command. For details, see the *Command Reference* of the desired model and version. • You can also run the **create file_system general** or **change file_system general** command to create or modify a file system respectively. For details, see the *Command Reference* of the desired model and version.
Dtree	A dtree is the first-level subdirectory of a file system. In a dtree, you can set directory quotas, user quotas, and user group quotas to manage the space utilization of the subdirectory.

Parameter	Description
Quota	A quota restricts the file quantity and storage space size in a dtree. **Directory Quota**, **User Quota,** and **User Group Quota** are available. • If you want to restrict the space used by files or the number of files in the root directory, select **Directory quota**. • If you want to restrict the space used by files or the number of files for a single user, select **User Quota**. • If you want to restrict the space used by files or the number of files for a single user group, select **User Group Quota**.

NOTE

- For details about file system parameters, refer to "Creating a File System" in this document.
- For details about how to plan value-added features, see the corresponding feature guides.

2.2 Planning Networks

Properly plan the network settings of a storage system to ensure that application servers can safely and efficiently access shared files.

NOTE

You are advised to configure IP address failover before configuring basic storage services to ensure service reliability in the event of port or link failures. You must reserve at least two Ethernet, VLAN, or bond ports for IP address failover. When a port fails, services can be smoothly switched to the other port. IP address failover is implemented based on switches. For details about how to configure and manage IP address failover, see the IP address failover deployment guide specific to your product model and version.

Planning Ethernet Ports

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

Planning Bond Ports

Port bonding provides more bandwidth and higher redundancy for links. Although ports are bonded, each session still transmits data through a single port and the total bandwidth can be increased only when there are multiple sessions. Determine whether to bond ports based on site requirements.

Port bonding on the storage system has the following restrictions:

- Only Ethernet ports that have the same rate and are on the same controller can be bonded. Ports cannot be bonded across controllers. Non-Ethernet ports cannot be bonded.
- Link aggregation (IEEE 802.3ad) is supported.

  NOTE

  The storage system supports the IEEE 802.3ad protocol, that is, the bonding mode is **4**. You can run the **ifm.sh showbondmode** command in mini-system mode to query the bonding mode.
- For OceanStor 5310, OceanStor 5510 and OceanStor 5610:
  - GE interface modules (not supporting TOE) support port bonding across modules by default.
  - 10GE, 25GE, 40GE, and 100GE interface modules (supporting TOE) do not support port bonding across modules by default. They support port bonding across modules after TOE is disabled.

    NOTICE

    To disable the TOE function of a port, contact Huawei technical support.
  - The onboard network ports of OceanStor 5310 can be bonded across interface modules and the port rates must be the same.
- For OceanStor 6810, OceanStor 18510, and OceanStor 18810, interface modules in the same quadrant can be bonded across interface modules, and the TOE function of the ports to be bonded must be disabled.

  NOTICE

  To disable the TOE function of a port, contact Huawei technical support.

  For OceanStor 6810, OceanStor 18510, and OceanStor 18810, each interface module can use only one bonding mode. That is, an interface module does not allow bonding across modules and bonding within the module at the same time.
- Read-only users are not allowed to bond Ethernet ports.
- Each Ethernet port can be added to only one bond port.
- A member port of a port group cannot be added to a bond port.
- Management network ports cannot be bonded.
- Member ports in the same bond port cannot connect to different switch networks.
- Before using the port bonding function, ensure that the function of forwarding Layer 2 network protocol packets has been enabled on switches. For example, for a Huawei switch, BPDU packet forwarding must be enabled. For details, see the product documentation specific to your switches or consult the technical support of the corresponding vendor.
- After Ethernet ports are bonded, their MTU changes to the default value and you need to configure the switch port mode. Take Huawei switches as an

example. You must set the ports on the Huawei switches to work in static LACP mode.

NOTICE

The link aggregation modes vary with switch manufacturers. If a switch from another vendor is used, contact technical support of the switch manufacturer for specific link aggregation configurations.

Port bonding on the host has the following restriction:

If the TOE function is enabled on the storage system and the host port connecting to the switch must be bonded, the bonding mode must be set to 4.

NOTE

If the preceding restriction cannot be met, disable the TOE function of the port.

Planning VLANs

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

VLANs are created based on Ethernet ports or bond ports. One physical port can belong to multiple VLANs. A bond port instead of a single member port can be used to create a VLAN.

Planning Logical Ports

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

- A physical port can be configured with logical ports on the same or different network segments.
- Different physical ports on a controller can be configured with logical ports on the same or different network segments.
- Logical ports can be created on Ethernet ports, bond ports, or VLAN ports only if these ports are not configured with any IP addresses.
- You must specify a home port for logical ports. If the home port fails, services will fail over to a functional port.

Planning BGP

In the NAS HyperMetro scenario, the NAS LIF configuration is synchronized between two sites. When a NAS LIF is activated at the other site, the route from the NAS LIF to the host is configured. This route is the same at the two sites. In this case, the two sites must be on the same subnet. However, the next-generation data centers use Layer 3 networking, so the two HyperMetro sites may be deployed on different subnets. This requires LIF failover across subnets.

The storage system supports BGP and adds a VIP LIF. The storage system advertises the routing information of the VIP LIF through BGP, which allows the

VIP LIF to fail over across subnets. For details, see **A Configuring and Managing BGP**.

2.3 Planning NFS Shares

Table 2-2 lists items to be planned for NFS shares.

Table 2-2 NFS share planning

Planned Item	Subitem	Requirement
Network	Storage system IP address	The storage system provides shared space for a client through a logical interface (LIF[a]).
	Client IP address	The client and storage system are accessible and can ping each other.
	IP address of a maintenance terminal	The maintenance terminal and storage system are accessible and can ping each other.
	(Optional) NIS or LDAP domain	Collect the domain server's IP address and domain information. Ensure that the domain server and storage system reside on the same network and can ping each other.
Domain	Non-domain, NIS domain, or LDAP domain	Plan 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.
Permission	-	Plan a user's permissions for accessing a file system. When NFSv3 is used, a storage system supports User, Group, Other (UGO) permissions, and ACL permissions are not supported. UGO permissions include **Execute**, **Read**, and **Write**.
Quota	(Optional) Quota for file system's dtrees.	Quotas can be defined only for file system's dtrees based on customer requirements.
a: A LIF is created on an Ethernet port, bond port, or VLAN port. Each LIF is configured with an IP address.		

NOTE

If a firewall is deployed, ensure that the RPCBIND service on a client is properly running (that is, the client listens to TCP/UDP port 111) to provide RPC port mapping service. In addition, ensure that firewall rules allow the storage system to initiate connection requests and send messages to the client. For example, when an NFSv3 client uses Network Lock Manager (NLM) to request the block lock service from a storage system, the storage system establishes a connection to the client through port 2051 and notifies the client that a block lock is successfully added.

2.4 Planning CIFS Shares

Table 2-3 lists the items to be planned for CIFS shares.

Table 2-3 CIFS share planning

Planned Item	Subitem	Requirement
Network	Storage system IP address	The storage system provides shared space for a client through a logical interface (LIF[a]).
	Client IP address	The client and storage system are accessible and can ping each other.
	IP address of a maintenance terminal	The maintenance terminal and storage system are accessible and can ping each other.
	(Optional) AD domain	Collect IP addresses and host names of the AD domain server and DNS server. The servers and storage system must reside on the same network and can ping each other.
Domain	AD domain or non-domain	Plan an AD domain or non-domain environment based on onsite requirements. The advantages of the AD domain and non-domain environments are described as follows: • AD domain: A storage system can be seamlessly integrated with an AD domain. Domain users can directly access the shared space, and no local users need to be created. • Non-domain: No domain environments need to be set up.

Planned Item	Subitem	Requirement
Authentication mode	Local or domain authentication	Plan an authentication mode based on the domain environment (AD domain or non-domain environment). ● Local authentication: Local users are used to authenticate user identity. ● Domain authentication: Domain servers are used to authenticate user identity.
Share mode	CIFS share	In CIFS share mode, a file system or its Dtree is shared among authenticated users including local and domain authentication users. Users have their permissions set by the storage system for accessing CIFS shares.
	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.
User group	-	Local authentication user group or domain user group.
Permission	Permission of a user or user group to access a share	Plan a user's permission to access a CIFS share. Possible permissions are: ● Read-only, enabling a user to: – Read the CIFS share and its subdirectories. – Execute executable files. ● Read and write, enabling a user to: – Perform operations that are allowed by the read-only permission. – Create and delete shared files and subdirectories. – Modify file contents. ● Full control, enabling a user to: – Perform operations that are allowed by the read and write permission. – Modify ACLs of files and subdirectories in the CIFS share. ● Forbidden: A user is forbidden to access the CIFS share.

Planned Item	Subitem	Requirement
a: A LIF is created on an Ethernet port, bond port, or VLAN port. Each LIF is configured with an IP address.		

NOTE

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

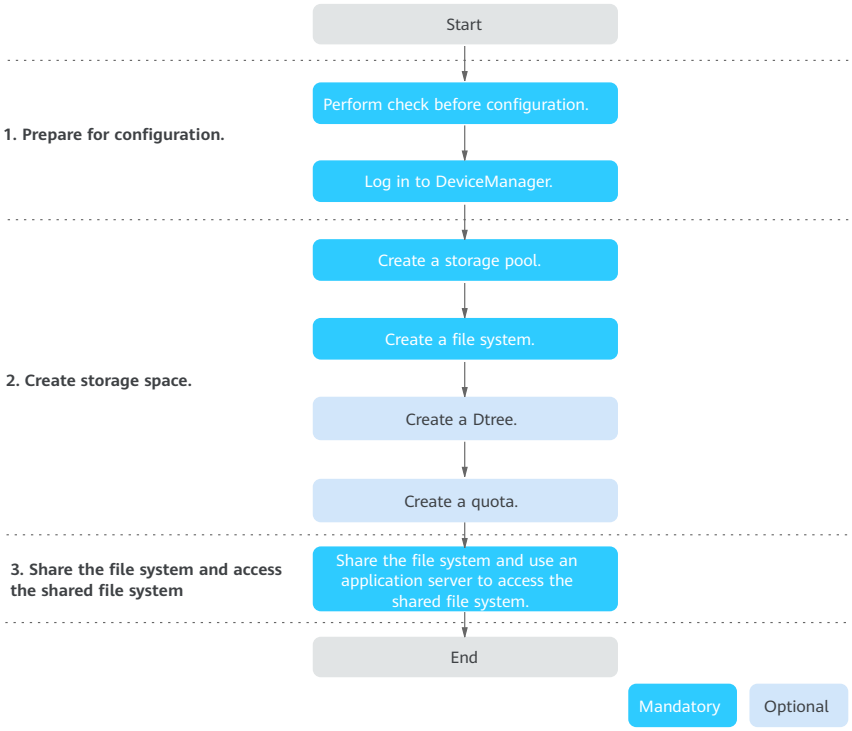
3 Configuring Basic Storage Services

This chapter describes how to configure a storage system to divide its storage space into file systems and configure shares so that application servers can use storage space by accessing shares.

3.1 Configuration Process

The following figure shows the process for configuring file services.

Figure 3-1 File service configuration process



3.2 Check Before Configuration

Check the license, network connection status, and compatibility to ensure that site requirements are met.

Checking the License

On DeviceManager, check whether a license file has been imported and **SmartQuota** and **NAS Foundation** are displayed in the feature list.

- If no license file has been imported, import a license file by referring to the initialization guide.
- If the features granted by the license are different from those you purchased, contact technical support engineers.

Checking Network Connection Status

Table 3-1 lists the check items and describes the check methods.

Table 3-1 Network connection status checklist

Category	Check Item	Check Method
Connection between a maintenance terminal and a storage system	Check whether the management network port on the storage system communicates with the maintenance terminal properly.	In CLI mode of the maintenance terminal, run the following command: • For IPv4, **ping** *ip* (where *ip* indicates the IP address of the management network port). • For IPv6, **ping6** *ip* (where *ip* indicates the IP address of the management network port). If the maintenance terminal receives data packets from the management network port, the storage system and maintenance terminal communicate properly. If the maintenance terminal receives no data packets from the management network port, verify that the physical link is up and the IP address is correctly configured.
Connection between a storage system and an application server (using a Windows application server as an example)	Check whether the front-end port communicates with the service network port on the application server properly.	On the CLI of the application server, run the following command: • For IPv4, **ping** *ip* (where *ip* indicates the IP address of the iSCSI front-end port). • For IPv6, **ping6** *ip* (where *ip* indicates the IP address of the iSCSI front-end port). If the application server receives data packets from the front-end port, the storage system and application server communicate properly. If the application server receives no data packets from the front-end port, replace the network cable or change the IP address of the front-end port, and try again.

Category	Check Item	Check Method
Connection between the storage system and switches (if switches are used)	To ensure that a link can be recovered as soon as possible after a fault occurs, you are advised to configure the ports on the switches connected to the storage system as edge ports. **NOTE** The commands for configuring a switch port as an edge port vary according to the switch vendor. For details, see the product documentation of the corresponding switch or consult the technical support of the corresponding vendor. Huawei CE series switches are used as an example. You can run the **stp edged-port enable** command to configure a port as an edge port.	Huawei CE series switches are used as an example. You can run the **display stp global** command and check the **Edged port default** field in the command output to determine whether the port is configured as an edge port. If the value is **Enabled**, the port is configured as an edge port. If the value is **Disabled**, the port is configured as a non-edge port.

Checking Compatibility

Verify that clients' operating systems are compatible with the storage system. You can query the compatibility using the **Huawei Storage Interoperability Navigator**.

3.3 Logging In to DeviceManager

DeviceManager is a device management program developed by Huawei. DeviceManager has been loaded to a storage system before delivery. You can log in to DeviceManager to manage storage resources in a centralized manner.

For details about how to log in to DeviceManager, see "Logging In to DeviceManager" in the initialization guide specific to your product model and version.

3.4 Creating a Storage Pool

Storage pools of a storage system can be used for both block services and file services. For details about how to plan and configure storage pools, see the *Basic Storage Service Configuration Guide for Block*.

This document focuses on the configuration and management of the file system sharing service.

3.5 Creating a File System

This section describes how to create a file system to share storage resources in the form of files or directories.

Context

- File systems created in the storage system are thin file systems. That is, the storage system will not allocate all of the configured capacity to file systems at a time. Within the configured capacity, the storage system allocates storage resources to file systems based on the actual capacity used by hosts.
- Before creating a file system, you are advised to handle the alarms indicating that the storage pool capacity is about to be used up.

Precautions

In a storage pool, if the total capacity of all thin file systems exceeds that of the storage pool, data cannot be written if the capacity of the storage pool is used up.

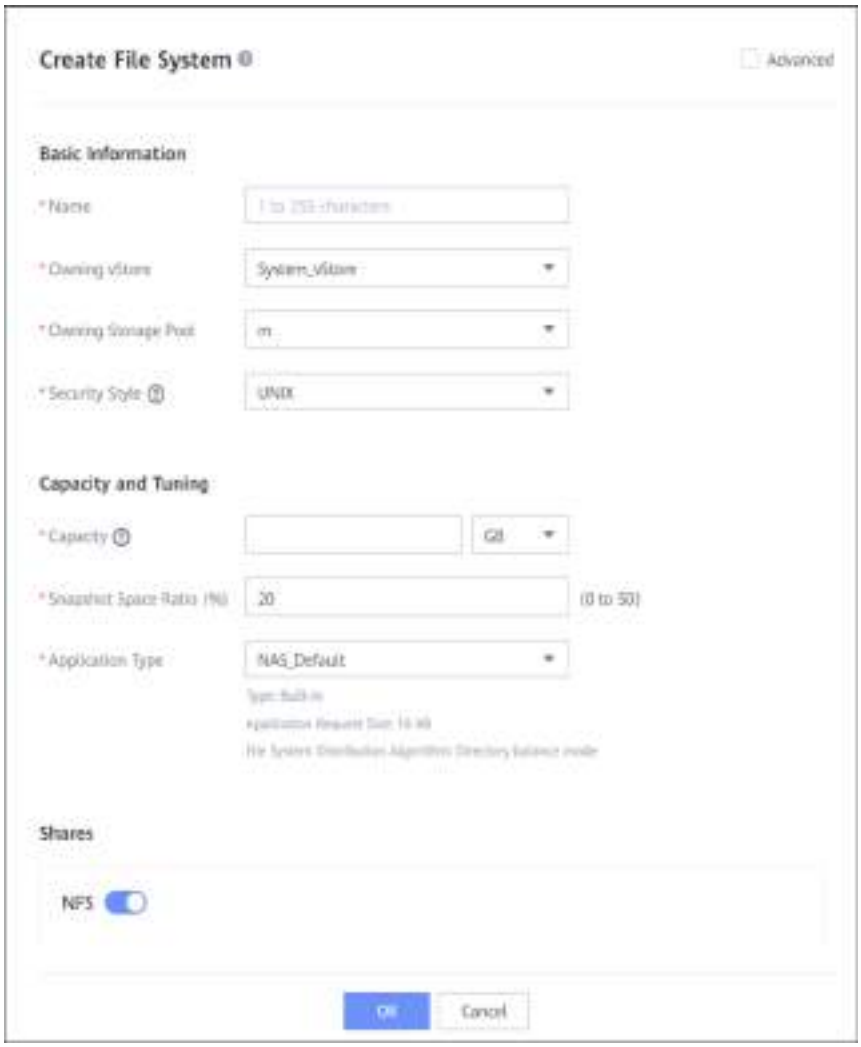
Procedure

Step 1 Choose **Services** > **File Service** > **File Systems**.

Step 2 In the **vStore** drop-down list in the upper left corner, select the vStore for which you want to create a file system.

Step 3 Click **Create**.

The **Create File System** page is displayed on the right.



NOTE

The screenshot is for reference only and the actual displayed information may vary.

For some device models, you can click in the upper right corner of the page to enable SmartGUI. SmartGUI mines users' historical operation data and builds a configuration parameter recommendation model based on user profiles to recommend configuration parameters for the block service and file service. After SmartGUI is enabled, the system presets parameters based on recommendations when you create a file system. You can click **Modify** in the upper right corner to modify the parameters or directly click **OK** to create a file system.

Step 4 Set the basic information about the file system.

Table 3-2 describes the parameters.

Table 3-2 File system parameters

Parameter	Description
Name	Name of the file system. [Value range] • The name must be unique. • The name can contain only letters, digits, periods (.), underscores (_), hyphens (-), and characters of different languages. • The name contains 1 to 255 characters.
Owning vStore	vStore to which the file system belongs. **NOTE** This parameter is mandatory when **vStore** is set to **All vStores** in **Step 2**.
Description	Description of the file system. **NOTE** **Description** is hidden. To display hidden parameters, click **Advanced**. [Value range] The description can be left blank or contain up to 255 characters.
Owning Storage Pool	Owning storage pool of the file system.

Parameter	Description
Security Style	Select a security style based on service requirements. It is used to set the access control style of a file system in multi-protocol mode. • **Mixed** Allows users of both CIFS and NFS clients to access and control file systems. The last configured permissions prevail. **NOTE** – If **Mixed** is selected, you are advised to enable user mapping and set **Mapping Mode** to **Support only user mapping of this system** in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameter**. – You are advised to configure a default UNIX user for the CIFS service in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameters**. The UNIX user must be an existing local authentication user, NIS domain user, or LDAP domain user. – You are advised to configure a default Windows user for the NFS service in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameters**. The Windows user must be an existing local authentication user or AD domain user. – Only 6.1.5 and later versions support the **Mixed** security style. • **Native** Controls CIFS users' permissions with Windows NT ACLs and NFS users' permissions with UNIX permissions (UNIX mode bits, POSIX ACLs, and NFSv4 ACLs). Windows NT ACLs and UNIX permissions will neither affect nor synchronize with each other. – For CIFS share access, Windows NT ACLs determine whether Windows users have access permission. **NOTE** If Windows NT ACLs do not exist, UNIX mode bits determine whether Windows users have access permission. – For NFS share access, access permission of UNIX users is determined by UNIX permissions.

Parameter	Description
	NOTE – If **Native** is selected, you are advised to enable user mapping and set **Mapping Mode** to **Support only user mapping of this system** in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameter**. – You are advised to configure a default UNIX user for the CIFS service in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameters**. The UNIX user must be an existing local authentication user, NIS domain user, or LDAP domain user. – You are advised to configure a default Windows user for the NFS service in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameters**. The Windows user must be an existing local authentication user or AD domain user. – Only 6.1.5 and later versions support the **Native** security style. ● NTFS Controls CIFS users' permissions with Windows NT ACLs. **NOTE** – If **NTFS** is selected, you are advised to enable user mapping and set **Mapping Mode** to **Support only user mapping of this system** in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameter**. – In addition, you are advised to configure a default Windows user for the NFS service in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameter**. The default Windows user must be an existing local authentication user or AD domain user. ● **UNIX** Controls NFS users' permissions with UNIX mode bits or NFSv4 ACLs. **NOTE** – If **UNIX** is selected, you are advised to enable user mapping and set **Mapping Mode** to **Support only user mapping of this system** in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameter**. – In addition, you are advised to configure a default UNIX user for the CIFS service in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameter**. The UNIX user must be an existing local authentication user, NIS domain user, or LDAP domain user. – In this mode, the default UNIX permission of the file system root directory is **755**. To change the value, run the **change file_system general file_system_id=? unix_permissions=?** command. For details on this command, refer to the *Command Reference*.

Parameter	Description
NAS Lock Policy	**NAS Lock Policy** includes **Mandatory Lock** and **Advisory Lock**. • **Mandatory Lock** is recommended if clients using different protocols simultaneously access the same file or directory. • **Advisory Lock** is recommended if high read and write performance is required and clients using different protocols do not access the same file or directory simultaneously. **NOTE** – This parameter is available only when **Security Style** is set to **Native**. – Only 6.1.5 and later versions support this parameter.
VAAI	Indicates whether to enable VAAI. VMware Storage APIs for Array Integration (VAAI) are a set of APIs that allow ESXi hosts to offload specific file operations to the storage array. This enables vSphere to quickly implement key operations and reduces the usage of the host CPU, memory, and storage bandwidth for higher efficiency and lower O&M costs. • Enabled: The host offloads file operations to the storage array. Once it is enabled, it cannot be disabled. • Disabled: VAAI is not used. **NOTE** – Only 6.1.5 and later versions support this parameter.

Step 5 Set the capacity and tuning information of the file system.

Table 3-3 describes the parameters.

Table 3-3 Capacity and tuning parameters

Parameter	Description
Capacity	Capacity of the file system, which indicates the maximum capacity allocated to the thin file system. That is, the total capacity dynamically allocated to the thin file system cannot exceed this value. **NOTE** • The maximum capacity of the file system cannot exceed the system specifications. For details about the specifications, see the **Specifications Query** tool. • The storage system uses the following capacity algorithms defined by Windows: 1 PB = 1,024 TB, 1 TB = 1,024 GB, 1 GB = 1,024 MB, 1 MB = 1,024 KB, and 1 KB = 1,024 bytes.

Parameter	Description
Capacity Alarm Threshold (%)	Alarm threshold of the file system capacity. An alarm will be generated when the threshold is reached. **NOTE** • **Capacity Alarm Threshold (%)** is hidden. To display hidden parameters, select **Advanced**. • Capacity threshold = File system capacity x (1 - Reserved snapshot space ratio (%)) x Capacity alarm threshold (%) • The alarm is cleared only when the used capacity of the file system is smaller than Max {90% of the threshold capacity, threshold capacity - 1 GB}.
Reserved Snapshot Space Ratio (%)	Percentage of the file system snapshot space to the file system capacity. **NOTE** • The file system space must not occupy the space reserved for snapshots. For example, if the capacity of a file system is 100 GB and the reserved snapshot space ratio is 20%, the used capacity of the file system cannot exceed 80 GB. • Snapshots can be created when the file system space is full but the space reserved for snapshots is not full. • Only 6.1.5 and later versions support this parameter.
Delete Obsolete Read-Only Snapshot	Indicates whether to delete obsolete read-only snapshots. If used space of the file system reaches the capacity alarm threshold and used space of snapshots is larger than space reserved for snapshots (source file system capacity x reserved snapshot space ratio), the system automatically deletes the oldest non-secure read-only snapshots. **NOTE** • **Delete Obsolete Read-Only Snapshot** is a hidden parameter. To display hidden parameters, click **Advanced**. • If both **Delete Obsolete Read-Only Snapshot** and **Capacity Auto-negotiation Policy** are enabled, the capacity auto-negotiation policy is executed first. • Only 6.1.5 and later versions support this parameter.

Parameter	Description
Capacity Auto-negotiation Policy	The available capacity auto-negotiation policies are as follows: • **Not used**: The storage capacity used by a file system is fixed and is not flexibly adjusted by the storage system. • **Auto expansion**: The file system capacity is automatically increased to meet user needs for more data writes, when the available space of a file system is about to run out and the storage pool has available space. • **Auto expansion/reduction**: The storage system automatically adjusts the file system capacity based on file system space usage. When the available space of a file system is about to run out and the storage pool has available space, automatic capacity expansion will be used to increase file system capacity. When the file system's storage space is released, it can be reclaimed into a storage pool and used by other file systems in data write requests. **NOTE** • **Capacity Auto-negotiation Policy** is a hidden parameter. To display hidden parameters, click **Advanced**. • If both **Delete Obsolete Read-Only Snapshot** and **Capacity Auto-negotiation Policy** are enabled, the capacity auto-negotiation policy is executed first. • Only 6.1.5 and later versions support this parameter.
Auto Expansion Trigger Threshold (%)	When the ratio of the used capacity to the total capacity of a file system is greater than this threshold, the storage system automatically triggers file system capacity expansion. **NOTE** • This parameter is displayed only when **Capacity Auto-negotiation Policy** is set to **Auto expansion** or **Auto expansion/reduction**. • The value of **Auto Expansion Trigger Threshold (%)** must be greater than that of **Auto Reduction Trigger Threshold (%)**. • Only 6.1.5 and later versions support this parameter.
Auto Reduction Trigger Threshold (%)	When the ratio of the used capacity to the total capacity of a file system is smaller than this threshold, the storage system automatically triggers space reclamation to reduce the file system capacity. **NOTE** • This parameter is displayed only when **Capacity Auto-negotiation Policy** is set to **Auto expansion/reduction**. • Only 6.1.5 and later versions support this parameter.

Parameter	Description
Auto Expansion Upper Limit	Upper limit of automatic capacity expansion. **NOTE** • This parameter is displayed only when **Capacity Auto-negotiation Policy** is set to **Auto expansion** or **Auto expansion/reduction**. • Only 6.1.5 and later versions support this parameter.
Auto Reduction Lower Limit	Lower limit of automatic capacity reduction. **NOTE** • This parameter is displayed only when **Capacity Auto-negotiation Policy** is set to **Auto expansion/reduction**. • Only 6.1.5 and later versions support this parameter.
Application Type	Application type of the file system. Preset application types are provided for typical applications. In file service scenarios, possible options are **NAS_Default**, **NAS_Virtual_Machine**, **NAS_Database**, **NAS_Large_File**, **Office_Automation**, and **NAS_EDA**. **NOTE** • The **Application Request Size** and **File System Distribution Algorithm** parameters are set for preset application types. The value of **Application Request Size** is **16 KB** for **NAS_Default**, **NAS_Virtual_Machine**, **Office_Automation**, and **NAS_EDA**, **8 KB** for **NAS_Database**, and **32 KB** for **NAS_Large_File**. If **Application Type** is set to **NAS_Default**, **NAS_Large_File**, **Office_Automation**, or **NAS_EDA**, **File System Distribution Algorithm** is **Directory balance mode**. In this mode, directories are evenly allocated to each controller by quantity. If **Application Type** is set to **NAS_Virtual_Machine** or **NAS_Database**, **File System Distribution Algorithm** is **Performance mode**. In this mode, directories are preferentially allocated to the controller to which the shared IP address belongs, improving access performance of directories and files. • **Application Type** cannot be changed once being configured. You are advised to set the value based on the service I/O model. • To create an application type, run the **create workload_type general name=? io_size=?** command. For details, see the *Command Reference* of the desired model and version. • You can also run the **create file_system general** or **change file_system general** command to create or modify a file system respectively. For details, see the *Command Reference* of the desired model and version.

Step 6 If a HyperMetro vStore pair has been created for the selected vStore, you need to configure HyperMetro for the newly created file system.

Specify **Remote Storage Pool** for creating a remote file system. The system will create a remote file system on the remote device of the HyperMetro vStore pair and add the local and remote file systems to a HyperMetro pair.

For details about HyperMetro, see the *HyperMetro Feature Guide for File* of the desired version.

Step 7 Configure shares for the file system.

- Set NFS shares for the file system.
  a. Enable **NFS**.
  b. Set **Create From**. Possible values are **Template** or **New**.
     - **Template**

       Select a share template from the drop-down list box. The system presets the description and permission of the created share based on the selected template. You can click **Modify** on the right of **Share** to modify the share information.
     - **New**

       The read/write permission of all clients is preset in the system, and the default root permission of clients is **root_squash**. You can click **Modify** on the right of **Share** to modify the share information.
- Set CIFS shares for the file system.
  a. Enable **CIFS**.
  b. Set **Create From**. Possible values are **Template** or **New**.
     - **Template**

       Select a share template from the drop-down list box. The system presets the description and permission of the created share based on the selected template. You can click **Modify** on the right of **Share** to modify the share information.
     - **New**

       The system presets the full control permission for everyone. You can click **Modify** on the right of **Share** to modify the share information.

Step 8 Set a quota for the file system.

NOTE

Quota is a hidden parameter. To display hidden parameters, click **Advanced**.

1. Enable **Quota**.

   NOTE

   - The quota switch is disabled by default.
   - When the **Quota** function is disabled, the system does not collect statistics on quota usage. In this case, hard and soft quotas do not take effect.
2. Click **Create**.

   The **Create Quota** page is displayed on the right.
3. Specify **Quota Type**. Possible options are **Directory quota**, **User quota**, and **User group quota**.
   - **Directory quota**

     The directory quota of a file system limits the space usage or file quantity used by all dtrees in the file system.

NOTE

The directory quota of a file system takes effect only for dtrees whose quota function is enabled. In addition, the quota of each dtree is limited separately.

- **User quota**

  User quota: limits the space usage or file quantity used by a single user.

  i. Click **Select**.

     The **Select User** page is displayed.

  ii. Select the users for which you want to create a quota.

     - If you select **All users**, the quota limits the space usage or file quantity of each user in the system.
     - If you select **Specified users**, click **Add**. On the **Add User** page that is displayed, select the **UNIX Users** or **Windows Users** tab, and select one or more desired users. Then click **OK**.

       NOTE

       If you set **User Type** to **Local authentication user**, select the desired users in the list below.

       If you set **User Type** to **LDAP domain user**, **NIS domain user**, or **AD domain user**, enter the user names in the **Name** text box.

       To remove added users, click **Remove** on the right of a desired user, or select one or more desired users and click **Remove**.

     - If you select **Specified user groups**, the quota limits the space usage or file quantity of each specified user group. To add a user group, click **Add**. On the **Add User Group** page that is displayed, select a user group type and select the desired user groups. Then click **OK**.

       NOTE

       If you set **User Group Type** to **Local authentication user group**, select the desired user groups in the list below.

       If you set **User Group Type** to **LDAP domain user group** or **NIS domain user group**, enter the user group names in the **Name** text box.

       To remove added user groups, click **Remove** on the right of a desired user group, or select one or more desired user groups and click **Remove**.

  iii. Click **OK**.

- **User group quota**

  User group quota: limits the space usage or file quantity used by a single user group.

  i. Click **Select**.

     The **Select User Group** page is displayed.

  ii. Select the user groups for which you want to create a quota.

     - If you select **All user groups**, the quota limits the space usage or file quantity of each user group in the system.
     - If you select **Specified user groups**, the quota limits the space usage or file quantity of each specified user group. To add a user

group, click **Add**. On the **Add User Group** page that is displayed, select a user group type and select the desired user groups. Then click **OK**.

NOTE

If you set **User Group Type** to **Local authentication user group**, select the desired user groups in the list below.

If you set **User Group Type** to **LDAP domain user group** or **NIS domain user group**, enter the user group names in the **Name** text box.

To remove added user groups, click **Remove** on the right of a desired user group, or select one or more desired user groups and click **Remove**.

iii. Click **OK**.

4. Set space quotas.

   Table 3-4 describes the parameters.

Table 3-4 Space quota parameters

Parameter	Description
Hard Quota	Space hard quota. If the quota is reached, the system immediately forbids writes. [Value range] 1 KB to 256 PB The value must be larger than that of **Soft Quota**.
Soft Quota	Space soft quota. If the quota is reached, the system generates an alarm but still allows writes. After the hard quota is reached, the system immediately forbids writes. [Value range] 1 KB to 256 PB The value must be smaller than that of **Hard Quota**.

5. Set file quantity quotas.

   Table 3-5 describes the parameters.

Table 3-5 File quantity quota parameters

Parameter	Description
Hard Quota	File quantity hard quota. If the quota is reached, new files cannot be added. Operations on existing files are not affected. [Value range] 1 to 2 billion The value must be larger than that of **Soft Quota**.

Parameter	Description
Soft Quota	File quantity soft quota. If the quota is reached, the system generates an alarm but new files can still be added. After the hard quota is reached, new files cannot be added. [Value range] 1 to 2 billion The value must be smaller than that of **Hard Quota**.

NOTE

- If you do not set the space quota or file quantity quota, the storage system only collects statistics on but does not control the space usage or file quantity. To view the statistics about used space quota and used file quantity quota, choose **Services** > **File Service** > **Quotas** > **Quota Reports**, and select the desired file system.
- To modify a quota, click **More** on the right of the quota and select **Modify**.
- To delete a quota, select the quota and click **Delete** above the list or click **More** on the right of the quota.
- The parameters for creating a quota are preset. A quota is created for a file system only after the file system has been created.

Step 9 Configure data protection for the file system.

1. Enable **Add to HyperCDP Schedule**.
2. Select a HyperCDP schedule to create a HyperCDP object for the file system.

NOTE

- HyperCDP is a high-density snapshot technology that provides continuous data protection for file systems. For details about the HyperCDP feature, see *HyperCDP Feature Guide for File* of the desired version.
- The system has a built-in HyperCDP schedule **NAS_DEFAULT_BUILDIN**. The schedule is executed once an hour (retains the latest three copies), once at 00:05 every day (retains the latest two copies), and once at 00:10 every Sunday (retains the latest two copies).
- When you create a file system, the system selects the built-in HyperCDP schedule **NAS_DEFAULT_BUILDIN** by default.
- A file system can be added to only one HyperCDP schedule. For a file system that has been added to a HyperCDP schedule, if you want to change its owning HyperCDP schedule, you need to remove the file system from the original HyperCDP schedule first.
- If a file system has not been added to a HyperCDP schedule during the file system creation, you can add it to a HyperCDP schedule after the file system is created.

Step 10 Select **Advanced** in the upper right corner and set the audit log items of the file system. The system records audit logs of operations on the file system. The audit log items include **Create**, **Delete**, **Read**, **Write**, **Open**, **Close**, **Rename**, **List folders**, **Obtain properties**, **Set properties**, **Obtain security properties**, **Set security properties**, **Obtain extension properties**, and **Set extension properties**.

NOTE

- To ensure that the selected audit log items take effect, choose **Settings** > **File Service** > **Audit Log** to enable the audit log function.
- If too many audit logs are generated and the audit log collection speed is lower than the audit log writing speed, the temporary buffer space may be insufficient, causing service interruption risks. You are advised to properly configure the items to be audited. For example, configure only **Create**, **Delete**, and **Write** for a file system.

Step 11 Set advanced attributes of the file system.

Table 3-6 describes the parameters.

Table 3-6 Advanced file system parameters

Parameter	Description
Snapshot Directory Visibility	Indicates whether to visualize the directory of the file system snapshots.
Auto Atime Update	Indicates whether to enable **Auto Atime Update**. Atime indicates the time when a namespace is accessed. After this function is enabled, the system updates the Atime based on the value of **Atime Update Frequency**. **NOTE** Enabling **Auto Atime Update** compromises the system performance.
Atime Update Frequency	Indicates the Atime update frequency. The options can be **Hourly** and **Daily**.

Step 12 Set the WORM (Write Once Read Many) properties of the file system. The WORM file system ensures that a file enters the protected state after being written. In this case, the file cannot be modified, moved, or deleted, but can be read for multiple times.

NOTE

Due to the sensitivity of a WORM file system to data security, the following configuration operations on file systems are restricted:

- Only read-only snapshots can be created for the WORM file system. The snapshot file systems created for the WORM file system also have the WORM feature. The WORM file system cannot be rolled back using a snapshot.
- When configuring the remote replication function, if **Pair Creation** is set to **Manual**, ensure that the WORM file system modes at both ends are the same. Otherwise, the primary/secondary relationship cannot be established.
- When configuring remote replication, if **Pair Creation** is set to **Automatic**, ensure that the global WORM regulatory clock has been initialized on the remote end.

Table 3-7 describes the parameters.

NOTE

The WORM properties are hidden. To display hidden parameters, click **Advanced**.

Table 3-7 WORM properties of a file system

Parameter	Description
Mode	Indicates the compliance mode of WORM protection. The **Mode** is **Regulatory compliance**: • Files within the protection period cannot be modified, renamed, or deleted by common users or system administrators. • Files whose protection period expires can be deleted but cannot be modified or renamed by common users or system administrators. • A file system that contains files within the protection period cannot be deleted by system administrators. • A file system that contains files whose protection period expires can be deleted by system administrators. [Value range] Regulatory compliance
Min. Protection Period	Minimum protection period supported by the WORM file system. The protection period of a file in the WORM file system cannot be smaller than the value of this parameter. [Value range] 0 to 70 years or **Indefinite**. **NOTE** The value of **Min. Protection Period** must be less than or equal to that of **Max. Protection Period**. [Default value] 3 years
Max. Protection Period	Maximum protection period supported by the WORM file system. The protection period of a file in the WORM file system cannot be longer than the value of this parameter. [Value range] 1 day to 70 years or **Indefinite**. **NOTE** The value of **Max. Protection Period** cannot be 0. [Default value] 70 years

Parameter	Description
Default Protection Period	Default protection period supported by the WORM file system. The protection period of a file in the WORM file system is the default value of the parameter if you do not set a protection period for the file. [Value range] • If the value of **Max. Protection Period** ranges from 1 day to 70 years, **Default Protection Period** is a value from **Min. Protection Period** to **Max. Protection Period**. • If **Max. Protection Period** is set to **Indefinite**, **Default Protection Period** is a value from **Min. Protection Period** to 70 years or is **Indefinite**. **NOTE** To set **Default Protection Period** to **Indefinite**, you must set **Max. Protection Period** to **Indefinite**. Otherwise, the setting fails. [Default value] 70 years
Automatic Lockout	After this function is enabled, a file automatically enters the locked state if not being modified within **Lockout Wait Time** (hours). The file in the locked state is protected. You can only read the file, but cannot modify, rename, or delete it. **NOTE** Modification operations include file data change and metadata change. [Default value] Disabled
Lockout Wait Time	Indicates the wait time before a file automatically enters the locked state. This parameter is displayed only when **Automatic Lockout** is enabled. [Value range] 1 minute to 10 years. [Default value] If **Automatic Lockout** is enabled, the default value is 2 hours.
Automatic Deletion	After this function is enabled, the system automatically deletes files whose protection periods have expired. **NOTE** Before enabling this function, ensure that files do not need protection and can be automatically deleted by the system after they expire. [Default value] Disabled

Parameter	Description
WORM Audit Log File System	After the WORM audit log file system is enabled, the system records operation logs of the WORM file system, including **Add a litigation** and **Remove a litigation**. [Default value] Disabled
Global WORM Regulatory Clock	Before creating a WORM file system for the first time, you need to initialize the WORM regulatory clock. After this parameter is enabled, the global security regulatory clock is initialized to the current system time and time zone. The WORM regulatory clock prevents modification to file protection periods caused by system time tampering attacks. The WORM regulatory clock includes a global WORM regulatory clock and a file system WORM regulatory clock. To initialize the WORM regulatory clock, you only need to initialize the global WORM regulatory clock. The file system WORM regulatory clock will be automatically initialized using the global WORM regulatory clock when a WORM file system is created. **NOTICE** • The global WORM regulatory clock cannot be modified after being initialized. Before the setting, ensure that the system time and time zone are correct. • Only super administrators can initialize the global WORM regulatory clock.

Step 13 Click **OK**.

Confirm your operation as prompted.

NOTE

After the task is created successfully, the **Execution Result** page is displayed. You can view details about the current task on this page.

----End

3.6 (Optional) Creating a Dtree

A dtree is a subdirectory of a file system. You can set quotas and shares for a dtree and manage file space usage and access permissions of the dtree.

Prerequisites

You have created a file system.

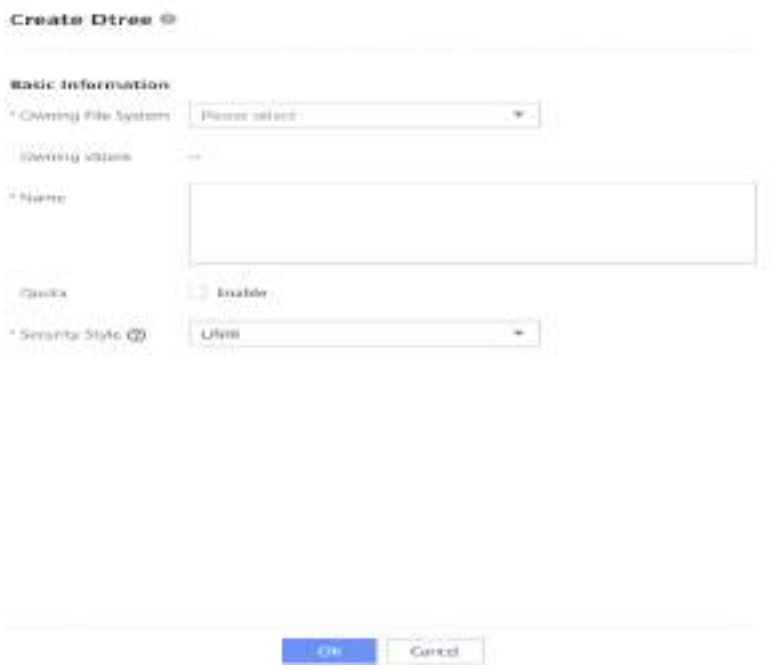
Procedure

Step 1 Choose **Services** > **File Service** > **Dtrees**.

Step 2 Select a vStore to which the desired file system belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Click **Create**.

The **Create Dtree** page is displayed on the right.



NOTE

The screenshot is for reference only and the actual GUI may vary.

Step 4 Set dtree parameters.

Table 3-8 describes the parameters.

Table 3-8 Dtree parameters

Parameter	Description
Owning File System	File system to which a dtree belongs.

Parameter	Description
Name	Name of a dtree. [Value range] You can enter multiple dtree names separated by commas (,) or carriage returns. A dtree name: • The name must be unique. • The name can contain only letters, digits, characters of different languages, and special characters (!\"#&%$'()*+-.;<=>?@[]^_`{|}~ and spaces). • The name contains 1 to 255 characters. • The name cannot only contain one or two consecutive periods (**.** or **..**).
Quota	Determine whether to enable the quota function of a dtree based on service requirements. When the **Quota** function is disabled, the system does not collect statistics on quota usage. In this case, hard and soft quotas do not take effect.

Parameter	Description
Security Style	Select a security style based on service requirements. It is used to set the access control style of a dtree in multi-protocol mode. • Mixed Allows users of both CIFS and NFS clients to access and control dtrees. The last configured permissions prevail. **NOTE** – If **Mixed** is selected, you are advised to enable user mapping and set **Mapping Mode** to **Support only user mapping of this system** in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameter**. – You are advised to configure a default UNIX user for the CIFS service in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameters**. The UNIX user must be an existing local authentication user, NIS domain user, or LDAP domain user. – You are advised to configure a default Windows user for the NFS service in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameters**. The Windows user must be an existing local authentication user or AD domain user. – Only 6.1.5 and later versions support the **Mixed** security style. • Native Controls CIFS users' permissions with Windows NT ACLs and NFS users' permissions with UNIX permissions (UNIX mode bits, POSIX ACLs, and NFSv4 ACLs). Windows NT ACLs and UNIX permissions will neither affect nor synchronize with each other. – For CIFS share access, Windows NT ACLs determine whether Windows users have access permission. **NOTE** If Windows NT ACLs do not exist, UNIX mode bits determine whether Windows users have access permission. – For NFS share access, access permission of UNIX users is determined by UNIX permissions.

Parameter	Description
	NOTE – If **Native** is selected, you are advised to enable user mapping and set **Mapping Mode** to **Support only user mapping of this system** in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameter**. – You are advised to configure a default UNIX user for the CIFS service in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameters**. The UNIX user must be an existing local authentication user, NIS domain user, or LDAP domain user. – You are advised to configure a default Windows user for the NFS service in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameters**. The Windows user must be an existing local authentication user or AD domain user. – Only 6.1.5 and later versions support the **Native** security style. ● NTFS Controls CIFS users' permissions with Windows NT ACLs. **NOTE** – If **NTFS** is selected, you are advised to enable user mapping and set **Mapping Mode** to **Support only user mapping of this system** in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameter**. – In addition, you are advised to configure a default Windows user for the NFS service in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameter**. The default Windows user must be an existing local authentication user or AD domain user. ● UNIX Controls NFS users' permissions with UNIX mode bits or NFSv4 ACLs. **NOTE** – If **UNIX** is selected, you are advised to enable user mapping and set **Mapping Mode** to **Support only user mapping of this system** in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameter**. – In addition, you are advised to configure a default UNIX user for the CIFS service in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameter**. The UNIX user must be an existing local authentication user, NIS domain user, or LDAP domain user.

Parameter	Description
NAS Lock Policy	**NAS Lock Policy** includes **Mandatory Lock** and **Advisory Lock**. • **Mandatory Lock** is recommended if clients using different protocols simultaneously access the same file or directory. • **Advisory Lock** is recommended if high read and write performance is required and clients using different protocols do not access the same file or directory simultaneously. **NOTE** • This parameter is available only when **Security Style** is set to **Native**. • Only 6.1.5 and later versions support this parameter.

Step 5 Click **OK**.

----End

3.7 (Optional) Creating a Quota

This operation enables you to create a quota to control and collect statistics of the space usage or file quantity of one or all dtrees in a file system or of a single user or user group.

Prerequisites

- You have created a dtree in a file system.
- When creating a quota for a specified user or user group, the user or user group has been created.

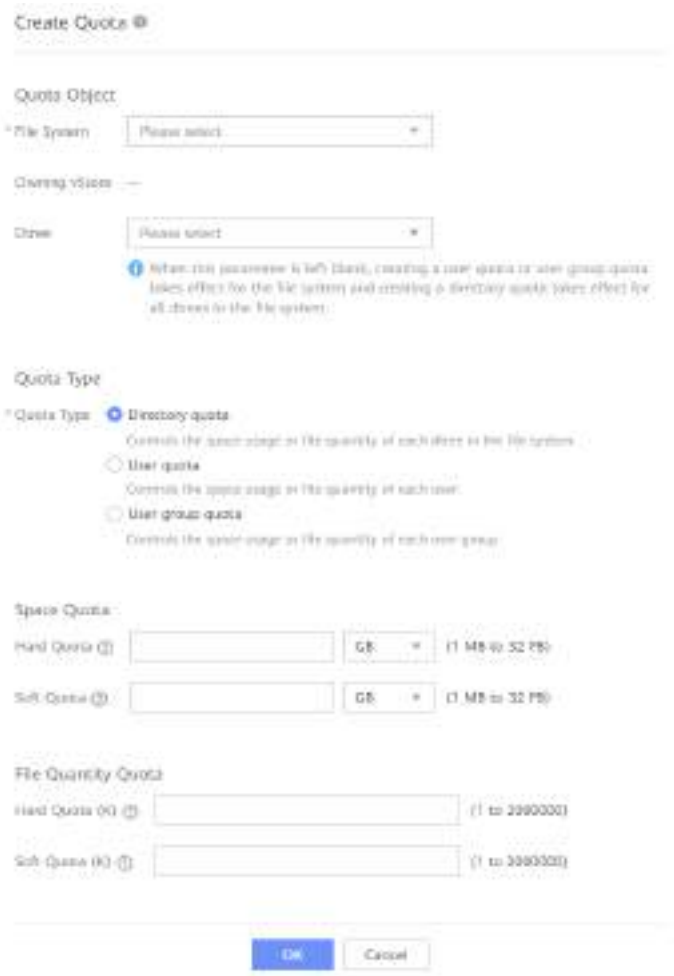
Procedure

Step 1 Choose **Services** > **File Service** > **Quotas** > **Custom Quotas**.

Step 2 Select the vStore to which the desired file system belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Click **Create**.

The **Create Quota** page is displayed on the right.



NOTE

The screenshot is for reference only and the actual displayed information may vary.

Step 4 Select the file system and dtree for which you want to create a quota.

NOTE

When the **Dtree** parameter is blank, the created user or user group quota takes effect for the file system and the directory quota takes effect for all dtrees in the file system.

Step 5 Select a quota type. Possible options are **Directory quota**, **User quota**, and **User group quota**.

- **Directory quota**
- **User quota**
  a. Click **Select**.
     The **Select User** page is displayed.
  b. Select the users for which you want to create a quota.
     - If you select **All users**, the quota controls the space usage or file quantity of each user in the system.
     - If you select **Specified users**, click **Add**. On the **Add User** page that is displayed, select the **UNIX Users** or **Windows Users** tab, and select one or more desired users. Then, click **OK**.

NOTE

- If you set **User Type** to **Local authentication user**, select the users to be added in the list below.
- If you set **User Type** to **LDAP domain user**, **NIS domain user**, or **AD domain user**, enter the user names in the **Name** text box.
- If you set **User Type** to **LDAP domain user**, the system automatically detects whether the LDAP domain has been configured. If no LDAP domain is configured, the system prompts you to configure an LDAP domain first.
- If you set **User Type** to **NIS domain user**, the system automatically detects whether the NIS domain has been configured. If no NIS domain is configured, the system prompts you to configure an NIS domain first.
- If you set **User Type** to **AD domain user**, the system automatically detects whether the AD domain has been configured. If no AD domain is configured, the system prompts you to configure an AD domain first.
- To remove added users, click **Remove** on the right of a desired user, or select one or more desired users and click **Remove**.

- If you select **Specified user groups**, the quota controls the space usage or file quantity of each user in specified user groups. Click **Add**. On the **Add User Group** page that is displayed, select a user group type and select the desired user groups. Then, click **OK**.

NOTE

- If you set **User Group Type** to **Local authentication user group**, select the user groups to be added in the list below.
- If you set **User Group Type** to **LDAP domain user group** or **NIS domain user group**, enter the user group names in the **Name** text box.
- If you set **User Group Type** to **LDAP domain user group**, the system automatically detects whether the LDAP domain has been configured. If no LDAP domain is configured, the system prompts you to configure an LDAP domain first.
- If you set **User Group Type** to **NIS domain user group**, the system automatically detects whether the NIS domain has been configured. If no NIS domain is configured, the system prompts you to configure an NIS domain first.
- To remove added user groups, click **Remove** on the right of a desired user group, or select one or more desired user groups and click **Remove**.

c. Click **OK**.

- **User group quota**

a. Click **Select**.

The **Select User Group** page is displayed.

b. Select the user groups for which you want to create a quota.

- If you select **All user groups**, the quota controls the space usage or file quantity of all user groups in the system.
- If you select **Specified user groups**, the quota controls the space usage or file quantity of each specified user group. Click **Add**. On the **Add User Group** page that is displayed, select a user group type and select the desired user groups. Then, click **OK**.

NOTE

- If you set **User Group Type** to **Local authentication user group**, select the user groups to be added in the list below.
- If you set **User Group Type** to **LDAP domain user group** or **NIS domain user group**, enter the user group names in the **Name** text box.
- If you set **User Group Type** to **LDAP domain user group**, the system automatically detects whether the LDAP domain has been configured. If no LDAP domain is configured, the system prompts you to configure an LDAP domain first.
- If you set **User Group Type** to **NIS domain user group**, the system automatically detects whether the NIS domain has been configured. If no NIS domain is configured, the system prompts you to configure an NIS domain first.
- To remove added user groups, click **Remove** on the right of a desired user group, or select one or more desired user groups and click **Remove**.

c. Click **OK**.

Step 6 Set space quotas.

Table 3-9 describes the parameters.

Table 3-9 Space quota parameters

Parameter	Description
Hard Quota	Space hard quota. If the quota is reached, the system immediately forbids writes. [Value range] 1 KB to 256 PB The value must be larger than that of **Soft Quota**.
Soft Quota	Space soft quota. If the quota is reached, the system generates an alarm but still allows writes. After the hard quota is reached, the system immediately forbids writes. [Value range] 1 KB to 256 PB The value must be smaller than that of **Hard Quota**.

NOTE

When the used capacity exceeds the soft quota or hard quota, the system generates an alarm. The alarm is cleared only when the used capacity is smaller than 90% of the soft quota or hard quota.

Step 7 Set file quantity quotas.

Table 3-10 describes the parameters.

Table 3-10 File quantity quota parameters

Parameter	Description
Hard Quota	File quantity hard quota. If the quota is reached, new files cannot be added. However, operations on existing files are not affected. [Value range] 1 to 2 billion The value must be larger than that of **Soft Quota**.
Soft Quota	File quantity soft quota. If the quota is reached, the system generates an alarm but new files can still be added. After the hard quota is reached, new files cannot be added. [Value range] 1 to 2 billion The value must be smaller than that of **Hard Quota**.

NOTE

If you do not set the space quota or file quantity quota, the storage system only collects statistics on but does not control the space usage or file quantity. To view the statistics about used space quota and used file quantity quota, choose **Services** > **File Service** > **Quotas** > **Quota Reports**, and select the desired file system.

Step 8 Click **OK**.

----End

3.8 Sharing File Systems

File systems can be accessed only after being shared. This section describes how to share file systems using different protocols.

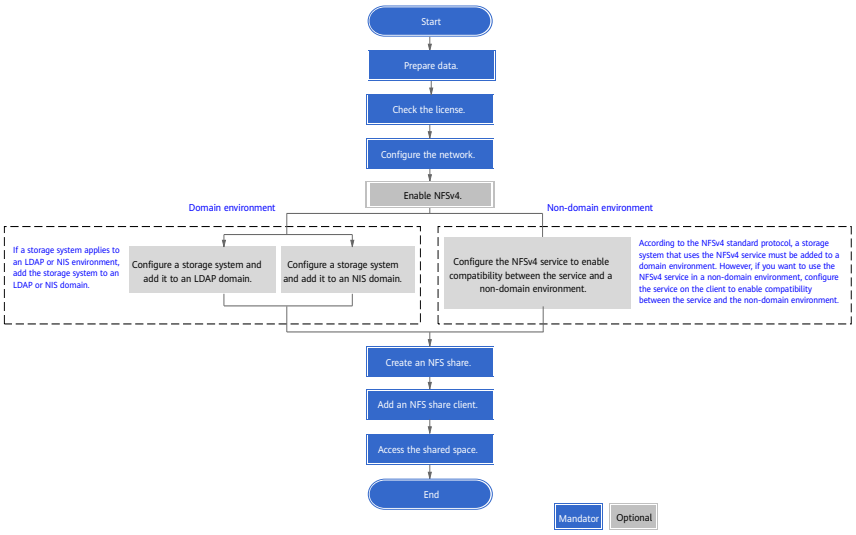
3.8.1 Configuring an NFS Share

This section describes how to configure an NFS share.

3.8.1.1 Configuration Process

Figure 3-2 shows the NFS share configuration process.

Figure 3-2 NFS share configuration process



3.8.1.2 Preparing Data

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

You need to prepare the following data:

- Logical IP address

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

  File system shared through the NFS share.
- LDAP or NIS domain information
- Permission

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

NOTE

You can contact your network administrator to obtain desired data.

3.8.1.3 Checking the License

Before configuring NFS, ensure that the license grants the use of NAS Foundation.

Procedure

Step 1 Choose **Settings** > **License Management**.

Step 2 In the middle function pane, verify that **NAS Foundation** is displayed in the feature list.

NOTE

- If no license file has been imported, import a license file by referring to the initialization guide.
- If **NAS Foundation** is not displayed in the feature list, contact technical support engineers.

----End

3.8.1.4 Configuring the Network

Before configuring shared services, plan and configure the network properly for accessing and managing file services.

3.8.1.4.1 (Optional) Creating a Bond Port

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

Prerequisites

The IP addresses of the Ethernet ports you want to bond have been cleared. Ethernet ports that have IP addresses cannot be bonded.

Context

Port bonding provides more bandwidth and higher redundancy for links. Although ports are bonded, each session still transmits data through a single port and the total bandwidth can be increased only when there are multiple sessions. Determine whether to bond ports based on site requirements.

Port bonding on the storage system has the following restrictions:

- Only Ethernet ports that have the same rate and are on the same controller can be bonded. Ports cannot be bonded across controllers. Non-Ethernet ports cannot be bonded.
- Link aggregation (IEEE 802.3ad) is supported.
- For OceanStor 5310, OceanStor 5510 and OceanStor 5610:
  - GE interface modules (not supporting TOE) support port bonding across modules by default.
  - 10GE, 25GE, 40GE, and 100GE interface modules (supporting TOE) do not support port bonding across modules by default. They support port bonding across modules after TOE is disabled.

    NOTICE

    To disable the TOE function of a port, contact Huawei technical support.

  - The onboard network ports of OceanStor 5310 can be bonded across interface modules and the port rates must be the same.
- For OceanStor 6810, OceanStor 18510, and OceanStor 18810, interface modules in the same quadrant can be bonded across interface modules, and the TOE function of the ports to be bonded must be disabled.

NOTICE

To disable the TOE function of a port, contact Huawei technical support.

For OceanStor 6810, OceanStor 18510, and OceanStor 18810, each interface module can use only one bonding mode. That is, an interface module does not allow bonding across modules and bonding within the module at the same time.

- Read-only users are not allowed to bond Ethernet ports.
- Each Ethernet port can be added to only one bond port.
- A member port of a port group cannot be added to a bond port.
- Management network ports cannot be bonded.
- Member ports in the same bond port cannot connect to different switch networks.
- After Ethernet ports are bonded, their MTU changes to the default value and you need to configure the switch port mode. Take Huawei switches as an example. You must set the ports on the Huawei switches to work in static LACP mode.

NOTICE

The link aggregation modes vary with switch manufacturers. If a switch from another vendor is used, contact technical support of the switch manufacturer for specific link aggregation configurations.

Port bonding on the host has the following restriction:

If the TOE function is enabled on the storage system and the host port connecting to the switch must be bonded, the bonding mode must be set to 4.

NOTE

If the preceding restriction cannot be met, disable the TOE function of the port.

Procedure

Step 1 Choose **Services** > **Network** > **Ethernet Network** > **Bond Ports**.

Step 2 Click **Create**.

The **Create Bond Port** page is displayed on the right.

Step 3 Set a bond name and select ports you want to bond.

1. Specify a name for the bond port in **Name**.

   NOTE

   The name must meet the following requirements:

   - The value can contain only letters, digits, underscores (_), hyphens (-), and periods (.).
   - The name contains 1 to 31 characters.

2. Select the controller where the bond port resides.
3. In **Available Ports**, select one or more ports you want to bond.

Step 4 Click **OK**.

Confirm your operation as prompted.

----End

3.8.1.4.2 (Optional) Creating a VLAN

This section describes how to create VLANs for Ethernet ports or bond ports.

Prerequisites

VLANs cannot be created on the Ethernet ports that are configured with IP addresses or used for networking.

Procedure

Step 1 Choose **Services** > **Network** > **Ethernet Network** > **VLANs**.

Step 2 Click **Create**.

The **Create VLAN** page is displayed on the right.

Step 3 In the **Port Type** drop-down list, select the type of the ports used to create VLANs.

Possible values are **Ethernet Port** and **Bond Port**.

Step 4 In the **Home Port** list, select a home port.

Step 5 In **ID**, specify the ID of a VLAN, and then click **Add**.

NOTE

- The VLAN ID ranges from 1 to 4094. You can specify multiple VLAN IDs one by one or in a batch. When creating multiple VLANs and specifying VLAN IDs in a batch, the VLAN IDs are in the following format: Start VLAN ID-End VLAN ID.
- To delete a VLAN ID, click × next to it.

Step 6 Click **OK**.

----End

Follow-up Procedure

When creating a logical port based on a VLAN, ensure that the port type is VLAN and the home port is the VLAN's home port.

3.8.1.4.3 (Optional) Creating a DNS Zone

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

Context

It is recommended that a DNS zone be associated with only logical ports with the same IP address type (IPv4 or IPv6).

If the host interface card supports both IPv4 and IPv6 protocols, the DNS client initiates IPv4 and IPv6 resolution requests. If the storage system is associated with both IPv4 and IPv6 logical ports in the same DNS zone and the host interface card is configured with only IPv4 addresses, the host may fail to access the domain name.

Procedure

Step 1 Choose **Services** > **vStore Service** > **vStores**.

Step 2 Click the name of the desired vStore. On the details page that is displayed on the right, click the **File Service** tab and click **Configure** in the **DNS Zone** area.

The **Configure DNS Zone** page is displayed on the right.

Step 3 Configure a DNS zone.

- Add a DNS zone.
  a. Click **Add**.
  b. In **Name**, enter the name of the DNS zone to be added.

     NOTE

     The name complexity requirements are as follows:

     - A name contains 1 to 255 characters and consists of multiple labels separated by periods (.).
     - A label contains 1 to 63 characters including letters, digits, hyphens (-), and underscores (_), and must start and end with a letter or a digit.
     - A name must be unique.

  c. If a HyperMetro vStore pair has been created for the vStore and **Working Mode** of the selected HyperMetro domain is **Active-active mode**, you need to set the owning site of the DNS zone. In normal cases, the host can access the logical port that belongs to the local site through the domain name of the local site. DNS zones with owning sites are mainly used when the active-active sites are far away from each other. In this case, hosts can access the nearest site to ensure access performance.
- Modify a DNS zone.

  In **Name**, modify the name of the desired DNS zone.

  NOTE

  The name complexity requirements are as follows:

  – A name contains 1 to 255 characters and consists of multiple labels separated by periods (.).
  – A label contains 1 to 63 characters including letters, digits, hyphens (-), and underscores (_), and must start and end with a letter or a digit.
  – A name must be unique.

- Remove a DNS zone.

  In the row that contains the desired DNS zone, click **Remove**.

Step 4 Click **Save**.

----End

3.8.1.4.4 Creating a Logical Port

This section describes how to create and manage logical ports that are used to access file services. A logical port is created based on an Ethernet port, a bond port, or a VLAN.

Context

When configuring an NFS share, set **Role** to **Service** for the logical port, and set **Data Protocol** to **NFS** or **NFS + CIFS** for the logical port.

Precautions

- It is recommended that you create no more than 64 logical ports for each controller. If more than 64 logical ports are created for one controller, the logical ports will fail over to a few available physical ports in the event that a large number of physical ports fail, decreasing service performance.
- In the case of file access across network segments, if a Remote Authentication Dial-In User Service (RADIUS) server is used for network device authentication in the data center and IP address failover occurs on a logical port, the IP address of the logical port will be re-registered on the RADIUS server. In this process, the IP address is not available. File services will be restored after the IP address becomes available.

Procedure

Step 1 Choose **Services** > **Network** > **Logical Ports**.

Step 2 Click **Create**.

The **Create Logical Port** page is displayed on the right.

Step 3 Set the parameters listed in **Table 3-11**.

Table 3-11 Logical port parameters

Parameter	Description
Name	Name of the logical port. The name must meet the following requirements: • The name must be unique. • The name can contain only letters, digits, underscores (_), hyphens (-), and periods (.). • The name contains 1 to 255 characters.

Parameter	Description
Role	Role of the logical port. Possible values are: **Management**: A port of this role is used by a vStore administrator to log in to the system for management. **Service**: A port of this role is used to access services, such as accessing CIFS shares of file systems. **Management + service**: A port of this role is used to access services or for a vStore administrator to log in to the storage system for system management. **Replication**: A port of this role is used for replication link connection in remote replication or HyperMetro, or for quorum link connection in HyperMetro.
Data Protocol	Data protocol of a logical port. Possible values are **NFS**, **CIFS**, **NFS + CIFS**, **iSCSI**, and **NVMe over RoCE**. **NOTE** • **NFS**, **CIFS**, and **NFS + CIFS** are applicable to file service configuration. **iSCSI** and **NVMe over RoCE** are applicable to block service configuration. • This parameter is displayed only when **Role** is set to **Service** or **Management + service**.
Owning vStore	vStore to which the logical port belongs. **NOTE** This parameter is displayed only when **Role** is set to **Service**, **Management**, or **Management + service**.
Owning Site	Site to which a logical port belongs. If a HyperMetro vStore pair has been created for the owning vStore, the configuration information of the front-end service logical port at the local site is automatically synchronized to the remote site, and the logical port at the owning site processes service access. The logical port is in connected state at the owning site and is in to-be-working state at the non-owning site. After the logical port creation is complete, its owning site cannot be modified. If a fault occurs for the port, the logical port at the non-owning site is used to process service access. **NOTE** This parameter is displayed only when a HyperMetro vStore pair has been created for the owning vStore and **Working Mode** of the HyperMetro domain of the HyperMetro vStore pair is **Active-active mode**.
IP Address Type	IP address type of the logical port, which can be **IPv4** or **IPv6**.
IP Address	IPv4 or IPv6 address of the logical port.
Subnet Mask	Subnet mask of the logical port's IPv4 address. **NOTE** This parameter is available only when **IP Address Type** is set to **IPv4**.

Parameter	Description
Prefix	Prefix length of the logical port's IPv6 address. **NOTE** This parameter is available only when **IP Address Type** is set to **IPv6**.
Gateway	Gateway of a logical port's IP address.
Port Type	Type of the port to which the logical port belongs. Possible values are **Ethernet port**, **Bond port**, **VLAN**, and **RoCE port**. **NOTE** • When **Data Protocol** is **NFS**, **CIFS**, **NFS + CIFS**, or **iSCSI**, you can select an Ethernet port, bond port, or VLAN. • When **Data Protocol** is **NVMe over RoCE**, you can select a VLAN or RoCE port. • Only 6.1.5 and later versions support RoCE ports.
Home Port	Ethernet port, bond port, VLAN, or RoCE port to which the logical port belongs. **NOTE** If **Port Type** is **RoCE port**, the system displays only the RoCE ports with a trust mode of DSCP.
Activation Status	Determine whether to activate the logical port. **NOTE** This parameter is available only when **Data Protocol** is set to **NFS**, **CIFS**, or **NFS + CIFS**.

Step 4 When **Role** is set to **Management**, **Service**, or **Management + service**, select **Advanced** in the upper right corner and set the advanced attributes of the logical port.

NOTE

If **Role** is set to **Service**, you can set advanced attributes only when **Data Protocol** is set to **NFS**, **CIFS**, or **NFS + CIFS**.

Table 3-12 describes the parameters.

Table 3-12 Advanced logical port parameters

Parameter	Description
Failover Group	Name of a failover group. **NOTE** • This parameter is available only when **Data Protocol** is set to **NFS**, **CIFS**, or **NFS + CIFS**. • If a failover group is specified, services on the failed home port will be taken over by an available port in the specified failover group. • If no failover group is specified, services on the failed home port will be taken over by an available port in the default failover group. • It is recommended that the logical ports of the same vStore use the same failover group. This ensures that the fault domains of the logical ports are the same.
IP Address Failover	After IP address failover is enabled, services on the failed home port will be taken over by other available ports in the failover group. In the entire process, the IP address used by services remains unchanged. **NOTE** • This parameter is available only when **Data Protocol** is set to **NFS**, **CIFS**, or **NFS + CIFS**. • Shares of file systems do not support the multipathing mode. They use IP address failover to improve the reliability of links.
Failback Mode	After the fault of the home port is rectified, services fail back to the home port. Possible values are **Automatic** and **Manual**. **NOTE** • This parameter is available only when **Data Protocol** is set to **NFS**, **CIFS**, or **NFS + CIFS**. • If **Failback Mode** is **Manual**, ensure that the link to the home port is normal before the failback. You can manually switch services back to the home port only when the link to the home port keeps normal for over five minutes. • If **Failback Mode** is **Automatic**, ensure that the link to the home port is normal before the failback. Services will automatically fail back to the home port only when the link to the home port keeps normal for over five minutes.
Listen for DNS Query	With this function enabled, external NEs can access the DNS service provided by the storage system by using the IP address of this logical port. **NOTE** This parameter is available only when **Data Protocol** is set to **NFS**, **CIFS**, or **NFS + CIFS**.

Parameter	Description
DNS Zone	Name of a DNS zone. **NOTE** • This parameter is available only when **Data Protocol** is set to **NFS**, **CIFS**, or **NFS + CIFS**. • If the value is blank, the logical port is not used for DNS-based load balancing. • One logical port can be associated with only one DNS zone. One DNS zone can be associated with multiple logical ports. • It is recommended that **Listen for DNS Query** be enabled for at least one logical port of each DNS zone. • It is recommended that a DNS zone be associated with only logical ports with the same IP address type (IPv4 or IPv6). If the host interface card supports both IPv4 and IPv6 protocols, the DNS client initiates IPv4 and IPv6 resolution requests. If the storage system is associated with both IPv4 and IPv6 logical ports in the same DNS zone and the host interface card is configured with only IPv4 addresses, the host may fail to access the domain name. • The load balancing effect varies with the distribution of logical ports associated with a DNS zone. To obtain a better load balancing effect, ensure that logical ports associated with a DNS zone are evenly distributed among controllers. • If a HyperMetro vStore pair has been created for the owning vStore, you can only select the DNS zones with the same owning site.

Step 5 Click **OK**.

----End

3.8.1.4.5 (Optional) Configuring DNS Load Balancing Parameters

The DNS load balancing feature can detect loads on various IP addresses on a storage system in real time and use a proper IP address as the DNS response to achieve load balancing among IP addresses.

Prerequisites

- If the storage system connects to an external DNS server, the external DNS server has been configured and is running properly.
- If the storage system directly connects to a host, DNS client configurations have been set on the host.
- Port 53 for the TCP/UDP protocol between the storage system and the DNS server or host is enabled.

Context

- DNS load balancing applies to scenarios where a large number of NAS service IP addresses or NAS clients are involved. If only a small number of (for example, less than 20) NAS service IP addresses or NAS clients are involved, you are advised to directly use service IP addresses to mount shares.

- Working principle:
  a. When a host accesses the NAS service of a storage system using a domain name, the host first sends a DNS request to the built-in DNS server and the DNS server obtains the IP address according to the domain name.
  b. If the domain name contains multiple IP addresses, the storage system selects the IP address with a light load as the DNS response based on the configured load balancing policy and returns the DNS response to the host.
  c. After receiving the DNS response, the host sends a service request to the target IP address.
- When DNS load balancing resolves a domain name, a specific domain name resolution record is added. The following records are supported:
  – A record: added if a domain name points to an IPv4 address (for example, 192.168.20.10).
  – AAAA record: added if a host name (or domain name) points to an IPv6 address (for example, ff03:0:0:0:0:0:0:c1).
  – PTR record: reverse of an A or AAAA record for implementing reverse DNS lookups.
- DNS load balancing supports only the UDP protocol for domain name resolution.

Procedure

Step 1 Choose **Settings** > **Basic Information** > **DNS Service**.

Step 2 Enable **File Service DNS Load Balancing**.

1. Set the DNS load balancing policy. The storage system supports the following load balancing policies:

   NOTE

   – **Weighted round robin** applies to scenarios where the load of storage devices is light or unknown, for example, in the scenario where shares are initially mounted to a large number of NAS clients.
   – Other policies apply to scenarios where users want to balance loads based on a certain indicator (such as CPU usage, port bandwidth, number of connections, and overall loads) of running services, for example, in the scenario where shares are mounted to NAS clients in batches during capacity expansion of client applications.

   – **Weighted round robin**: IP addresses which process loads and are under the same domain name are randomly selected for processing.
   – **CPU usage**: The CPU usage of each node determines the weight. The storage system uses the weight to select a node to process client services.
   – **Port bandwidth usage**: The total bandwidth usage of each node determines the weight. The storage system uses the weight to select a node to process client services.
   – **Connections**: The NAS connections of each node determine the weight. The storage system uses the weight to select a node to process client services.

- **Overall loads**: The overall load of CPU usage, bandwidth usage, and number of NAS connections determines node selection. Less loaded nodes are more likely to be selected.

2. Click **Save**.

----End

Follow-up Procedure

After associating logical ports with a DNS zone, configuring logical ports to listen to DNS requests, setting a DNS load balancing policy, and enabling DNS load balancing, you need to configure DNS server addresses on clients. For details about how to configure and use DNS load balancing, see **5.1 How Can I Configure and Use DNS Load Balancing?**

3.8.1.4.6 (Optional) Managing the Routes of a Logical Port

When configuring share access, ensure that the logical port can ping the IP addresses of the domain controller, DNS server, and clients. If the ping test fails, add routes from the IP address of the logical port to the network segment of the domain controller, DNS server, or clients.

Prerequisites

A logical port has been configured with an IP address.

Procedure

Step 1 Choose **Services** > **Network** > **Logical Ports**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Select the desired logical port and click **Manage Route**.

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

NOTE

Alternatively, perform either of the following operations to go to the **Manage Route** page:

- Click **More** on the right of the desired logical port and select **Manage Route**.
- Click the name of the desired logical port. In the upper right corner of the page that is displayed, click **Manage Route** from the **Operation** drop-down list.

Step 4 Configure the route information for the logical port.

1. In the **IP Address** drop-down list, select the IP address of the logical port for which you want to add a route.
2. Click **Add**.
3. Set the parameters listed in **Table 3-13**.

Table 3-13 Route parameters

Parameter	Description
Type	Three types of routes are available: – **Default route** A route through which data is forwarded by default if no preferred route is available. The destination address and mask (IPv4) or prefix (IPv6) of the default route are automatically set to 0. To use this option, you only need to add a gateway. – **Host route** A route to a host. The destination mask (IPv4) or prefix (IPv6) of the host route are automatically set to 255.255.255.255 or 128. To use this option, you only need to add the destination address and gateway. – **Network segment route** A route to a network segment. You must add the destination address, destination mask (IPv4) or prefix (IPv6), and gateway.
Destination Address	IPv4 address, IPv6 address, or network segment of the destination service network port on the application server or destination logical port on another storage system.
Subnet Mask/ Prefix	Subnet mask of the IPv4 address or prefix of the IPv6 address for the destination service network port on the application server or destination logical port on another storage system.
Gateway	Gateway where the local logical port's IP address resides. **NOTE** The IP address of the gateway must be different from all internal heartbeat IP addresses. Otherwise, routing will fail.

4. Click ✓. The route information is added to the list.

   NOTE

   Click 🗑 on the right of a desired route to delete it.

Step 5 Click **Close**.

----End

3.8.1.5 (Optional) Enabling the NFSv4 Service

The NFSv4.0 and NFSv4.1 services are disabled by default in the storage system. To use the NFSv4.0 or NFSv4.1 protocol for share access, you must enable the NFSv4 service first. If you use NFSv3 for share access, skip this section.

Context

- The storage system supports NFSv3, NFSv4.0, and NFSv4.1.

- The NFSv4.0 and NFSv4.1 services are disabled by default in the storage system.
- The NFSv4 service can be enabled on DeviceManager or on the CLI.

Enabling the NFSv4 Service on DeviceManager

Step 1 Choose **Settings** > **File Service** > **NFS Service**.

Step 2 In the **vStore** drop-down box in the upper left, select the vStore for which you want to enable the NFSv4 service.

Step 3 Click **Modify** in the upper right.

The page for configuring the NFS service is displayed.

NOTE

The screenshot is for reference only and the actual GUI may vary.

Step 4 Select **Enable** after **NFSv4.0 Service** or **NFSv4.1 Service** as required.

Step 5 In **Domain Name**, enter the storage domain name.

NOTE

- NFSv4.0 and NFSv4.1 use a user name + domain name mapping mechanism, enhancing the security of clients' access to shared resources.
- In a non-domain or LDAP environment, retain the default domain name **localdomain**.
- In an NIS environment, the entered information must be the same as the domain name in the **/etc/idmapd.conf** file on the Linux client that accesses the share. (You are advised to set both of them to the NIS domain name.)
- The domain name must contain 1 to 64 characters.
- Only 6.1.5 and later versions support domain name setting.

Step 6 Click **Save**.

A **Danger** dialog box is displayed.

NOTICE

If a host is accessing the shares of the storage system, enabling or disabling the NFS service may interrupt services. Exercise caution when performing this operation.

Step 7 Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation**.

Step 8 Click **OK**.

----End

Enabling the NFSv4 Service on the CLI

Step 1 Log in to the CLI of the storage system.

Step 2 **Optional:** To configure the NFSv4 service for a vStore, run the **change vstore view id=?** command to enter the vStore view.

You can run the **show vstore** command to query the value of **id**.

Step 3 Specify whether to enable the NFSv4.0 or NFSv4.1 service.

- To enable the NFSv4.0 service, run the **change service nfs_config nfsv40_status=enable** command.
- To enable the NFSv4.1 service, run the **change service nfs_config nfsv41_status=enable** command.

Step 4 Run the **show service nfs_config** command to check the running status of the NFSv4 service.

- The **Nfsv4.0 Service Status** field in the command output indicates the running status of the NFSv4.0 service of the current vStore.
- The **Nfsv41 Service Status** field in the command output indicates the running status of the NFSv4.1 service of the current vStore.

----End

3.8.1.6 (Optional) Adding the Storage System to an LDAP Domain

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

3.8.1.6.1 Preparing LDAP Domain Configuration Data

Before adding a storage system to an LDAP domain, collect the configuration data of an LDAP domain server.

LDAP Domain Parameters

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

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

The following figure shows the data structure of an LDAP server:

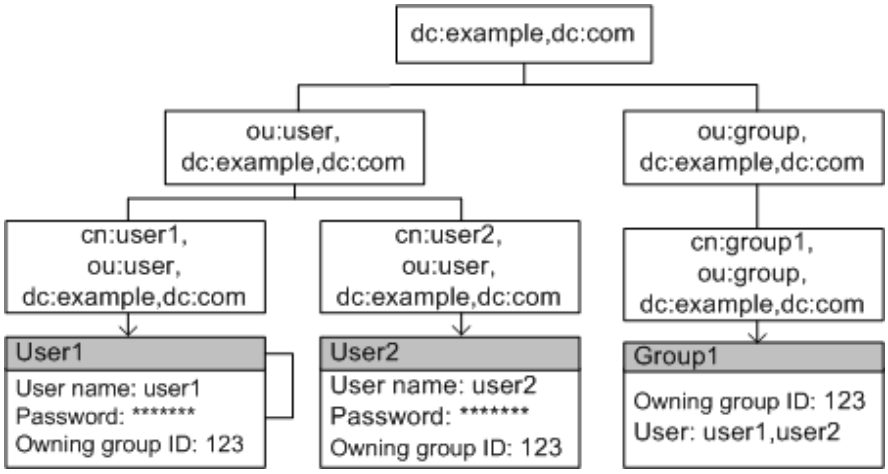


Table 3-14 defines LDAP entry acronyms.

Table 3-14 LDAP entry definitions

Acronym	Meaning
o	Organization
ou	Organization unit
c	Country name
dc	Domain component
sn	Surname
cn	Common name

What Is OpenLDAP?

OpenLDAP is an open implementation of LDAP that is now widely used in various popular Linux releases.

OpenLDAP consists of the following four components:

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

The OpenLDAP website does not provide OpenLDAP installation packages for Windows. You can obtain OpenLDAP installation packages for the following Windows operating systems from the Userbooster website: Windows XP, Windows Server 2003, Windows Server 2008, Windows Vista, Windows 7, Windows 8, and Windows Server 2012.

Obtaining LDAP Configuration Data in Windows

The following describes how to obtain LDAP configuration data in Windows using OpenLDAP as an example:

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

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

rootpw    XXXXXXXXXXXX
```

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

4. Find configuration files (**.ldif** files) of the users and user groups that need to access the storage system.

   NOTE

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

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

```
#root on the top
dn: dc=example,dc=com
dc: example
objectClass: domain
objectClass: top
#First organization unit name: user
dn: ou=user,dc=example,dc=com
ou: user
objectClass: organizationalUnit
objectClass: top
#Second organization unit name: groups
dn: ou=group,dc=example,dc=com
ou: group
objectClass: organizationalUnit
objectClass: top
#The first user represents user1 that belongs to organization unit user in the organizational structure topology.
dn: cn=user1,ou=user,dc=example,dc=com
cn: user1
objectClass: posixAccount
objectClass: shadowAccount
objectClass: inetOrgPerson
sn: user1
uid: user1
uidNumber: 2882
gidNumber: 888
homeDirectory: /export/home/ldapuser
loginShell: /bin/bash
userPassword: {ssha}eoWxtWNl8YbqsulnwFwKMw90Cx5BSU9DRA==xxxxxx
#The second user represents user2 that belongs to organization unit user in the organizational structure topology.
```



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

Obtaining LDAP Configuration Data in Linux

The following describes how to obtain LDAP configuration data in Linux using OpenLDAP as an example:

1. Log in to an LDAP server as user **root**.
2. Run the **cd /etc/openldap** command to go to the **/etc/openldap** directory.
   ```
   linux-ldap:~ # cd /etc/openldap
   linux-ldap:/etc/openldap #
   ```
3. Run the **ls** command to view the system configuration file **slapd.conf** and the configuration files (**.ldif** files) of the users and user groups who want to access the storage system.
   ```
   linux-ldap:/etc/openldap #ls
   example.ldif ldap.conf schema slap.conf slap.con slapd.conf
   ```
4. Run the **cat** command to open the system configuration file **slapd.conf** where you can view related parameters.
   ```
   linux-ldap:/etc/openldap #cat slapd.conf

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

   rootpw    XXXXXXXXXXXX
   ```
   - **dc=example,dc=com** corresponds to **Base DN**.
   - **cn=Manager,dc=example,dc=com** corresponds to **Bind DN**.
   - **XXXXXXXXXXXX** corresponds to **Bind Password**. If the password is in ciphertext, contact LDAP server administrators to obtain the password.
5. Run the **cat** command to open the **example.ldif** file. Find the DNs of a user and a user group that correspond to **User Directory** and **Group Directory** respectively on the storage system configuration page. For details about the parameters, see **5**.

3.8.1.6.2 Configuring LDAP Domain Authentication Parameters

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

Prerequisites

- An LDAP domain has been set up.
- Required data has been obtained.

  NOTE

  - The storage systems can connect to an LDAP server through management network ports or service network ports (logical ports). If a storage system connects to an LDAP server through management network ports, ensure that the management network ports on at least two controllers can properly communicate with the LDAP server. If a storage system connects to an LDAP server through service network ports, it is recommended that the service network ports on at least two controllers can properly communicate with the LDAP server. It is recommended that storage systems connect to LDAP servers through service network ports.
  - A storage system can connect to only one LDAP server.
  - An LDAP server with high performance is recommended. This prevents issues such as I/O latency increase when the storage system sends a large number of concurrent query requests to the LDAP server.

Precautions

- You are advised to use physical isolation and end-to-end encryption to ensure security of data transfer between the LDAP domain server and clients.
- You are advised to configure a static IP address for the LDAP server. If a dynamic IP address is configured, security risks may exist.
- In the following scenario (the three situations occurred in sequence), use **clear nfs nfsv4_idmap_cache controller=?** to clear the IDMAP cache of all controllers:

  a. First, the storage system had not been added to an LDAP domain or had not been correctly added to an LDAP domain.

  b. Then, an LDAP domain user of the host accessed the shared space of the storage system through the NFSv4.0 or NFSv4.1 protocol.

  c. Finally, the storage system has been correctly added to an LDAP domain.

Procedure

Step 1 Choose **Settings** > **User and Security** > **Domain Authentication** > **File Service LDAP Domain**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 View LDAP domain parameters of the file service. **Table 3-15** describes the parameters.

NOTE

- On the file service LDAP domain management page, click  to refresh file service LDAP domain information.
- On the file service LDAP domain management page, click  and select the file service LDAP domain information you want to view.

Table 3-15 LDAP domain parameters of the file service

Parameter	Description
Status	Indicates whether the file service LDAP domain is enabled.
Server Address	IP address or domain name of the LDAP server. **NOTE** The first server in the list is the active LDAP server, and others are standby.
Protocol	Encryption protocol used for domain authentication.
Port	Port used by the storage device to communicate with the LDAP domain server.
Base DN	LDAP domain's start distinguished name (DN) specified for searching.

NOTE

You can click the LDAP information bar of the file service to view and manage the LDAP information.

Step 4 You can also configure and restore the file service LDAP domain to initial configuration.

- Configure
  a. Select the LDAP domain to be configured and click **Configure**.
     The **Configure File Service LDAP Domain** page is displayed on the right.

     NOTE

     Alternatively, choose **Services** > **vStore Service** > **vStores** and click the name of a vStore. On the details page that is displayed on the right, select the **File Service** tab and click **Configure** in the **LDAP Domain** area.
  b. Select **Advanced** in the upper right corner and set server information. **Table 3-16** describes the parameters.

Table 3-16 File service LDAP domain server information

Parameter	Description
Server	In the **Server** area, click **Add** to set the IP address or domain name of the LDAP server. **NOTE** The first server in the list is the active LDAP server, and others are standby. The domain name format requirements are as follows: 1. The domain name can contain 1 to 255 characters, including letters, digits, underscores (_), periods (.), and hyphens (-). 2. Must start with a letter or digit and cannot end with an underscore (_) or a hyphen (-). 3. The domain name cannot contain consecutive periods (.), underscores (_), periods (.), or only digits. **NOTE** ■ Ensure that the IP address or domain name is reachable. Otherwise, user authentication commands and network commands will time out. ■ To remove an LDAP server, select the desired server and click **Remove**. ■ To test connectivity, select the desired server and click **Test**. [Example] 192.168.1.10 www.test.com
Protocol	Protocol used by the storage system to communicate with the LDAP domain server. ■ **LDAP**: The system uses the standard LDAP protocol to communicate with the LDAP domain server. ■ **LDAPS**: The system uses the LDAPS protocol to communicate with the LDAP domain server if the server supports SSL. **NOTE** ■ LDAP is vulnerable to security risks. You are advised to select the LDAPS protocol. ■ Before selecting the LDAPS protocol, choose **Settings** > **Certificates** > **Certificate Management** and select a desired certificate to import the CA certificate file of the LDAP domain server. If the LDAP server is required to authenticate the storage system, import the certificate file and private key file.

Parameter	Description
Port	Port used by the storage device to communicate with the LDAP domain server. ■ The default port number of the LDAP protocol is **389**. ■ The default port number of the LDAPS protocol is **636**. [Value range] The value must be an integer ranging from 1 to 65535.
Base DN	LDAP domain's start DN specified for searching. [Rule] A DN consists of RDNs, which are separated by commas (,). An RDN is in the format of key=value. The value cannot start with a number sign (#) or a space and cannot end with a space. For example, testDn=testDn,xxxDn=xxx. [Format] xxx=yyy, separated by commas (,) [Example] dc=example,dc=com
Bind Using AD Credential	Indicates whether to enable **Bind Using AD Credential**.

c. Set the binding information about the file service LDAP domain. **Table 3-17** describes the parameters.

Table 3-17 Binding information about the file service LDAP domain

Parameter	Description
Bind Level	Bind level for the LDAP domain server. **Simple**: simple authentication. **SASL**: simple authentication and security layer.

Parameter	Description
Bind DN	Binding directory on the server. Binding is a process that a client initiates a connection request to establish a session to the LDAP server. During binding, the client specifies accounts to access directories on the server. You must search the binding directory for desired contents. A bind DN consists of RDNs, which are separated by commas (,). An RDN is in the format of key=value. The value cannot start with a number sign (#) or a space and cannot end with a space. For example: testDn=testDn,exampleDn=example **NOTE** The default access account is the administrator account. If you use another account, ensure that it has access permission to the domain service on the LDAP server.
Bind Password	Password used for accessing the binding directory. **NOTE** A simple password may result in security issues. A complex password that contains uppercase letters, lowercase letters, digits, and special characters is recommended.
Confirm Bind Password	Confirms the password for logging in to the LDAP domain server.

d. Set the query information about the file service LDAP domain. **Table 3-18** describes the parameters.

Table 3-18 Query information about the file service LDAP domain

User Directory	Indicates the user directory configured on the LDAP domain server. The directory of a user consists of RDNs, which are separated by commas (,). An RDN is in the format of key=value. The value cannot start with a number sign (#) or a space and cannot end with a space. For example: testDn=testDn,exampleDn=example
User Search Scope	Indicates the search scope for user queries. ■ **Subtree**: searches the named DN and subnodes under the DN. ■ **One-level**: searches the subnodes under the DN. ■ **Base**: searches just the named DN.

User Group Directory	Indicates the user group directory configured on the LDAP domain server. The directory of a user group consists of RDNs, which are separated by commas (,). An RDN is in the format of key=value. The value cannot start with a number sign (#) or a space and cannot end with a space. For example: testDn=testDn,exampleDn=example
User Group Search Scope	Indicates the search scope for user group queries. **Subtree**: searches the named DN and subnodes under the DN. **One-level**: searches the subnodes under the DN. **Base**: searches just the named DN.
Network Group DN	Indicates the network group DN. The directory where a network group is located consists of RDNs, which are separated by commas (,). An RDN is in the format of key=value. The value cannot start with a number sign (#) or a space and cannot end with a space. For example: testDn=testDn,exampleDn=example
Network Group Search Scope	Indicates the search scope for network group queries. ▪ **Subtree**: searches the named DN and subnodes under the DN. ▪ **One-level**: searches the subnodes under the DN. ▪ **Base**: searches just the named DN.
Search Timeout Duration (s)	Indicates the timeout duration that the client waits for the LDAP domain server to return the query result. The default value is 3 seconds.
Connection Timeout Duration (s)	Indicates the timeout duration that the client establishes a connection with the LDAP domain server. The default value is 3 seconds.
Idle Timeout Duration (s)	Indicates the timeout duration that the client has no communication with the LDAP domain server. The default value is 30 seconds.

e. Set the LDAP template information. **Table 3-19** describes the parameters.

Table 3-19 LDAP template information.

Parameter	Description
LDAP Schema Template	You can select a type for the LDAP schema template. ■ **RFC2307**: schema based on RFC2307 ■ **AD-IDMU**: schema based on active directory identity management in UNIX. **NOTE** ■ You can select a schema template for which relevant parameters are entered automatically. You can also customize relevant parameters instead of selecting a schema template. ■ A schema defines the structure and rules for LDAP directories and how LDAP servers identify category, attribute, and other information of LDAP directories.
RFC2307 posixAccount Object Class	Schema defines the name of the RFC2307 posixAccount object class. [Default value] ■ **posixAccount** (displayed by default when **RFC2307** is selected in **LDAP Schema Template**) ■ **User** (displayed by default when **AD-IDMU** is selected in **LDAP Schema Template**)
RFC2307 posixGroup Object Class	Schema defines the name of the RFC2307 posixGroup object class. [Default value] ■ **posixGroup** (displayed by default when **RFC2307** is selected in **LDAP Schema Template**) ■ **Group** (displayed by default when **AD-IDMU** is selected in **LDAP Schema Template**)
RFC2307 nisNetgroup Object Class	Schema defines the name of the RFC2307 nisNetgroup object class. [Default value] nisNetgroup
RFC2307 uid Attribute	Schema defines the name of the RFC2307 uid attribute. [Default value] uid

Parameter	Description
RFC2307 uidNumber Attribute	Schema defines the name of the RFC2307 uidNumber attribute. [Default value] uidNumber
RFC2307 gidNumber Attribute	Schema defines the name of the RFC2307 gidNumber attribute. [Default value] gidNumber
RFC2307 CN Attribute for User Group	Schema defines the name of the RFC2307 CN attribute for user group. [Default value] cn
RFC2307 CN Attribute for Network Group	Schema defines the name of the RFC2307 CN attribute for network group. [Default value] ■ **cn** (displayed by default when **RFC2307** is selected in **LDAP Schema Template**) ■ **name** (displayed by default when **AD-IDMU** is selected in **LDAP Schema Template**)
RFC2307 memberUid Attribute	Schema defines the name of the RFC2307 memberUid attribute. [Default value] memberUid
RFC2307 memberNisNetgroup Attribute	Schema defines the name of the RFC2307 memberNisNetgroup attribute. [Default value] memberNisNetgroup
RFC2307 nisNetgroupTriple Attribute	Schema defines the name of the RFC2307 nisNetgroupTriple attribute. [Default value] ■ **nisNetgroupTriple** (displayed by default when **RFC2307** is selected in **LDAP Schema Template**) ■ **nisNetgroupTriple** (displayed by default when **AD-IDMU** is selected in **LDAP Schema Template**)
Support RFC2307bis	Indicates whether to enable the RFC2307bis attribute.

Parameter	Description
RFC2307bis groupOfUniqueNames Object Class	Schema defines the name of the RFC2307bis groupOfUniqueNames object class. This parameter is valid only when **Support RFC2307bis** is enabled. [Default value] groupOfUniqueName
RFC2307bis uniqueMember Object Class	Schema defines the name of the RFC2307bis uniqueMember attribute. This parameter is valid only when **Support RFC2307bis** is enabled. [Default value] uniqueMember

f. Click **OK**.

- Restore to Initial

  Select **File Service LDAP Domain** and click **Restore to Initial**.

----End

3.8.1.7 (Optional) Adding a Storage System to an NIS Domain

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

3.8.1.7.1 Preparing NIS Domain Configuration Data

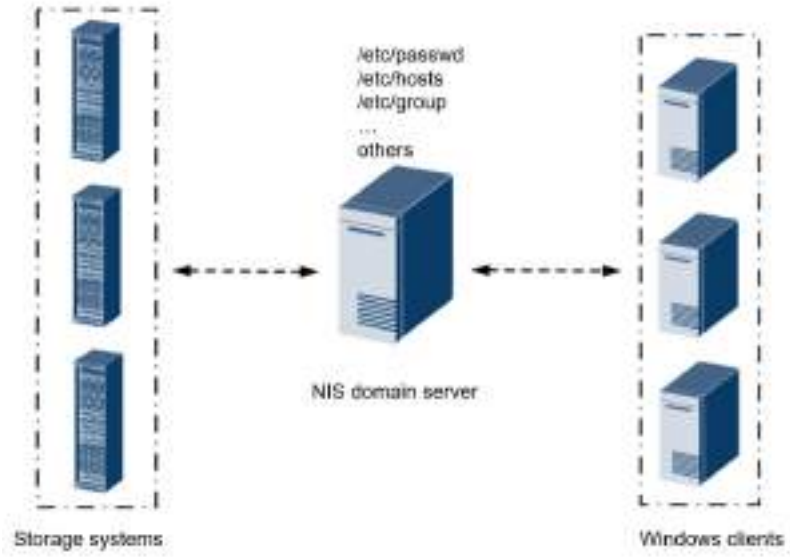
Before adding a storage system to an NIS domain, collect the configuration data of an NIS server.

Why NIS Domains?

In UNIX shared mode, all nodes that provide sharing services must maintain their configuration files such as **/etc/hosts** and **/etc/passwd**. For example, if you add a new node to the shared network, all UNIX-based systems need to update their **/etc/hosts** files to include the name of the new node. If you add a new user who may need to access all nodes, all the systems need to modify their **/etc/passwd** files. These operations are time-consuming when more than 10 nodes are deployed.

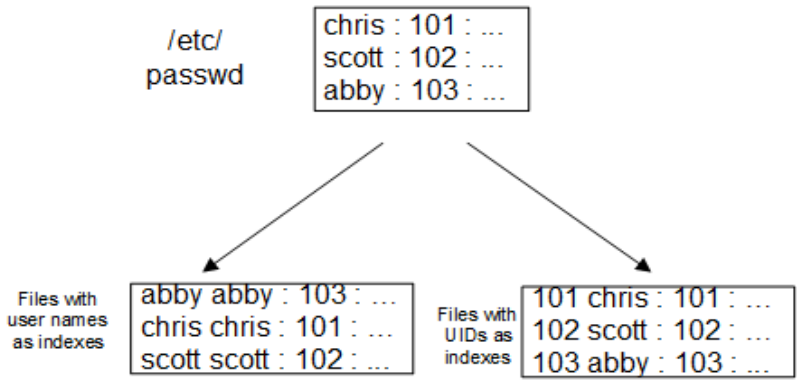
NIS developed by SUN Microsystem uses a single system (NIS server) to manage and maintain the files containing information about host names and user accounts, providing references for all the systems configured as NIS clients. When NIS is used, if you want to add a host to the shared network, you only need to modify a related file on the NIS server and transfer the modification to other nodes on the network.

The following figure shows the relationship between an NIS server and other hosts.



Working Principles

When NIS is configured, the ASCII files in the NIS domain are converted to NIS database files (or mapping table files). Hosts in the NIS domain query and parse the NIS database files to perform operations such as authorized access and updates. For example, common password file **/etc/passwd** of a UNIX host is converted to the following NIS database files:



Parameters

Default maps for an NIS domain are located in each server's **/var/yp/domainname** directory. For example, the maps that belong to the domain test.com are located in each server's **/var/yp/test.com** directory.

The system super administrator can run the **/usr/bin/domainname** command to rename a domain in interactive mode. Common users can run the **domainname** command without parameters to obtain the default domain name of the local system.

Data Preparation

Collect **Domain Name**, **Active Server Address**, **Standby Server Address 1 (Optional)**, and **Standby Server Address 2 (Optional)**. For details about how to

obtain the data, see **3.8.1.7.2 Configuring NIS Domain Authentication Parameters**.

3.8.1.7.2 Configuring NIS Domain Authentication Parameters

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

Prerequisites

- An NIS domain has been set up.
- Required data has been obtained.

  NOTE

  - The storage systems can connect to a NIS server through management network ports or service network ports (logical ports). If a storage system connects to a NIS server through management network ports, ensure that the management network ports on at least two controllers can properly communicate with the NIS server. If a storage system connects to an NIS server through service network ports, it is recommended that the service network ports on at least two controllers can properly communicate with the NIS server. It is recommended that storage systems connect to NIS servers through service network ports.
  - A storage system can connect to only one NIS server.

Precautions

- You are advised to use physical isolation and end-to-end encryption to ensure security of data transfer between the NIS domain server and clients.
- In the following scenario (the three situations occurred in sequence), use **clear nfs nfsv4_idmap_cache controller=?** to clear the IDMAP cache of all controllers:
  a. First, the storage system had not been added to an NIS domain or had not been correctly added to an NIS domain.
  b. Then, an NIS domain user of the host accessed the shared space of the storage system through the NFSv4.0 or NFSv4.1 protocol.
  c. Finally, the storage system has been correctly added to an NIS domain.

Procedure

Step 1 Choose **Settings** > **User and Security** > **Domain Authentication** > **File Service NIS Domain**.

Step 2 Select a desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 View NIS domain parameters of the file service. **Table 3-20** describes the parameters.

NOTE

- On the file service NIS domain management page, click to refresh file service NIS domain information.
- On the file service NIS domain management page, click and select the file service NIS domain information you want to view.

Table 3-20 NIS domain parameters of the file service

Parameter	Description
Status	Indicates whether the file service NIS domain is enabled.
Domain Name	Indicates the domain name of the NIS domain server.
Active Server Address	Indicates the active NIS server IP address or domain name.
Standby Server Address 1	Indicates the IP address or domain name of standby NIS server 1.
Standby Server Address 2	Indicates the IP address or domain name of standby NIS server 2.

Step 4 You can also configure and restore the file service NIS domain to initial configuration.

- Configure
  a. Select the NIS domain to be configured and click **Configure**.
     The **Configure File Service NIS Domain** page is displayed on the right.

     NOTE

     Alternatively, choose **Services** > **vStore Service** > **vStores** and click the name of a vStore. On the details page that is displayed on the right, select the **File Service** tab and click **Configure** in the **NIS Domain** area.
  b. Configure basic information. **Table 3-21** describes the parameters.

Table 3-21 Basic information about the file service NIS domain

Parameter	Description
Domain Name	Indicates the domain name of the NIS domain server. The domain name format requirements are as follows: 1. The domain name can contain 1 to 63 characters, including letters, digits, underscores (_), periods (.), and hyphens (-). 2. The domain name cannot start or end with an underscore (_) or hyphen (-). 3. The domain name can contain multi-level sub-domain names, which are separated by periods (.). A period (.) cannot be at the beginning or end of a domain name, and multiple periods (.) cannot be entered consecutively. [Example] abc.com
Active Server Address	Indicates the active NIS server IP address or domain name. **NOTE** ■ Ensure that the IP address or domain name is reachable. Otherwise, user authentication commands and network commands will time out. ■ Click **Test** to check the connectivity of the entered IP address or domain name. [Example] 192.168.0.100 www.test.com
Standby Server Address 1	Indicates the IP address or domain name of standby NIS server 1. **NOTE** ■ Ensure that the IP address or domain name is reachable. Otherwise, user authentication commands and network commands will time out. ■ Click **Test** to check the connectivity of the entered IP address or domain name. [Example] 192.168.0.101 www.test1.com

Parameter	Description
Standby Server Address 2	Indicates the IP address or domain name of standby NIS server 2. **NOTE** ■ Ensure that the IP address or domain name is reachable. Otherwise, user authentication commands and network commands will time out. ■ Click **Test** to check the connectivity of the entered IP address or domain name. [Example] 192.168.0.102 www.test2.com

c. Click **OK**.

- Restore to Initial

  Select **File Service NIS Domain** and click **Restore to Initial**.

----End

3.8.1.8 (Optional) Configuring the NFSv4 Service for a Non-Domain Environment

This section describes how to configure the NFSv4 service for a non-domain environment.

Background

According to the NFSv4 standard protocol, the NFSv4 service can be used only in a domain environment to ensure proper running. 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. Then, the NFSv4 service will use UIDs and GIDs to transfer owner and group information about files during service transactions between your storage system and client.

Risks

- In scenarios where the NFSv4 service is used in a non-domain environment, the user authentication method of the NFSv4 service is the same as that of the NFSv3 service. The method cannot meet the theoretical security requirements of the NFSv4 standard protocol.
- Users mapped by each client depend on the configuration files of client users and user groups. The configuration file of each user and user group must be independently maintained for proper mapping.
- UIDs and GIDs must be used when ACLs are configured for non-root users and non-root user groups. Otherwise, the configuration will fail.
- The NFSv4 service is not recommended in a non-domain environment. If operations in **Configuration on Clients** are not performed, executing the **chown** command may fail.

Configuration on Clients

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 NFSv4 service is successfully configured.

NOTICE

If you have used the NFSv4 service to mount NFS shares before configuring the NFSv4 service for a non-domain environment, mount the NFS shares again after configuring the NFSv4 service.

----End

3.8.1.9 Creating an NFS Share

This section describes how to create an NFS share. After an NFS share is created, shared file systems are accessible to clients that run SUSE, Red Hat, HP-UX, Solaris, and AIX.

Prerequisites

You have obtained required data for configuring an NFS share.

Procedure

Step 1 Choose **Services** > **File Service** > **Shares** > **NFS Shares**.

Step 2 Select the vStore to which the desired file system belongs from the **vStore** drop-down list in the upper left corner.

Step 3 On the **NFS Shares** tab page, click **Create**.

The **Create NFS Share** page is displayed on the right.

NOTE

The screenshot is for reference only and the actual displayed information may vary.

For some device models, you can click in the upper right corner of the page to enable SmartGUI. SmartGUI mines users' historical operation data and builds a configuration parameter recommendation model based on user profiles to recommend configuration parameters for the block service and file service. After SmartGUI is enabled, the system presets the **File System** and **Permission** parameters based on recommendations when you create an NFS share. You can directly use the parameters or modify them as required.

Step 4 Set basic NFS share parameters.

Table 3-22 describes the parameters.

Table 3-22 Basic NFS share parameters

Parameter	Description
File System	File system for which you want to create an NFS share. **NOTE** When the global root directory **/** is selected for **File System**, you can create an NFS global namespace (GNS) share. ● Each vStore can only create one GNS. ● You must add an independent share for a file system. After the share is added, this file system will not be displayed if a host is only authorized to access **/** but not the file system. ● GNS root directory **/** is read-only. You cannot create, modify, and delete directories or files under **/** and you cannot modify directory attributes of **/**. Once the directory of a file system is entered, the permission will change to the share permission of the file system. ● If no GNS is created, root directory **/** cannot be mounted to an NFSv3 client. Only shared file systems can be viewed when **/** is mounted to an NFSv4 directory. ● When creating an NFS GNS share, you can only set the description for the share. ● If you want to create a HyperMetro or HyperReplication vStore pair and a GNS has been created for the primary vStore, the version of the secondary storage system must be the same as that of the primary storage system. If a vStore pair has been created, you can create a GNS share only when the versions of the primary and secondary storage systems are the same and support GNSs. [Example] FileSystem001 **NOTICE** If the selected file system is the secondary storage system in a remote replication pair or remote storage system in a HyperMetro pair, data in the file system is probably being modified when it is accessed. Before performing this operation, confirm that the application allows possible data inconsistency.
Dtree	Dtree for which you want to create an NFS share. If you do not select a dtree, the NFS share is created for the entire file system. [Example] Dtree_test
Share Path	Share path of the file system, which is generated based on the **File System** and **Dtree** parameters. [Example] /Filesystem001/Dtree_test
Description	Description of the NFS share. [Value range] The description can be left blank or contain up to 255 characters.

Parameter	Description
Character Encoding	Clients communicate with the storage system using codes. Codes configured on the NFS share must be the same as that of the clients. These codes apply to names and metadata of shared files, but do not change the codes of file data. Codes include: • UTF-8 International code set • EUC-JP euc-j*[ja] code set • JIS JIS code set • S-JIS cp932*[ja_jp.932] code set • ZH Simplified Chinese code set, in compliance with GB 2312 • GBK Simplified Chinese code set, in compliance with GB 2312 • EUC-TW Traditional Chinese code set, in compliance with CNS 11643 • BIG5 cp950 traditional Chinese code set • DE German character set, in compliance with ISO 8859-1 • PT Portuguese character set, in compliance with ISO 8859-1 • ES Spanish character set, in compliance with ISO 8859-1 • FR French character set, in compliance with ISO 8859-1 • IT Italian character set, in compliance with ISO 8859-1 • KO cp949 Korean code set • AR Arabic character set, in compliance with ISO 8859-6 • CS Czech character set, in compliance with ISO 8859-2 • DA Danish character set, in compliance with ISO 8859-1 • FI Finnish character set, in compliance with ISO 8859-1 • HE Hebrew character set, in compliance with ISO 8859-8

Parameter	Description
	• HR Croatian character set, in compliance with ISO 8859-2 • HU Hungarian character set, in compliance with ISO 8859-2 • NO Norwegian character set, in compliance with ISO 8859-1 • NL Dutch character set, in compliance with ISO 8859-1 • PL Polish character set, in compliance with ISO 8859-2 • RO Romanian character set, in compliance with ISO 8859-2 • RU Russian character set, in compliance with ISO 8859-5 • SK Slovak character set, in compliance with ISO 8859-2 • SL Slovenian character set, in compliance with ISO 8859-2 • SV Swedish character set, in compliance with ISO 8859-1 • TR Turkish character set, in compliance with ISO 8859-9 • EN-US English character set, in compliance with ISO 8859-1 **NOTE** • Method of querying character encoding on clients (for example, in Linux): Run the **locale** command to view character encoding of the current system. • NFSv4 supports only UTF-8. If NFSv4 is used, ensure that the host uses UTF-8 character encoding.
Show Snapshot	This function allows clients to show and traverse snapshot directories.

NOTE

Description, **Character Encoding**, and **Show Snapshot** are hidden parameters. You can click **Advanced** to display them.

Step 5 Configure access permissions for the NFS share.

Click **Add** to add a client. For details, see **3.8.1.10 Adding an NFS Share Client**.

NOTE

- When **Type** is set to **Host**, the system automatically detects whether the LDAP domain, NIS domain, or DNS has been configured. To add a client by specifying the host name, configure at least one of them.
- When **Type** is set to **Network group**, the system automatically detects whether the LDAP domain or NIS domain has been configured. You must configure at least one of them.
- You can click **More** on the right of a client and select **Modify** to modify its information.
- You can select one or more clients and click **Remove**, or click **More** on the right of a client and select **Remove**, to remove clients.

Step 6 Click **OK**.

----End

3.8.1.10 Adding an NFS Share Client

An NFS share client enables client users to access shared file systems through the network.

Prerequisites

- You have obtained required data for configuring an NFS share.
- You have created a host name available on the DNS if you need to add a client whose **Type** is **Host**.
- You have created a network group name available on the LDAP or NIS server if you need to add a client whose **Type** is **Network group**.
- If **Share Path** is set to global root directory **/**, you cannot add a client.

Procedure

Step 1 Choose **Services** > **File Service** > **Shares** > **NFS Shares**.

Step 2 Select the vStore to which the desired NFS share belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Click **More** on the right of the desired NFS share and select **Add Client**.

The **Add Client** page is displayed.

NOTE

Alternatively, perform either of the following operations to add a client:

- Click the path of the desired NFS share. On the page that is displayed, click **Add** in the **Permissions** area.
- Click the path of the desired NFS share. In the upper right corner of the page that is displayed, click **Operation** and select **Add Client**.

NOTE

For some device models, you can click  in the upper right corner of the page to enable SmartGUI. SmartGUI mines users' historical operation data and builds a configuration parameter recommendation model based on user profiles to recommend configuration parameters for the block service and file service. After SmartGUI is enabled, the system presets the **Type** and **Permission** parameters based on recommendations when you add a client. You can directly use the parameters or modify them as required.

Step 4 Set client attributes.

Table 3-23 describes the parameters.

Table 3-23 Client parameters

Parameter	Description
Type	Client type of the NFS share. [Value range] • Host • Network group **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 > network segment > wildcard > network group > *. • When **Type** is set to **Network group** and the vStore to which the share belongs is configured with the DNS service, add the reverse lookup zones of the network segments where the client IP addresses reside on the DNS server. Otherwise, the host I/O latency may increase.

Parameter	Description
Clients	When **Type** is set to **Host**, enter client host names (FQDNs are recommended), IP addresses, or IP address segments, or use the asterisk (*) to represent IP addresses of all clients. When **Type** is set to **Network group**, enter the network group names configured in the LDAP or NIS domain. **NOTE** • When **Type** is set to **Host**, the system automatically detects whether the LDAP domain, NIS domain, or DNS has been configured. To add a client by specifying the host name, configure at least one of them. • When **Type** is set to **Network group**, the system automatically detects whether the LDAP domain or NIS domain has been configured. You must configure at least one of them. [Value range] You can enter multiple host names, IP addresses, or network group names of the clients separated by semicolons (;), spaces, or carriage returns. For host names: • A host name contains 1 to 255 characters and cannot contain spaces. • A host name cannot start with a hyphen (-). For IP addresses: • You can enter client IP addresses, client IP address segments, or an asterisk (*) to represent IP addresses of all clients. • IPv4 addresses, IPv6 addresses, or the combination of IPv4 and IPv6 addresses are supported. • The mask of an IPv4 address ranges from 1 to 32. The prefix of an IPv6 address ranges from 1 to 128. A network group name: • Contains 1 to 254 characters. • The value can contain only letters, digits, underscores (_), periods (.), and hyphens (-).
UNIX Permission	Indicates the permission level for a UNIX client to access the NFS share. Possible options are: • **Read-only**: The client can only read files in the share. • **Read-write**: The client can read and write files in the share. • **None**: No operation is allowed on the share.

Parameter	Description
Kerberos5 Permission	Indicates the permission level for the Kerberos5 client to access the NFS share. Possible options are: ● **Read-only**: The client can only read files in the share. ● **Read-write**: The client can read and write files in the share. ● **None**: No operation is allowed on the share. This parameter applies only to the scenario where the NFS Kerberos service is configured.
Kerberos5i Permission	Indicates the permission level for the Kerberos5i client to access the NFS share. Possible options are: ● **Read-only**: The client can only read files in the share. ● **Read-write**: The client can read and write files in the share. ● **None**: No operation is allowed on the share. This parameter applies only to the scenario where the NFS Kerberos service is configured.
Kerberos5p Permission	Indicates the permission level for the Kerberos5p client to access the NFS share. Possible options are: ● **Read-only**: The client can only read files in the share. ● **Read-write**: The client can read and write files in the share. ● **None**: No operation is allowed on the share. This parameter applies only to the scenario where the NFS Kerberos service is configured.
root Permission Constraint	Controls the **root** permission of the clients. ● **root_squash**: does not allow a client to access the share as user **root**. Otherwise, the client will be mapped as an anonymous user. ● **no_root_squash**: allows a client to access the share as user **root** that has full control and access permissions for shared directories. **NOTE** ● If a VM needs to be created in the NFS share, select **no_root_squash**. Otherwise, the VM may run abnormally. ● For a file system or dtree whose security mode is UNIX, the default UNIX permission is **755**. If **root_squash** is enabled for the NFS share permission of the file system or dtree, user **root** only has the read and execute permissions. You can run the **change file_system general file_system_id=? unix_permissions=?** or **change dtree dtree_id=? unix_permissions=?** command to modify the UNIX permission of the file system or dtree.

NOTE

In the NFS Kerberos service application scenario, the settings of **Kerberos5 Permission**, **Kerberos5i Permission**, and **Kerberos5p Permission** in the preceding table must match the **sec** field specified when an NFS share is mounted on a client. 00

For example, if the **sec** field is set to **krb5i** when an NFS share is mounted to a client, at least **Kerberos5i Permission** must be set for the client.

Step 5 Set advanced client parameters. Select **Advanced** in the upper right corner.

Table 3-24 describes the parameters.

Table 3-24 Advanced client parameters

Parameter	Description
Permission Constraint	Indicates whether to retain the user ID (UID) and group ID (GID) of a shared directory. • **all_squash**: The UID and GID of a shared directory are mapped to user **nobody**, which is applicable to public directories. • **no_all_squash**: retains the UID and GID of a shared directory. [Default value] **no_all_squash**
Source Port Verification Constraint	Indicates whether to enable source port verification. • **secure**: allows clients to access the NFS share using ports 1 to 1023. • **insecure**: allows clients to access the NFS share using any port. [Default value] **insecure**
Anonymous User ID	Indicates the UID and GID of a user who accesses the shared directory after the user is mapped as an anonymous user. [Default value] 65534 **NOTE** Only 6.1.5 and later versions support this parameter.

Step 6 Click **OK**.

----End

3.8.1.11 Accessing an NFS Share

This section describes how to use a client to access an NFS share. A client accesses an NFS share in an LDAP/NIS domain or a non-domain environment in the same way.

Context

- The storage system supports NFSv3, NFSv4.0, and NFSv4.1.
- The NFSv4.0 and NFSv4.1 services are disabled by default in the storage system. If you want to use NFSv4.0 or NFSv4.1 for share access, enable the NFSv4 service first.
- You can run the **change user_mode current_mode user_mode=developer** command to enter the developer mode. For details about the commands, see the advanced O&M command reference.

Precautions

When a file system is mounted using NFSv4.0 or NFSv4.1, ensure that the same domain name is configured for both the host and storage. (Generally, the default domain name is **localdomain** on both the host and storage device.) Otherwise, when files created by a host user are queried on the storage, the information about the user and group to which the files belong is incorrectly displayed. For example, user **root** is displayed as **nobody** on the storage.

- On the host, query the domain name in the configuration file of the idmapd service. For example, in the SUSE operating system, you can run the **vi /etc/idmapd.conf** command to query or edit the value of **Domain**.
- On the storage, run the **change vstore view id=***?* command to enter the vStore view. You can run the **show vstore** command to query the value of **id**. Then run the **show service nfs_config** command in developer mode to query the domain name. The default domain name is **localdomain**. To change the domain name on the storage, run the **change service nfs_config domain_name=***?* command.

SUSE, Red Hat, or Ubuntu Client

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

Step 2 Run the **showmount -e** *ipaddress* command to view available NFS shares in the storage system.

ipaddress represents the logical IP address of the storage system. 192.168.50.16 is used as an example.

```
#showmount -e 192.168.50.16
Export list for 192.168.50.16
/nfstest *
#
```

NOTE

/nfstest in the output represents the share path of the NFS share created in the storage system. If a GNS is created, **/** will be displayed.

Step 3 Run the **mount -t nfs -o vers=n,proto=m,rsize=o,wsize=p,hard,intr,timeo=q** *ipaddress*:*sharepath* **/mnt** command to mount an NFS share to the client. **Table 3-25** describes the related parameters.

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

```
#mount -t nfs -o vers=3,proto=tcp,rsize=262144,wsize=262144,hard,intr,timeo=50 192.168.50.16:/
nfstest /mnt
```


NOTE

- If the client uses NFSv4.1 to mount an NFS share, you are advised to specify the **minorversion** parameter. For a SUSE client, run the following command (commands for other operating systems are similar):
  ```
  mount -t nfs -o vers=4,minorversion=1,proto=tcp,rsize=262144,wsize=262144,hard,intr,timeo=50
  192.168.50.16:/nfstest /mnt
  ```
- To mount a GNS, run the following command:
  ```
  #mount -t nfs -o vers=3,proto=tcp,rsize=262144,wsize=262144,hard,intr,timeo=50
  192.168.50.16:/ /mnt
  ```

Table 3-25 Parameters for mounting an NFS share to a SUSE, Red Hat, or Ubuntu client

Parameter	Description	Setting
o	Mounting mode of the NFS share. Possible values are **ro** and **rw**. • **ro**: mounts a share that is read-only. • **rw**: mounts a share that can be read and written.	The default value is **rw**.
vers	NFS protocol version.	In an environment that requires high reliability, you are advised to use NFSv3.
proto	Transfer protocol.	Set this parameter to **tcp**.
rsize	Size of the transport block for read, in bytes.	**262144** is recommended.
wsize	Size of the transport block for write, in bytes.	**262144** is recommended.
timeo	Interval for retransmission upon timeout. The unit is 0.1 second.	• The default value is **600**. • If there is a high requirement on the service recovery time, you are advised to set this parameter to **50**.

NOTE

In the preceding table, **vers** is mandatory, and other parameters are optional. You are advised to use the recommended parameter settings.

Step 4 Run the **mount** command to verify that the NFS share has been mounted to the local computer.

```
#mount
192.168.50.16:/nfstest on /mnt type nfs
(rw,vers=3,proto=tcp,rsize=262144,wsize=262144,hard,intr,timeo=50,addr=192.168.50.16)
```


NOTE

If a GNS is mounted, the following information is displayed:

```
#mount
192.168.50.16:/ on /mnt type nfs
(rw,vers=3,proto=tcp,rsize=262144,wsize=262144,hard,intr,timeo=50,addr=192.168.50.16)
```

When the preceding information is displayed, the NFS share has been successfully mounted to the local computer.

----End

Debian Client

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

Step 2 On the client, run the **apt-get install nfs-common** command to install the **nfs-common** software package.

Step 3 Run the **showmount -e** *ipaddress* command to view available NFS shares in the storage system.

ipaddress represents the logical IP address of the storage system. 192.168.50.16 is used as an example.

```
#showmount -e 192.168.50.16
Export list for 192.168.50.16
/nfstest *
#
```

NOTE

/nfstest in the output represents the share path of the NFS share created in the storage system. If a GNS is created, **/** will be displayed.

Step 4 Run the **mkdir /mnt/share** command to create a directory on the client to mount an NFS share.

The following uses the **/share** directory as an example.

Step 5 Run the **mount** *ipaddress*:*sharepath* **/mnt/share** command to mount an NFS share.

sharepath represents the **Share Path** of the NFS share created in the storage system.

```
mount 192.168.50.16:/nfstest /mnt/share
```

NOTE

To mount a GNS, run the following command:

```
mount 192.168.50.16:/ /mnt/share
```

Step 6 Run the **df -hT** command to verify that the NFS share has been successfully mounted to the local computer.

----End

HP-UX or SUN Solaris Client

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

Step 2 Run the **showmount -e** *ipaddress* command to view available NFS shares in the storage system.

ipaddress represents the logical IP address of the storage system. 192.168.50.16 is used as an example.

```
#showmount -e 192.168.50.16
Export list for 192.168.50.16
/nfstest *
#
```

NOTE

/nfstest in the output represents the share path of the NFS share created in the storage system. If a GNS is created, **/** will be displayed.

Step 3 Run the **mount** [**-F nfs|-f nfs**] **-o vers=n,proto=m** *ipaddress*:*sharepath* **/mnt** command to mount an NFS share. **Table 3-26** describes the related parameters.

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

```
#mount -f nfs -o vers=3,proto=tcp 192.168.50.16:/nfstest /mnt
```

NOTE

To mount a GNS, run the following command:

```
#mount -f nfs -o vers=3,proto=tcp 192.168.50.16:/ /mnt
```

Table 3-26 Parameters for mounting an NFS share to an HP-UX or a SUN Solaris client

Parameter	Description	Setting
-F nfs or -f nfs	Optional	**-F nfs** is available to an HP-UX client and **-f nfs** is available to a Solaris client.
vers	NFS protocol version	In an environment that requires high reliability, you are advised to use NFSv3.
proto	Transfer protocol	Set this parameter to **tcp**.

NOTE

In the preceding table, **vers** is mandatory, and other parameters are optional. You are advised to use the recommended parameter settings.

Step 4 Run the **mount** command to verify that the NFS share has been mounted to the local computer.

```
#mount
192.168.50.16:/nfstest on /mnt type nfs (rw,vers=3,proto=tcp,addr=192.168.50.16)
```


NOTE

If a GNS is mounted, the following information is displayed:

```
#mount
192.168.50.16:/ on /mnt type nfs (rw,vers=3,proto=tcp,addr=192.168.50.16)
```

When the preceding information is displayed, the NFS share has been successfully mounted to the local computer.

----End

IBM AIX Client

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

Step 2 Run **showmount -e** *ipaddress* to view available NFS shares in the storage system.

ipaddress represents the logical IP address of the storage system. 192.168.50.16 is used as an example.

```
#showmount -e 192.168.50.16
Export list for 192.168.50.16
/nfstest *
#
```

NOTE

/nfstest in the output represents the share path of the NFS share created in the storage system. If a GNS is created, **/** will be displayed.

Step 3 Run the **mount** *ipaddress*:*sharepath* **/mnt** command to mount an NFS share.

sharepath represents the **Share Path** of the NFS share created in the storage system.

```
#mount 192.168.50.16:/nfstest /mnt
mount: 1831-008 giving up on:
192.168.50.16:/nfstest
Vmount: Operation not permitted.
#
```

NOTE

- To mount a GNS, run the following command:
  ```
  #mount 192.168.50.16:/ /mnt
  mount: 1831-008 giving up on:
  192.168.50.16:/
  Vmount: Operation not permitted.
  #
  ```
- If the default NFS port on an AIX client is different from that on the storage system, the preceding command cannot be executed and a message is displayed indicating that the operation permission is restricted. The NFS share fails to be mounted. In this case, run the following command to solve this problem. You can also use the SMIT menu to mount the NFS shared file system.
  ```
  #nfso -o nfs_use_reserved_ports=1
  Setting nfs_use_reserved_ports to 1
  ```

Step 4 Run the **mount** command to verify that the NFS share has been mounted to the local computer.

```
#mount
192.168.50.16:/nfstest on /mnt type nfs (rw,addr=192.168.50.16)
```


NOTE

If a GNS is mounted, the following information is displayed:

```
#mount
192.168.50.16:/ on /mnt type nfs (rw,addr=192.168.50.16)
```

When the preceding information is displayed, the NFS share has been successfully mounted to the local computer.

----End

VMware Client

NOTE

When you want to create VMs on an NFS share, **Root Permission Constraint** of the NFS share must be **no_root_squash**.

- vSphere Client

NOTE

GUIs may vary with versions. The actual GUIs prevail.

Step 1 Log in to VMware vSphere Client.

Step 2 Select the desired host from the left navigation tree.

Step 3 Choose **Configuration** > **Storage** > **Add Storage**.

The **Add Storage** wizard is displayed.

Step 4 In **Select Storage Type**, select **Network File System** and click **Next**.

The **Locate Network File System** page is displayed.

Step 5 Set the related parameters. **Table 3-27** describes related parameters.

Table 3-27 Parameters for adding an NFS share in VMware

Parameter	Description	Value
Server	Logical IP address of the storage system.	Example 192.168.50.16
Folder	**Share Path** of the NFS share created in the storage system.	Example /nfstest
Datastore Name	Name of the NFS share in VMware.	Example data

Step 6 Click **Next**.

Step 7 Confirm the information and click **Finish**.

Step 8 On the **Configuration** tab page, view the newly added NFS share.

----End

- vSphere Web Client (VMware vSphere 5.5 as an example)

NOTE

GUIs may vary with versions. The actual GUIs prevail.

Step 1 Log in to the VMware vSphere Web Client.

Step 2 Choose **Storage** > **Datastores** > **New datastore**.

The **New datastore** wizard is displayed.

Step 3 On the **Select creation type** page, select **Mount NFS datastore** and click **Next**.

The **Provide NFS mount details** page is displayed.

Step 4 Set related parameters.

Table 3-28 Parameter settings

Parameter	Description
Name	Name of the NFS datastore.
NFS server	Name of the NFS server, which can be the IP address of the logical port or DNS name.
NFS share	Path of the NFS share.

Parameter	Description
NFS version	NFS version, which can be **NFS 3** or **NFS 4**. **NOTE** • The system and data disks of VMs reside in datastores of ESXi hosts. NFSv3 has higher performance than NFSv4.1. Therefore, you are advised to use NFSv3 to mount NFS datastores to ESXi hosts. • If multiple hosts access the same datastore, you must use the same NFS protocol on all hosts.

Step 5 Click **Next**, confirm the information, and click **Finish**.

----End

Follow-up Procedure

If you modify NFS user information, new user authentication information takes effect after 30 minutes.

3.8.1.12 Using Linux ACLs

3.8.1.12.1 Overview

The Linux access control list (ACL), also called NFS ACL, is a set of access control entries (ACEs) for a file or directory on a Linux client. Each ACE is used to specify whether a specific user or user group can access a file or directory or not. In certain applications, users can access NFS shared files only after manually configuring the ACL.

About Linux UGO Permissions

On a Linux client, file permission control is to manage file permissions based on the UGO permissions (UNIX-mode bits). The read, write, and execute permissions can be set for the owner, owner group, and other users of a file.

1. Permission Types and Formats

Table 3-29 Permission types and formats

Permission	In Character Format	In Numeric Format
Read permission	r	4
Write permission	w	2
Execute permission	x	1
No read, write, or execute permission	-	0

2. Meaning of the Permission Character String

   The character string that represents the UGO permission contains 10 characters. The first character indicates the file type, and the other nine characters (the permission bits) indicate the file permissions.

   a. File Type

      Table 3-30 File type description

File Type	Description
-	Common file
d	Directory
l	Linked file
p	Pipeline file
b	Block device file
c	Character device file

   b. Permission Combination

      The nine permission bits in the permission character string are divided into three groups, and each group contains the combination of three permission bits.

      - The first three bits indicate the read, write, and execute permissions of the owner.
      - The middle three bits indicate the read, write, and execute permissions of users in the owner group.
      - The last three bits indicate the read, write, and execute permissions of other users.

      The permissions can be queried by running the **ls –l** *testfile* command. For example, the result is as follows:

```
-rwxr-xr-x 1 testuser testgroup 18 Jan 21 10:17 testfile
```

      The 10-character permission string (**-rwxr-xr-x**) in the command output has the following meanings:

      - The first character "-" indicates that the **testfile** file is a common file.
      - The second to fourth characters "rwx" indicate that the owner (that is, **testuser**) of the **testfile** file has the read, write, and execute permissions.
      - The fifth to seventh characters "r-x" indicate that all users in the owner group (that is, **testgroup**) of the **testfile** file have only the read and execute permissions.
      - The eighth to tenth characters "r-x" indicate that other users have only the read and execute permissions.

NOTE

The sequence of permissions in each permission combination is always rwx. Any permission of r, w, and x, if not available, is indicated by a hyphen (-).

For simplicity, the Linux client also often uses permissions in numeric format. A permission in numeric format consists of the following three numbers:

- The first number is the sum of the numbers of the first 3 permission bits.
- The second number is the sum of the numbers of the middle 3 permission bits.
- The third number is the sum of the numbers of the last 3 permission bits.

In the preceding example, if the permission character string "-rwxr-xr-x" is expressed in numeric format:

- The first number: 4 + 2 + 1 = 7
- The second number: 4 + 0 + 1 = 5
- The third number: 4 + 0 + 1 = 5

Thus, the permission character string "-rwxr-xr-x" is equivalent to the permission 755 in numeric format.

Common Linux permissions in numeric format are described as follows:

Table 3-31 Description of permissions in numeric format on a Linux client

Permission in Character Format	Permission in Numeric Format	Permission Description
-rw-------	600	Only the owner has the read and write permissions.
-rw-r--r--	644	Only the owner has the read and write permissions. The group to which the owner belongs and other users have only the read permission.
-rw-rw-rw-	666	Everyone has read and write permissions.
-rwx------	700	Only the owner has the read, write, and execute permissions.
-rwx--x--x	711	Only the owner has the read, write, and execute permissions. The group to which the owner belongs and other users have only the execute permission.

Permission in Character Format	Permission in Numeric Format	Permission Description
-rwxr-xr-x	755	Only the owner has the read, write, and execute permissions. The group to which the owner belongs and other users have only the read and execute permissions.
-rwxrwxrwx	777	Everyone has read, write, and execute permissions.

3. Command Line Example
   a. To grant the read, write, and execute permissions on the **test.text** file to everyone, run the following command:
   ```
   chmod 777 test.txt
   ```
   b. To grant the read, write, and execute permissions on the **dir_test** directory and all files in the directory to everyone, run the following command:
   ```
   chmod -R 777 dir_test
   ```

About Linux ACL Permissions

The UGO permission management can manage only the permissions of the owner, users in the same group, and users in other groups. It is difficult to manage the permissions of each user or user group.

ACLs are used to solve this problem. ACL permission management is an additional permission management mechanism for file systems on the basis of UGO permission management. It allows you to grant read, write, and execute permissions to any user or user group.

Linux ACL permissions are classified into the following two types:

- POSIX ACL: an extension to the NFSv3 protocol for permission control. For details, see **https://linux.die.net/man/5/acl**.

  NOTICE

  The storage system of the current version does not support the POSIX ACL permission. To use the Linux ACL, mount NFS shares to Linux clients using NFSv4 and use the NFSv4 ACL.

- NFSv4 ACL: an extension to the NFSv4 protocol and provides more fine-grained permission control than POSIX ACL.

  ACE syntax:

  ```
  [access type]:[flags]:[principal]:[permissions]
  ```

  For example:

  On the Linux client, run the **nfs4_getfacl** *testfile* command to query the NFSv4 ACL attribute of the file, which is as follows:


```
A::user@nfsdomain.com:rxtncy
```

Where:

- **A** indicates that the type of the ACE is **Allow**. The ACE principal is allowed to perform the operations corresponding to the permission.
- **user@nfsdomain.com** indicates the principal to which the ACE refers. **https://help.eecs.utk.edu/knowledge-base/linux-topics/nfsv4-acls**
- **rxtncy** indicates the permission bits contained in the ACE. For details, see **Description of NFSv4 ACL Permission Bits**.

NOTE

For more information, see **https://linux.die.net/man/5/nfs4_acl**.

Description of NFSv4 ACL Permission Bits

Each permission bit of the NFSv4 ACL has different meanings. Some permission functions take effect only when multiple permission bits exist at the same time.

Table 3-32 Description of NFSv4 ACL permission bits

Permission Bit	For Files	For Directories
r	Read a file.	List directories.
w	Write a file.	Create a file and directory.
a	Append data to a file.	Create a sub-directory.
x	Execute a file.	Access a directory.
d	Delete a file.	Delete a directory.
D	-	Delete a subfile and subdirectory from a directory.
t	Read the attributes of a file.	Read the attributes of a directory.
T	Modify the attributes of a file.	Write the attributes of a directory.
n	Read the named attributes of a file.	Read the named attributes of a directory.
N	Modify the named attributes of a file.	Modify the named attributes of a directory.
c	Read the ACL of a file.	Read the ACL of a directory.
C	Modify the ACL of a file.	Modify the ACL of a directory.
o	Modify the owner information of a file.	Modify the owner information of a file.
y	Allow the client and server to use synchronous I/Os.	

3.8.1.12.2 Managing Permissions Using NFSv4 ACLs

Prerequisites

- You have familiarized yourself with the basic knowledge of NFSv4 ACL permission management.
- A file system has been mounted on the Linux client using NFSv4.
- The **nfs4-acl-tools** software package has been installed on the Linux client.

  NOTE

  - You can run the **rpm -qa|grep nfs** command to check whether the **nfs4-acl-tools** software package has been installed on the client.
  - If it has not been installed, run the **sudo yum -y install nfs4-acl-tools** or **sudo apt-get install nfs4-acl-tools** command to install it.
  - After the installation is complete, you can use the **nfs4_getfacl**, **nfs4_setfacl**, and **nfs4_editfacl** services to set the NFSv4 ACL.

Context

- Before setting the NFSv4 ACL, you must be familiar with the **nfs4_getfacl**, **nfs4_setfacl**, and **nfs4_editfacl** commands. For example:
  - Check the ACL permissions on the file:
    ```
    nfs4_getfacl file
    ```
  - Set ACL permissions:

    Grant write permission to user 1003:
    ```
    nfs4_setfacl -a A::1003:W file
    ```
    Grant write permission to user group 10005:
    ```
    nfs4_setfacl -a A:g:10005:W file
    ```
    Grant read and write permissions on the files and directories in the **dir_test** directory to user group 10005:
    ```
    nfs4_setfacl -R -a A:g:10005:rW dir_test
    ```
  - Modify ACL permissions:

    nfs4_editfacl is equivalent to **nfs4_setfacl -e**.
    ```
    nfs4_editfacl file
    ```
- When setting the NFSv4 ACL, you are advised to add users to a group and grant permissions to the group instead of granting permissions to the users separately. In this way, you only need to remove the user from the specific group when you want to remove the permissions of the user.

Procedure

This part uses an example to describe how to set NFSv4 ACL for directories or files to implement permission management.

Step 1 Create a user and a group.

For example:

- Create a common user **testuser1** that belongs to a common user group **testgroup**.

- Create an administrator user **adminuser1** that belongs to an administrator group **admingroup**.
- Create a user **anonymoususer**.

```
sudo useradd testuser1
sudo groupadd testgroup
sudo usermod -g testgroup testuser1
sudo useradd adminuser1
sudo groupadd admingroup
sudo usermod -g admingroup adminuser1
sudo useradd anonymoususer
```

Step 2 Run the **cat /etc/group** command to query the IDs of **testgroup** and **admingroup**.

```
testgroup:x:1003:
admingroup:x:1005:
```

Step 3 Set NFSv4 ACL for directories and files.

For example:

Create the **dir_test1** directory and grant the following permissions on all files in the directory:

- Read-only permission to **testgroup**.
- Read, write, and execute permissions to **admingroup**.
- No permission to other users.

```
sudo umask 777
sudo mkdir dir_test1
sudo nfs4_setfacl -a A:fdg:1003:RX dir_test1
sudo nfs4_setfacl -a A:fdg:1005:RWX dir_test1
sudo nfs4_setfacl -a A:fdg:OWNER@: dir_test1
sudo nfs4_setfacl -a A:fdg:GROUP@: dir_test1
sudo nfs4_setfacl -a A:fdg:EVERYONE@: dir_test1
```

After the setting is complete, you can run the **sudo nfs4_getfacl dir_test1** command to query the setting result.

```
A::OWNER@:tTnNcCy
A::GROUP@:tncy
A::EVERYONE@:tncy
A:fdi:EVERYONE@:tncy
A:fdi:OWNER@:tTnNcCy
A:fdi:GROUP@:tncy
A:g:1003:rxtncy
A:g:1005:rwaDxtTnNcCy
A:fdig:1003:rxtncy
A:fdig:1005:rwaDxtTnNcCy
```

Step 4 Verify the permission settings.

1. The **testuser1** user should have the read-only permission on the **dir_test1** directory.

```
[root@localhost] sudo su testuser1 -c 'touch dir_test1/testfile'
touch: cannot touch 'dir_test1/testfile': Permission denied
[root@localhost] sudo su testuser1 -c 'echo 456 >> dir_test1/testfile'
bash: dir_test1/testfile: Permission denied
[root@localhost] sudo su testuser1 -c 'cat dir_test1/testfile'
123
[root@localhost] sudo su testuser1 -c 'nfs4_getfacl dir_test1/testfile'
A::OWNER@:tTnNcCy
A::GROUP@:tncy
A::EVERYONE@:tncy
A:g:1003:rxtncy
A:g:1005:rwaxtTnNcCy
```


2. The **adminuser1** user should have the read and write permissions on the **dir_test1** directory.
```
[root@localhost] sudo su adminuser1 -c 'touch dir_test1/testfile'
[root@localhost] sudo su adminuser1 -c 'echo 123 > dir_test1/testfile'
```
3. The **anonymoususer** user should have no permission on the **dir_test1** directory.
```
[root@localhost] sudo su anonymoususer -c 'ls dir_test1'
ls: cannot open directory dir_test1: Permission denied
[root@localhost] sudo su anonymoususer -c 'cat dir_test1/testfile'
cat: dir_test1/testfile: Permission denied
```

----End

Follow-up Procedure

To remove the permissions of a user, you only need to remove the user from a specific group.

3.8.2 Configuring the NFS Kerberos Service

3.8.2.1 Overview

Kerberos is a computer network authentication protocol. It uses the client/server structure and encryption technologies (such as AES), and supports mutual authentication (that is, both the client and server can authenticate each other). It provides identity authentication for communication parties on the network to ensure authenticity and security of the communication.

NFS uses Kerberos to implement strong identity authentication and prevent unauthorized users from accessing NFS services. Kerberos supports encryption and signature to prevent tampering or disclosure of NFS data.

Application Scenarios

- Kerberos is to improve NFS security and applies to scenarios with high requirements on network security.
- Although Kerberos improves NFS security, enabling krb5 authentication, especially krb5 encryption and signature, affects performance. You can use it as required.

Basic Concepts

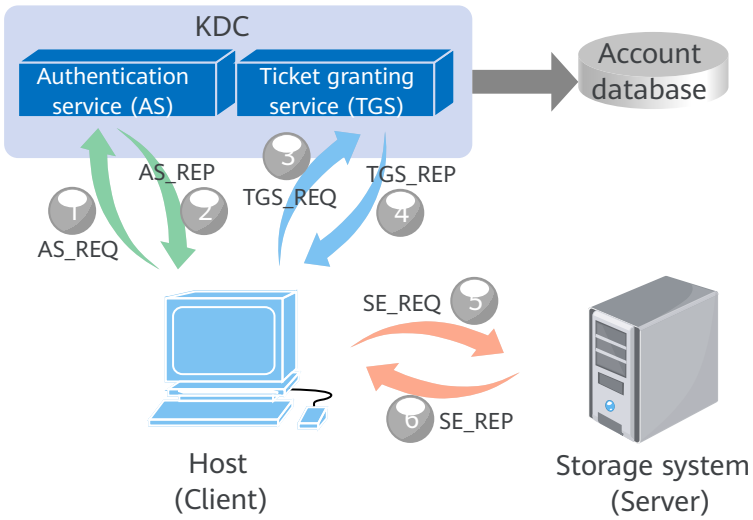
- Key distribution center (KDC): KDC is a service running on a secure server and maintains the account database of all principals in the Kerberos realm. KDC provides the following services:
  - Authentication service (AS): authenticates Kerberos clients based on the account database and issues a ticket granting ticket (TGT) to the clients.
  - Ticket granting service (TGS): verifies that a client is allowed to access the requested service and issues a service ticket. TGS acts as a trusted third party in the Kerberos protocol.
- Ticket granting ticket (TGT): an encrypted identification certificate with a limited validity period. A client uses the TGT to prove its identity to the TGS and obtain a service ticket from the TGS.

- Service ticket: an encrypted ticket from the client to the server. A client obtains a service ticket from the TGS after providing a valid TGT to the TGS.
- Kerberos realm: a network domain that a Kerberos authentication database is responsible for. The database stores all service principals and their keys in the network domain, which are used by the AS and TGS of Kerberos. Kerberos realm example: **TEST.EXAMPLE.COM**.
- Principal: a unique identifier for which the KDC can assign tickets. A principal can be a user or a service (for example, NFS). A principal consists of the name, instance, and Kerberos realm, for example, **nfs/ctest.jzb.com@JZB.COM**.
  - A principal name can be a user principal name (UPN) or service principal name (SPN), for example, **nfs**.
  - An instance is optional for a user principal and mandatory for a service principal. For a service principal, the instance is a fully qualified domain name (FQDN), for example, **ctest.jzb.com**.
  - A Kerberos realm defines a group of principals, similar to a DNS zone. An example of the Kerberos realm is **JZB.COM**.

Kerberos Authentication Principles

Kerberos authentication uses the KDC server to manage user information. The authentication information and data between the host and KDC and between the host and storage system can be signed or encrypted, ensuring secure authentication.

Figure 3-3 Kerberos authentication principles



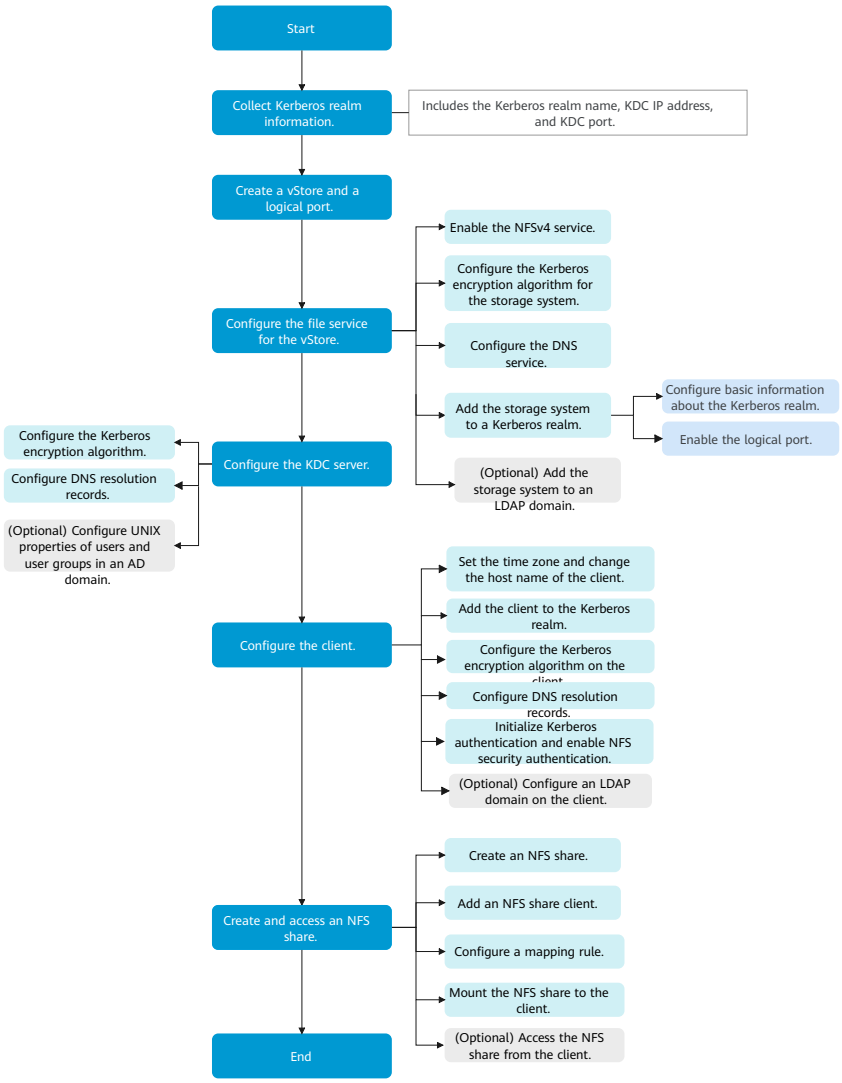
1. A client sends a TGT request in plaintext to the AS of the KDC.

2. After receiving the request from the client, the AS checks whether the client user name is in the whitelist of the Kerberos account database.
   - If not, the authentication fails.
   - If yes, the AS sends a TGT to the client, together with a session key for communication between the client and the TGS.
3. The client decrypts the session key returned by the AS and sends a request to the TGS for the service ticket.
4. The TGS decrypts the request, verifies the access permission of the client to the requested service, and sends a service ticket and a session key to the client. The session key is used for encrypted communication between the client and server.
5. The client sends an access request to the server and provides the service ticket and session key for the server.
6. The server verifies the validity of the service ticket and returns a service acknowledgement to the client. The client verifies the validity of the acknowledgement, and the mutual authentication between the client and the server is complete. Then the client can send service requests, and the server provides the requested service for the client.

3.8.2.2 Configuration Process

The Kerberos service must be configured on the storage system, KDC, and client. The following is a recommended configuration process.

Figure 3-4 Process for configuring the NFS Kerberos service



3.8.2.3 Collecting Kerberos Realm Information

Before adding a storage system to a Kerberos realm, collect configuration data of the Kerberos realm.

Prerequisites

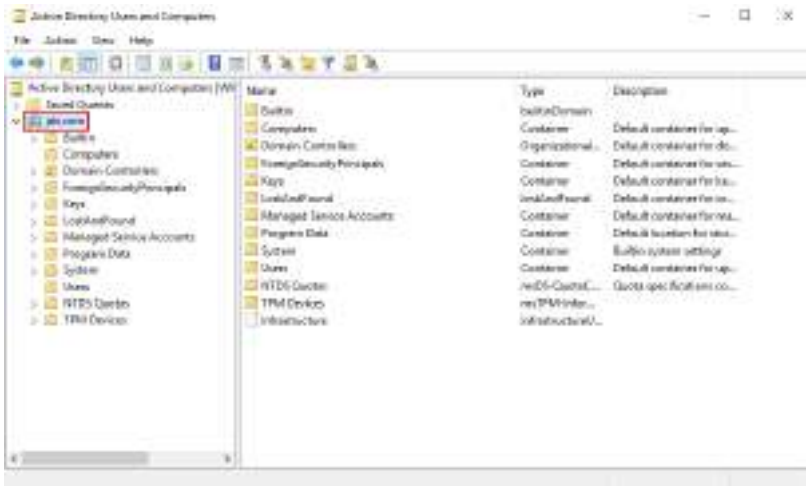
- A Kerberos realm has been set up.
- The administrator is familiar with the basic knowledge of the Kerberos realm, AD domain, and Linux.
- If the DNS and AD domain use different servers, the DNS server should have been added to the AD domain first. In this document, the DNS server and AD domain server are the same server.

Collecting Kerberos Realm Information

- Kerberos realm name

If the AD domain server is used as the KDC server, the Kerberos realm name is the AD domain name queried on the Active Directory Users and Computers tool.

Example: **jzb.com**

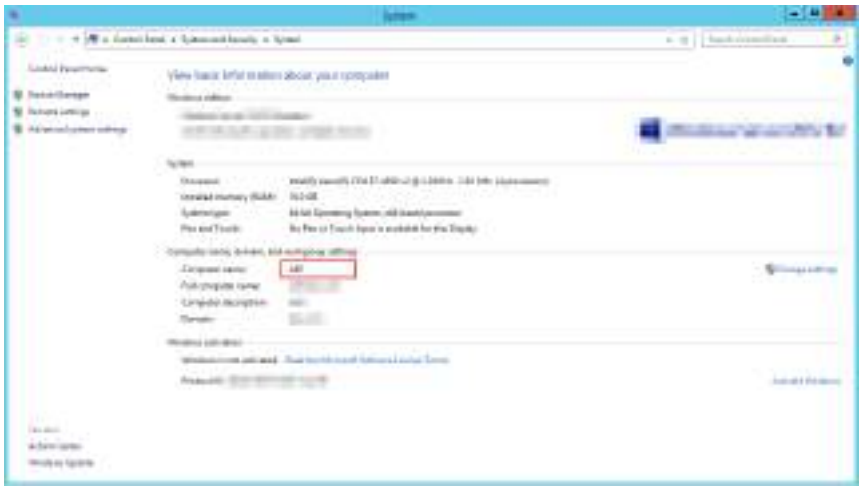


NOTE

This realm name must be in uppercase when you add a storage system to the Kerberos realm in **3.8.2.5.4 Adding the Storage System to a Kerberos Realm**.

- Device name of the KDC server

  Record the device name queried on the KDC server, for example, **AD1**.

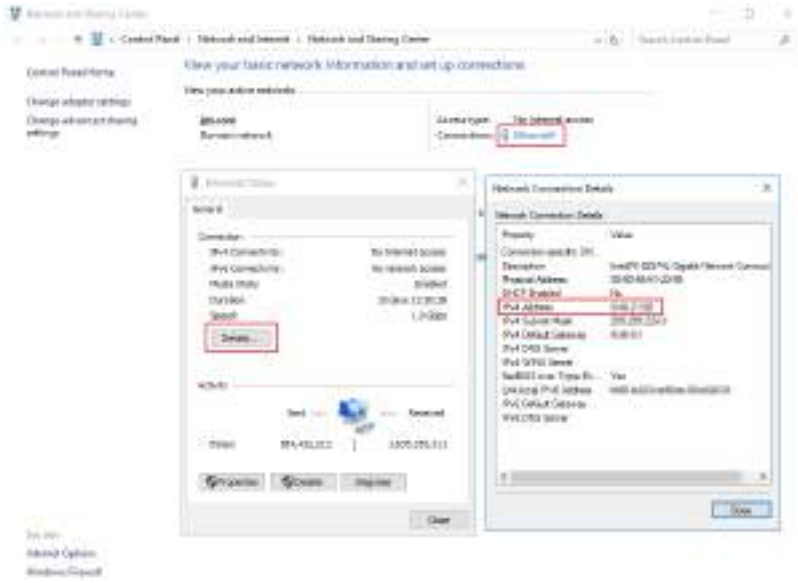


NOTE

The device name will be used when you configure the client.

- KDC IP address

  This is the management plane IP address of the server queried on the KDC server.



- KDC port

  Set the port number to 88.

- KDC vendor
  - If a Windows AD domain server is used as the KDC server, set the KDC vendor to Windows.
  - If a non-Windows AD domain server is used as the KDC server, set the KDC vendor to non-Windows.
- AD domain name

  If the KDC vendor is set to Windows, you must set the AD domain name. Currently, this name does not affect the configuration result.
- AD domain IP address

  If the KDC vendor is set to Windows, you must set the AD domain IP address. Currently, this IP address does not affect the configuration result.
- Kerberos realm user name and password

  If you enable or disable a logical port when adding a storage system to a Kerberos realm, you are required to enter the Kerberos realm user name and password to verify user permissions. Example of the Kerberos realm user name: **administrator**.

3.8.2.4 Creating a vStore and a Logical Port

Create a vStore to obtain storage services that are isolated from the resources and networks of other vStores. In addition, you must create a logical port that supports the NFS data protocol for the vStore. After the logical port is added to the Kerberos realm, the service principal name (SPN) of the NFS service is generated on the KDC, implementing the interaction between the storage system and KDC.

Prerequisites

Only the super administrator and administrators can create vStores.

Context

- Set **Role** of the logical port to **Service** and **Data Protocol** to **NFS** or **NFS + CIFS**.
- If a vStore already exists, skip this section and create a logical port for the vStore by referring to **3.8.1.4.4 Creating a Logical Port**.

Procedure

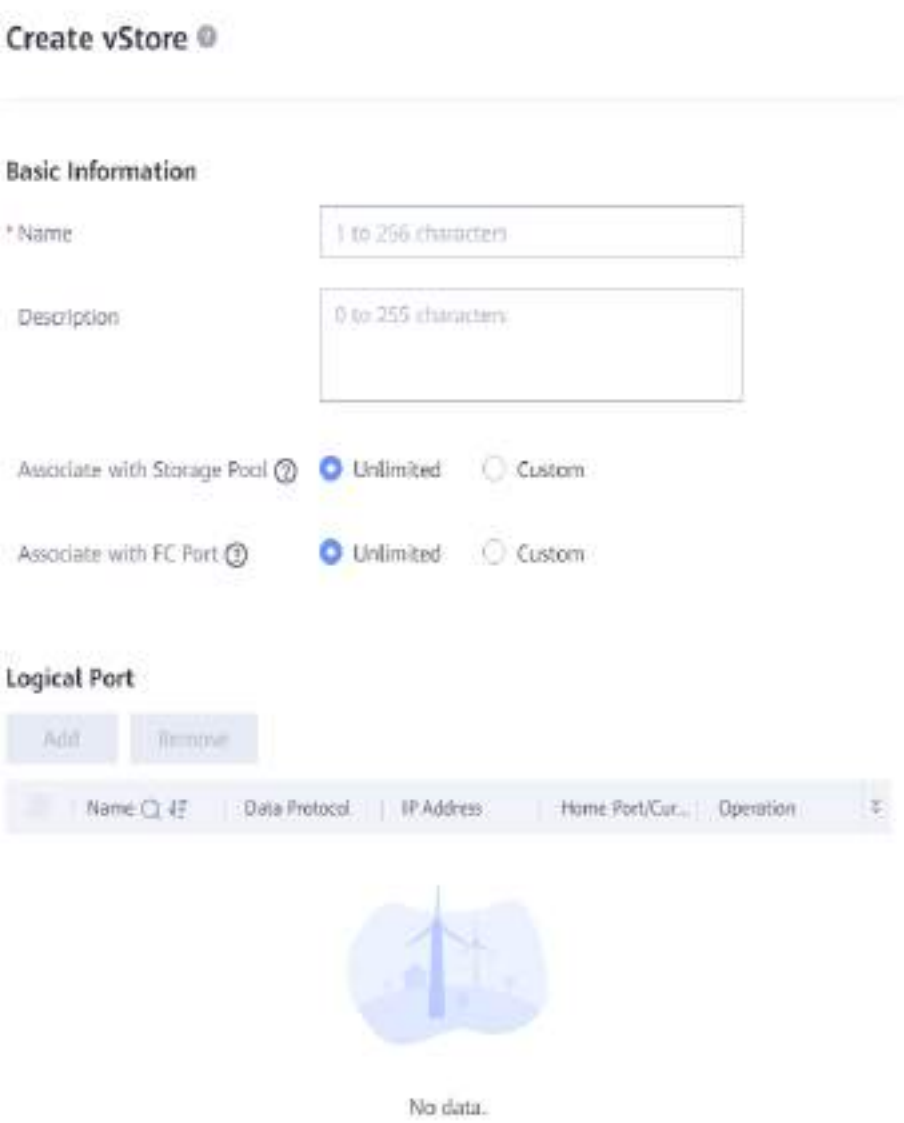
Step 1 Choose **Services** > **vStore Service** > **vStores**.

Step 2 Click **Create**.

The **Create vStore** page is displayed on the right.

NOTE

If you want to set a NAS capacity quota for a vStore during creation, use the **create vstore general** command on the CLI. After the capacity quota is set, the total file system capacity of the vStore cannot exceed the quota. For details on this command, refer to the *Command Reference*.



Step 3 Set vStore parameters.

Table 3-33 describes the parameters.

Table 3-33 vStore parameters

Parameter	Description
Name	Name of the new vStore. [Value range] • The name must be unique. • The name contains only letters, digits, periods (.), underscores (_), and hyphens (-). • The name contains 1 to 256 characters.

Parameter	Description
Description	Description of the vStore. [Value range] The description can be left blank or contain up to 255 characters.
Associate with Storage Pool	Select the storage pool associated with the vStore. The options are as follows: • **Unlimited**: The current vStore can use all storage pools. • **Custom**: The vStore can only use the selected storage pool. Click **Selected:** *X*. On the **Associate with Storage Pool** page that is displayed, select a storage pool.
Associate with FC Port	FC port associated with the vStore. The options are as follows: • **Unlimited**: The current vStore can use all FC ports. • **Custom**: The current vStore can only use the selected FC port. Click **Selected:** *X*. On the **Associate with FC Port** page that is displayed, select an FC port.

Step 4 Configure a management logical port for the vStore and a data logical port for communicating with the host.

1. Click **Add**.

   The **Create Logical Port** page is displayed.

2. Configure parameters for the logical port. **Table 3-34** describes the parameters.

Table 3-34 Logical port parameters

Parameter	Description
Name	Name of the logical port. To be compatible with the software, the name must meet the following requirements: – The name must be unique. – The name can contain only letters, digits, underscores (_), hyphens (-), and periods (.). – The name contains 1 to 255 characters.

Parameter	Description
Role	Role of the logical port. Possible options are: **Management**: A port of this role is used by a vStore administrator to log in to the system for management. **Service**: A port of this role is used to access services, such as accessing CIFS shares of file systems. **Management + service**: A port of this role is used to access services or for a vStore administrator to log in to the storage system for management.
Data Protocol	Data protocol of a logical port. Possible values are **NFS**, **CIFS**, **NFS + CIFS**, **iSCSI**, and **NVMe over RoCE**. **NOTE** **NFS**, **CIFS**, and **NFS + CIFS** are applicable to file service configuration. **iSCSI** and **NVMe over RoCE** are applicable to block service configuration.
IP Address Type	IP address type of the logical port. Possible options are **IPv4** and **IPv6**.
IP Address	IPv4 or IPv6 address of the logical port.
Subnet Mask	Subnet mask of the logical port's IPv4 address. **NOTE** This parameter is available only when **IP Address Type** is set to **IPv4**.
Prefix	Prefix length of the logical port's IPv6 address. **NOTE** This parameter is available only when **IP Address Type** is set to **IPv6**.
Gateway	Gateway of a logical port's IP address.
Port Type	Type of the port to which the logical port belongs. Possible options are **Ethernet port**, **Bond port**, and **VLAN**. **NOTE** This parameter is available only when **Data Protocol** is set to **NFS**, **CIFS**, **NFS + CIFS**, or **iSCSI**.
Home Port	Ethernet port, bond port, or VLAN to which the logical port belongs.
Activation Status	Determine whether to activate the logical port.

3. Select **Advanced** in the upper right corner to set the advanced attributes of the logical port.

   Table 3-35 describes the parameters.

Table 3-35 Advanced logical port parameters

Parameter	Description
Failover Group	Name of a failover group. **NOTE** – If a failover group is specified, services on the failed home port will be taken over by an available port in the specified failover group. – If no failover group is specified, services on the failed home port will be taken over by an available port in the default failover group.
IP Address Failover	After IP address failover is enabled, services on the failed home port will be taken over by other available ports in a failover group. In the entire process, the IP address used by services remains unchanged. **NOTE** Shares of file systems do not support the multipathing mode. They use IP address failover to improve the reliability of links.
Failback Mode	After the fault of the home port is rectified, services fail back to the home port. Possible values are **Automatic** and **Manual**. **NOTE** – If **Failback Mode** is **Manual**, ensure that the link to the home port is normal before the failback. You can manually switch services back to the home port only when the link to the home port keeps normal for over five minutes. – If **Failback Mode** is **Automatic**, ensure that the link to the home port is normal before the failback. Services will automatically fail back to the home port only when the link to the home port keeps normal for over five minutes.

4. Click **OK**.

   NOTE

   Select one or more logical ports and click **Remove** or click ⊖ on the right of a logical port to remove logical ports.

Step 5 Click **OK**.

NOTE

- After a vStore is created, you can select **Configure LDAP Domain**, **Configure File Service NIS Domain**, **Configure File Service AD Domain**, or **Create HyperMetro vStore Pair** as required on the operation success page.
- After a vStore is created, you can select it on other pages to manage its storage resources.

----End

3.8.2.5 Configuring the File Service for the vStore

After the vStore and logical port have been created, configure basic file services for the vStore, including the NFSv4 service, Kerberos encryption algorithm, DNS service, and adding the storage system to the Kerberos realm.

3.8.2.5.1 Enabling the NFSv4 Service

Only NFSv4.0 and NFSv4.1 support the Kerberos service. NFSv3 does not support the Kerberos service. Therefore, you must enable the NFSv4.0 or NFSv4.1 service for the vStore.

Prerequisites

A vStore exists in the system.

Context

- The storage system supports NFSv3, NFSv4.0, and NFSv4.1.
- The NFSv4.0 and NFSv4.1 services are disabled by default in the storage system.
- The NFSv4 service can be enabled on DeviceManager or on the CLI.

Enabling the NFSv4 Service on DeviceManager

Step 1 Choose **Settings** > **File Service** > **NFS Service**.

Step 2 In the **vStore** drop-down box in the upper left, select the vStore for which you want to enable the NFSv4 service.

Step 3 Click **Modify** in the upper right.

The page for configuring the NFS service is displayed.

NOTE

The screenshot is for reference only and the actual GUI may vary.

Step 4 Select **Enable** after **NFSv4.0 Service** or **NFSv4.1 Service** as required.

Step 5 In **Domain Name**, enter the storage domain name.

NOTE

- NFSv4.0 and NFSv4.1 use a user name + domain name mapping mechanism, enhancing the security of clients' access to shared resources.
- In a non-domain or LDAP environment, retain the default domain name **localdomain**.
- In an NIS environment, the entered information must be the same as the domain name in the **/etc/idmapd.conf** file on the Linux client that accesses the share. (You are advised to set both of them to the NIS domain name.)
- The domain name must contain 1 to 64 characters.
- Only 6.1.5 and later versions support domain name setting.

Step 6 Click **Save**.

A **Danger** dialog box is displayed.

NOTICE

If a host is accessing the shares of the storage system, enabling or disabling the NFS service may interrupt services. Exercise caution when performing this operation.

Step 7 Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation**.

Step 8 Click **OK**.

----End

Enabling the NFSv4 Service on the CLI

Step 1 Log in to the CLI of the storage system.

Step 2 **Optional:** To configure the NFSv4 service for a vStore, run the **change vstore view id=?** command to enter the vStore view.

You can run the **show vstore** command to query the value of **id**.

Step 3 Specify whether to enable the NFSv4.0 or NFSv4.1 service.

- To enable the NFSv4.0 service, run the **change service nfs_config nfsv40_status=enable** command.
- To enable the NFSv4.1 service, run the **change service nfs_config nfsv41_status=enable** command.

Step 4 Run the **show service nfs_config** command to check the running status of the NFSv4 service.

- The **Nfsv4.0 Service Status** field in the command output indicates the running status of the NFSv4.0 service of the current vStore.
- The **Nfsv41 Service Status** field in the command output indicates the running status of the NFSv4.1 service of the current vStore.

----End

3.8.2.5.2 Configuring the Kerberos Encryption Algorithm for the Storage System

Before configuring the Kerberos service, check the Kerberos encryption algorithm configured on the storage system. You can change the encryption algorithm if necessary.

Context

- The storage system supports the AES128, AES256, and DES3 encryption algorithms.
- The default Kerberos encryption algorithms of the storage system are AES128 and AES256. You are advised to retain the default values.
- The Kerberos encryption algorithm can be modified only on the CLI.

Precautions

- Changing the Kerberos encryption algorithm may interrupt services. Before the change, stop service operations to prevent exceptions caused by possible service interruption. The secure algorithms AES128 and AES256 are preferred.
- The DES3 algorithm has security risks. Exercise caution when using this algorithm.

Procedure

Step 1 Log in to the CLI of the storage system.

Step 2 Run the **show kerberos encrypt_types** command to query the Kerberos encryption algorithm configured on the storage system.

Example:

```
admin:/>show kerberos encrypt_types
  Supported Types : AES128,AES256
```

Step 3 **Optional:** Run the **change kerberos encrypt_types supported_types=***?* command to change the Kerberos encryption algorithm.

The **supported_types** field indicates the encryption algorithm, which can be a combination of AES128, AES256, or DES3.

NOTICE

- Changing the Kerberos encryption algorithm may interrupt services. Therefore, perform this operation only when necessary. Before the change, stop service operations to prevent exceptions caused by possible service interruption. The secure algorithms AES128 and AES256 are preferred.
- The DES3 algorithm has security risks. Exercise caution when using this algorithm.

Example:

Change the Kerberos encryption algorithm to AES128 and AES256.

```
admin:/>change kerberos encrypt_types supported_types=AES128,AES256
DANGER: You are about to change the NFS Kerberos encryption type.
```



```
This operation will change the encryption type supported by NFS Kerberos of the vStore, which may
interrupt services. The 3DES algorithm has security risks.
Suggestion: Before performing this operation, ensure that you want to change the encryption type. If yes,
preferentially select AES128 and AES256 algorithms which are more secure and stop service operations to
prevent service exceptions caused by service interruption.
Have you read danger alert message carefully?(y/n)y
Are you sure you really want to perform the operation?(y/n)y
Command executed successfully.
```

----End

3.8.2.5.3 Configuring the DNS Service

After a storage system is connected to a DNS server, the storage system can access the AD domain server using a domain name. This operation enables you to configure the IP address of the DNS service for the file storage service.

Prerequisites

- A DNS server has been configured and is running properly.
- Port 53 for the TCP/UDP protocol between the storage system and the DNS server is enabled.

Context

- A DNS server is used to resolve names of hosts in a domain.
- If you want to configure a standby DNS server, keep the domain names of the active and standby servers consistent.

Procedure

Step 1 Choose **Services** > **vStore Service** > **vStores**.

Step 2 Click the name of the desired vStore. On the details page that is displayed on the right, click the **File Service** tab and click **Configure** in the **DNS Service** area.

The **Configure DNS Service** page is displayed on the right.

Step 3 Configure an IP address for the DNS service.

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

   NOTE

   Set **Standby DNS IP Address 1** first and then **Standby DNS IP Address 2**.
4. (Optional) Test the connectivity between the DNS server and the storage system.
   - You can click **Test** next to a DNS IP address to test its availability.
   - You can click **Test All** to test the connectivity between the DNS server and the storage system.

Step 4 Set DNS domain names.

NOTE

Domain names are used in sequence. A maximum of six domain names are supported.

- Adding a domain name
  a. Click **Add**.
  b. Set a domain name.

  NOTE

  The domain name must comply with the following rules:

  - The domain name is case insensitive and must be unique.
  - The domain name contains 1 to 255 characters, including only letters (a to z and A to Z), digits (0 to 9), periods (.), underscores (_), and hyphens (-).
  - A domain name is separated by periods into several segments. Each segment cannot exceed 63 characters and must start or end with a letter or digit.
- Modifying a domain name
  a. Click the domain name to be modified.
  b. Set a domain name.

  NOTE

  The domain name must comply with the following rules:

  - The domain name is case insensitive and must be unique.
  - The domain name contains 1 to 255 characters, including only letters (a to z and A to Z), digits (0 to 9), periods (.), underscores (_), and hyphens (-).
  - A domain name is separated by periods into several segments. Each segment cannot exceed 63 characters and must start or end with a letter or digit.
- Removing a domain name

  Click on the right of the domain name to be deleted.
- Moving up a domain name

  Click on the right of the domain name to be moved up.
- Moving down a domain name

  Click on the right of the domain name to be moved down.

Step 5 Click **OK**. Confirm your operation as prompted.

----End

3.8.2.5.4 Adding the Storage System to a Kerberos Realm

Kerberos authentication depends on the KDC. Therefore, KDC information must be configured on the storage system, including the Kerberos realm name, KDC IP address, KDC port, and KDC vendor (Windows or non-Windows). If the AD domain is used as the KDC, you must also configure the AD domain name and IP address.

Prerequisites

- A Kerberos realm environment has been set up.

- The Kerberos realm server has time synchronization with the storage system. The time difference must be no larger than 5 minutes.
- Port 88 (TCP/UDP protocol) between the storage system and the Kerberos realm is enabled.

Context

- Collect the Kerberos realm information by referring to **3.8.2.3 Collecting Kerberos Realm Information**. Perform the follow-up configuration after all information has been collected.
- For details about the service principals, see **Basic Concepts**.

Precautions

- The client to be authenticated and the storage system must be added to the same Kerberos realm.
- Before adding a storage system to a Kerberos realm, ensure that the primary controller of the storage system is connected to the Kerberos realm server.
- If **Overwrite Service Principal Name** is enabled and the entered service principal name is the same as an existing name on the domain controller, the logical port information of the current storage system will overwrite the existing service principal information on the domain controller.

Procedure

Step 1 Choose **Services** > **vStore Service** > **vStores**.

Step 2 Click the name of a desired vStore. The details page is displayed on the right. In the **File Service** tab page, click **Add** in the **Kerberos Realms** area.

The **Add Kerberos Realm** page is displayed on the right.

Step 3 Configure basic information. **Table 3-36** describes the parameters.

Table 3-36 Basic information about the Kerberos realm

Parameter	Description
Realm Name	Kerberos realm name. If the AD domain server is used as the KDC server, the Kerberos realm name is the AD domain name queried on the Active Directory Users and Computers tool. [Rule] Letters contained in a realm name must be uppercase. [Example] JZB.COM
KDC IP Address	IP address of the Kerberos key distribution center (KDC). [Example] 192.168.1.11

Parameter	Description
KDC Port	Port number of the Kerberos KDC. [Rule] Use port 88. [Example] 88
KDC Vendor	Vendor of the Kerberos KDC. • If a Windows AD domain server is used as the KDC server, set **KDC Vendor** to **Windows**. • If a non-Windows AD domain server is used as the KDC server, set **KDC Vendor** to **Non-Windows**. [Example] Windows
Kerberos Realm Username	User name for logging in to the Kerberos realm server. [How to obtain] Contact the Kerberos realm administrator to obtain the value. [Example] administrator **NOTE** This parameter needs to be set when a logical port is enabled or disabled.
Password	Password for logging in to the Kerberos realm server. [How to obtain] Contact the Kerberos realm administrator to obtain the password. **NOTE** This parameter needs to be set when a logical port is enabled or disabled.

Step 4 Enable the Kerberos service of the logical port.

1. Click **Enable**.

   The **Enable Logical Port** page is displayed.
2. Select the logical port to be enabled from the **Logical Port** drop-down list.
3. Set the **Service Principal Name** (SPN) of the logical port to identify a unique identity in the Kerberos realm. An SPN is the name of the logical port of the storage system in the Kerberos realm. After the name is set, the client can use the name to access the storage system.

NOTE

- An SPN is in the format of nfs/FQDN@Kerberos realm name.
- If the entered SPN already exists in the domain controller and **Overwrite Service Principal Name** is not enabled, the logical port will fail to be enabled.
- Special characters ~!$%^&{}`' are not recommended because the realm name of the DNS server does not support these characters.

4. Determine whether to enable **Overwrite Service Principal Name**. If a device with the same SPN already exists in the domain controller, the original SPN will be overwritten after this function is enabled.

NOTICE

After this function is enabled, the information about the logical port with the same SPN in the domain controller will be overwritten. As a result, the authentication between the domain controller and the device to which the logical port belongs will be affected.

5. Click **OK**.
6. If **KDC Vendor** is set to **Non-Windows**, upload a **.keytab** key file after the Kerberos service of the logical port is enabled.

NOTE

Select a port and click **Remove** or choose **More** > **Remove** on the right of the port to remove the logical port and disable the Kerberos service of the logical port.

To upload the .keytab file, perform the following steps:

a. Log in to the CLI as an administrator or a super administrator.

b. Run the **change vstore view name=?** command to switch to the vStore view. To obtain the value of **name**, run the **show vstore** command without parameters. Example:

```
admin:/>change vstore view name=nfstest
Command executed successfully.
```

c. Run the **import kerberos keytab ip=? user=? password=? spn=? lif_name=? keytab_path=? [protocol=?] [port=?]** command to import the .keytab file to the storage system. Example:

```
admin@nfstest:/>import kerberos keytab ip=10.133.194.20 user=admin password=****** spn=nfs/test.ad.com@AD.COM lif_name=test_ip keytab_path=krb5.keytab protocol=SFTP port=22
Command executed successfully.
```

NOTE

Ensure that the .keytab file has been uploaded to the FTP or SFTP server that can communicate with the storage system.

Table 3-37 Description

Parameter	Description
ip=?	IP address of a File Transfer Protocol (FTP) or Secure File Transfer Protocol (SFTP) server.

Parameter	Description
user=?	User name for the FTP or SFTP server. [Value range] The value contains 1 to 64 characters without colons (:).
password=?	Password for the FTP or SFTP server, which is displayed as asterisks (*). [Value range] The value contains 1 to 64 characters.
spn=?	SPN specified when joining the Kerberos realm. [Value range] The value consists of nfs/, FQDN, @, and the Kerberos realm name. An FQDN contains 1 to 128 characters and cannot contain @#*()=+[]|;:",<>\/? or control characters. Characters such as ~!$ %^&{}`' are not recommended. The Kerberos realm name is a string of 1 to 256 characters. It starts with a digit or uppercase letter and consists of digits, uppercase letters, and the following characters: ._- The value cannot contain a period before or after an underscore (_. or ._) or consecutive periods (..).
lif_name=?	Name of the logical IP address. [Value range] The value contains 1 to 256 characters.
keytab_path=?	Path of the Kerberos keytab file on the FTP or SFTP server. The file name extension must be .keytab. [Value range] Character string that ends with .keytab.

Parameter	Description
protocol=?	File transfer protocol used for transferring the .keytab file. [Value range] The value can be **FTP** or **SFTP**. The default value is **SFTP**. To ensure the security of data transfer, you are advised to use SFTP.
port=?	Port number of the FTP or SFTP server. [Value range] The value is an integer from 1 to 65535. ■ If **protocol** is set to **FTP**, the default value is **21**. ■ If **protocol** is set to **SFTP**, the default value is **22**.

Step 5 Click **OK**.

Confirm your operation as prompted.

----End

Follow-up Procedure

After the storage system has been added to the Kerberos realm, a computer name corresponding to the SPN of the logical port is generated on the KDC server.

Query and record this computer name on the KDC server for subsequent configurations on the KDC server.

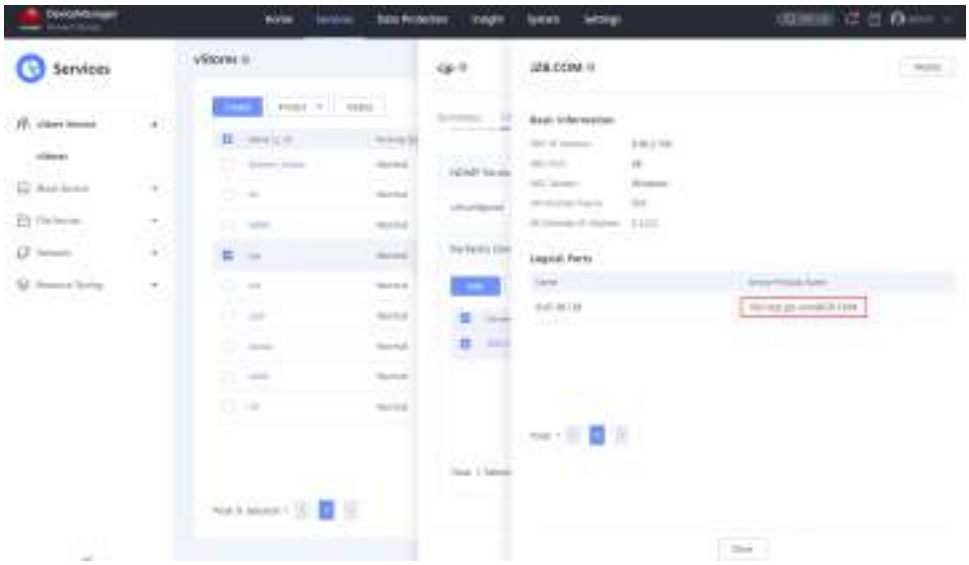
NOTE

The computer name generated on the KDC is a conversion of the principal name and instance part of the SPN configured on the storage system.

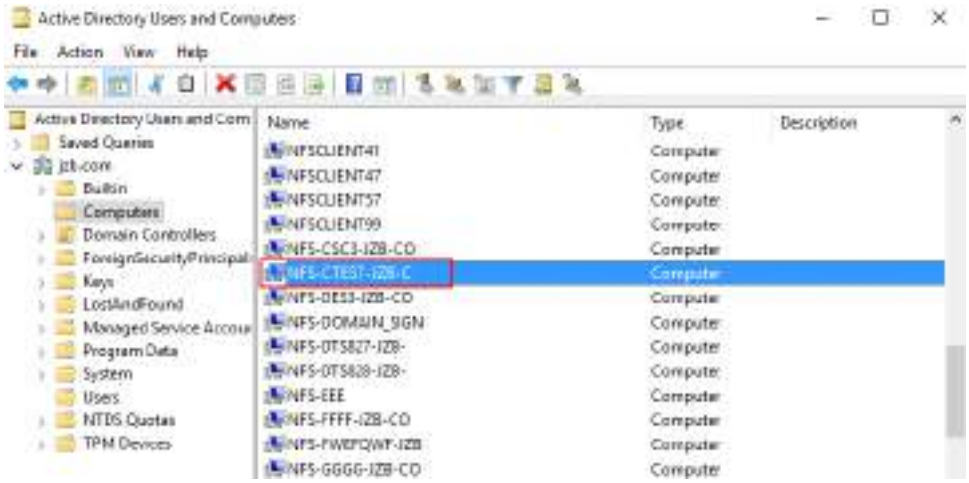
- Lowercase letters are converted to uppercase letters.
- Slashes (/) and periods (.) are converted to hyphens (-).
- Due to the limitation of the KDC server, the maximum length of the computer name is 16 characters.

The following is an example:

- Assume that the SPN of the logical port configured on the storage system is **nfs/ctest.jzb.com@JZB.COM**.



- The computer name generated on the KDC server is **NFS-CTEST-JZB-C**.



3.8.2.5.5 (Optional) Adding the Storage System to an LDAP Domain

To use an LDAP domain user, you must add the storage system to an LDAP domain. For details, see **3.8.1.6 (Optional) Adding the Storage System to an LDAP Domain**.

NOTE

This document describes the configuration of the NFS Kerberos service. LDAP domain users use the LDAP service provided by the AD domain.

3.8.2.6 Configuring the KDC Server

After the configurations on the storage system are complete, set the Kerberos encryption algorithm on the KDC for the storage system and configure resolution records on the DNS.

NOTE

On the KDC server, set the Kerberos encryption algorithm for the client and configure DNS resolution records. For details, see **3.8.2.7 Configuring the Client**.

3.8.2.6.1 Configuring the Kerberos Encryption Algorithm

To ensure the communication between the storage system and the KDC server, configure the Kerberos encryption algorithm of the storage system on the KDC server.

Prerequisites

You have recorded the computer name generated on the KDC server after adding the storage system to the Kerberos realm. For details, see **Follow-up Procedure**.

Procedure

Step 1 Open the command line tool (for example, Windows PowerShell) of the KDC server.

Step 2 Run the **Set-ADComputer** *Computer_Name* **-KerberosEncryptionType AES128,AES256** command to set the Kerberos encryption algorithm of the storage system.

Computer_Name is the computer name generated on the KDC server after the storage system has been added to the Kerberos realm.

NOTE

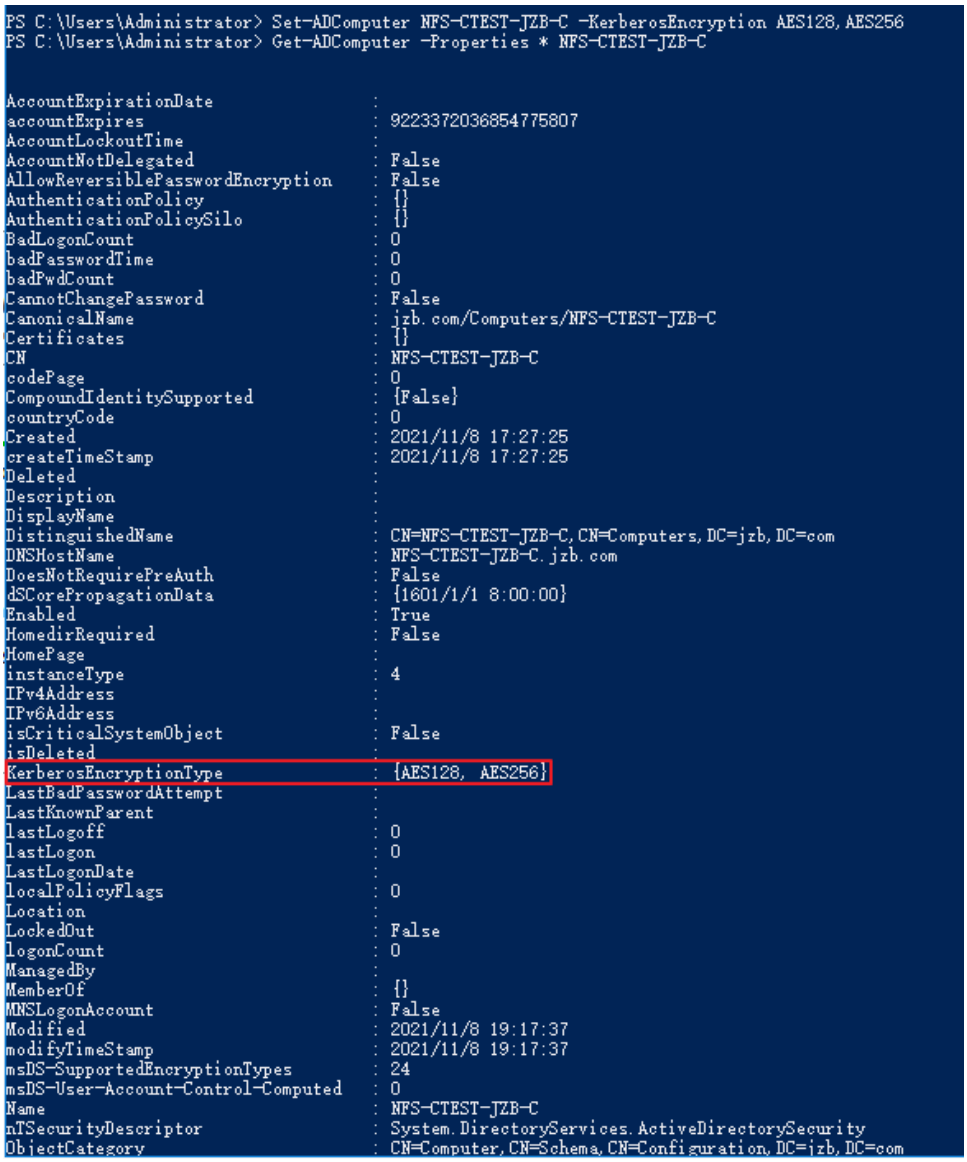
- Refer to **Follow-up Procedure** to check the computer name generated on the KDC server, for example, **NFS-CTEST-JZB-C**.
- At least one of the Kerberos encryption algorithms configured on the KDC server must be the same as that configured in **3.8.2.5.2 Configuring the Kerberos Encryption Algorithm for the Storage System**.

Example:

```
Set-ADComputer NFS-CTEST-JZB-C -KerberosEncryptionType AES128,AES256
```

Step 3 Run the **Get-ADComputer -Properties *** *Computer_Name* command and check the **KerberosEncryptionType** field in the command output, which is the Kerberos encryption algorithm configured on the KDC server.

Example:



----End

3.8.2.6.2 Configuring DNS Resolution Records

After the Kerberos service has been enabled for the logical port on the storage system, you must manually create a resolution record on the DNS server corresponding to the logical port.

Prerequisites

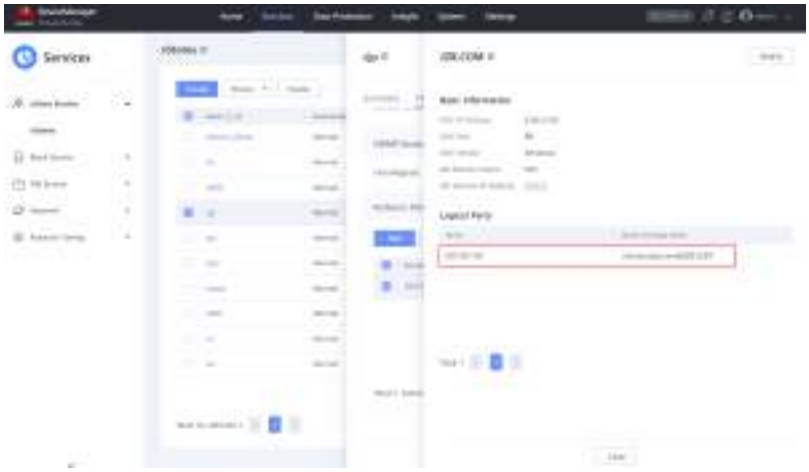
The Kerberos service has been enabled for the logical port on the storage system in **3.8.2.5.4 Adding the Storage System to a Kerberos Realm**.

Context

You can use either of the following methods to check whether the Kerberos service has been enabled for the logical port on the storage system:

- On DeviceManager:

  Click the Kerberos realm name of the vStore. If the logical port name and service principal name are displayed on the details page of the Kerberos realm, the Kerberos service has been enabled for the logical port.

- On the CLI:

  In the vStore view, run the **show kerberos interface** command. If the command output includes the logical port and SPN, the Kerberos service has been enabled for the logical port.

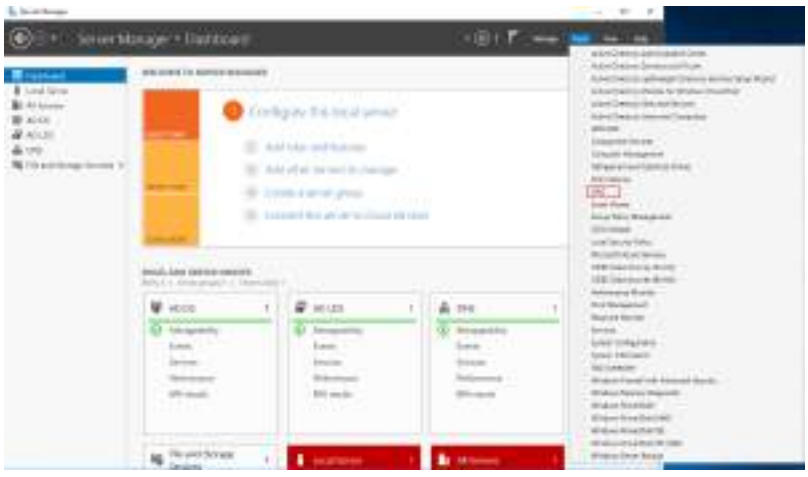
```
admin@cjp:/>show kerberos interface
  Lif Name : lif-zxl
  Spn      : nfs/ctest.jzb.com@JZB.COM
```

Precautions

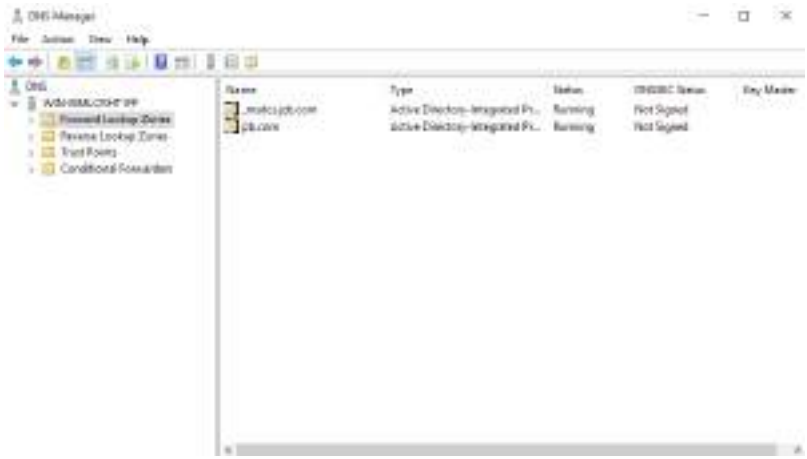
If the Kerberos service is disabled for the logical port on the storage system, delete the resolution record from the DNS server. For details, see **Follow-up Procedure**.

Procedure

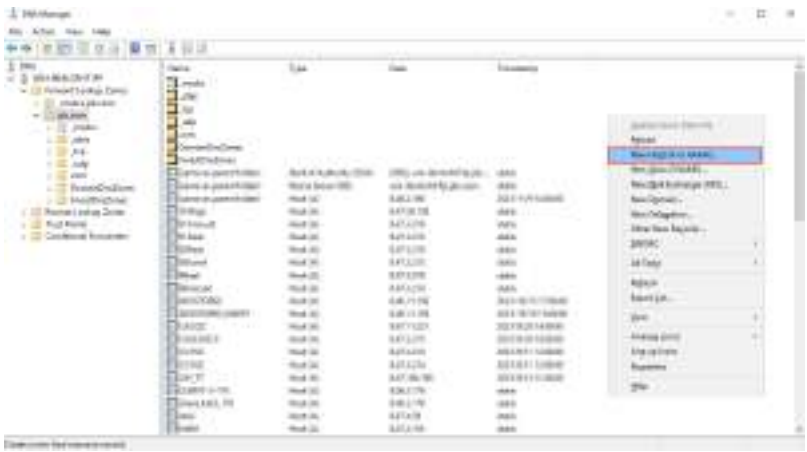
Step 1 Log in to the DNS server and open the DNS management tool of the KDC server.



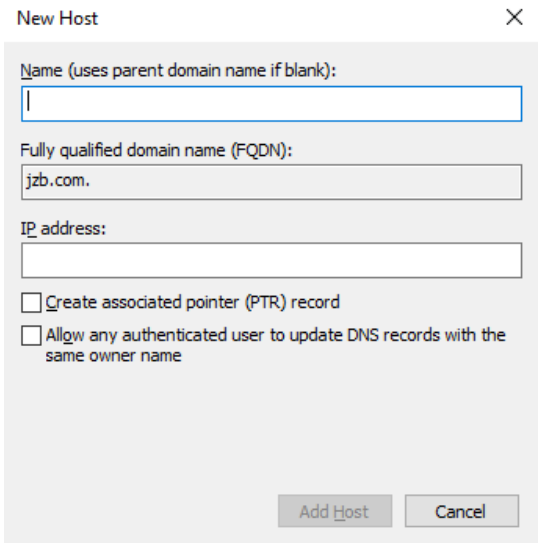
The **DNS Manager** page is displayed.



Step 2 On the **DNS Manager** page, click **Forward Lookup Zones** and select a domain name, for example, **jzb.com**. Right-click in the blank area on the right and choose **New Host (A or AAAA)** from the shortcut menu.



The **New Host** dialog box is displayed.

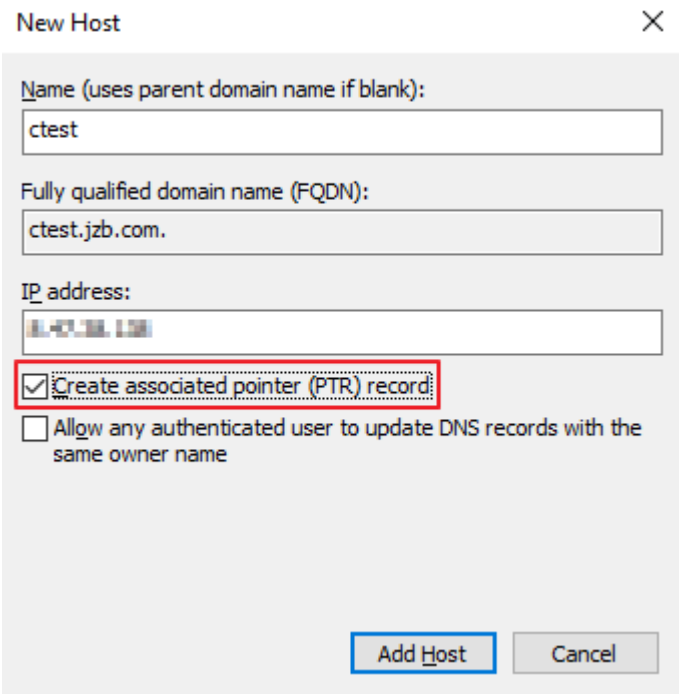


Step 3 Set the parameters correctly.

Assume that the SPN of the logical port configured on the storage system is **nfs/ctest.jzb.com@JZB.COM**.

Set the parameters as follows:

- Name: host name, for example, **ctest**.
- **Fully qualified domain name (FQDN)**: automatically generated based on the **Name** parameter and domain name. This value is the same as the instance name of the logical port SPN on the storage system, for example, **ctest.jzb.com**.
- **IP address**: IP address of the logical port on the storage system.
- **Create associated pointer (PTR) record**: Select this option to ensure that the DNS can generate forward and reverse resolution records.



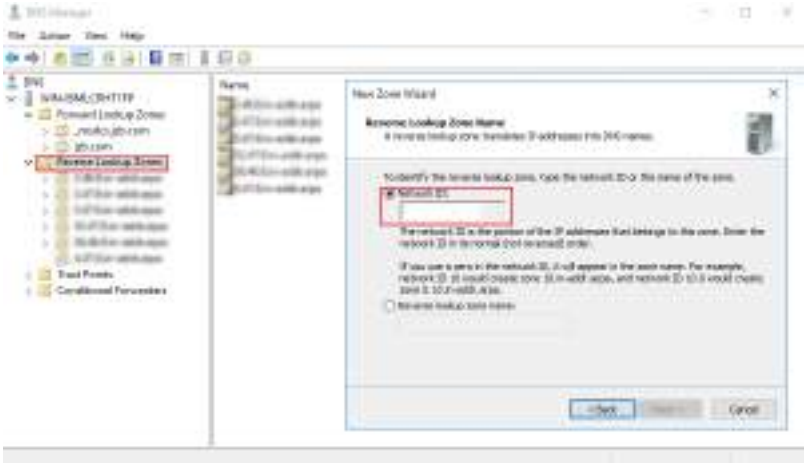
Step 4 Click **OK**.

The system displays a message indicating that the record is created successfully.

NOTE

If the system displays a message indicating that the creation fails, as shown in the following figure, check whether a zone in **Reverse Lookup Zones** is on the same network segment as the logical port of the storage system.

If not, create a zone on the same network segment as the logical port in **Reverse Lookup Zones** and then create a DNS resolution record again.



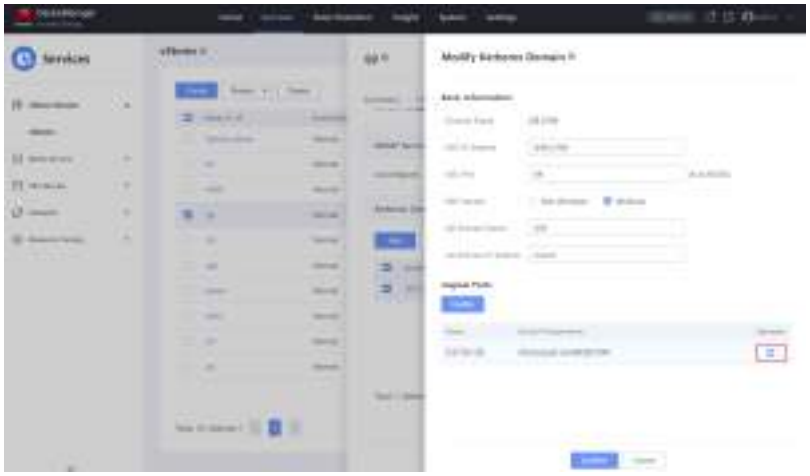
----End

Follow-up Procedure

When the Kerberos service is disabled for the logical port on the storage system, you must manually delete the resolution record from the DNS server.

You can disable the Kerberos service of the logical port in either of the following ways:

- On DeviceManager:



- On the CLI:

  In the vStore view, run the **change kerberos interface lif_name=? status=close spn=? admin_name=? passwd=?** command to disable the Kerberos service of the logical port.

```
admin@cjp:/>show kerberos interface
  Lif Name : lif-zxl
  Spn      : nfs/ctest.jzb.com@JZB.COM
admin@cjp:/>change kerberos interface lif_name=lif-zxl status=close admin_name=admin
passwd=*********
DANGER: You are about to disable the Kerberos service on the LIF.
This operation may interrupt services.
Suggestion: Ensure that you want to perform this operation.
Have you read danger alert message carefully?(y/n)y
Are you sure you really want to perform the operation?(y/n)y
Command executed successfully.
admin@cjp:/>show kerberos interface
Command executed successfully.
No matching records.
```

3.8.2.6.3 (Optional) Configuring the UNIX Properties of Users and User Groups in an AD Domain

To use LDAP domain users, you must configure the UNIX properties of the users and user groups in an AD domain.

NOTE

This document describes the configuration of the NFS Kerberos service. LDAP domain users use the LDAP service provided by the AD domain.

Procedure

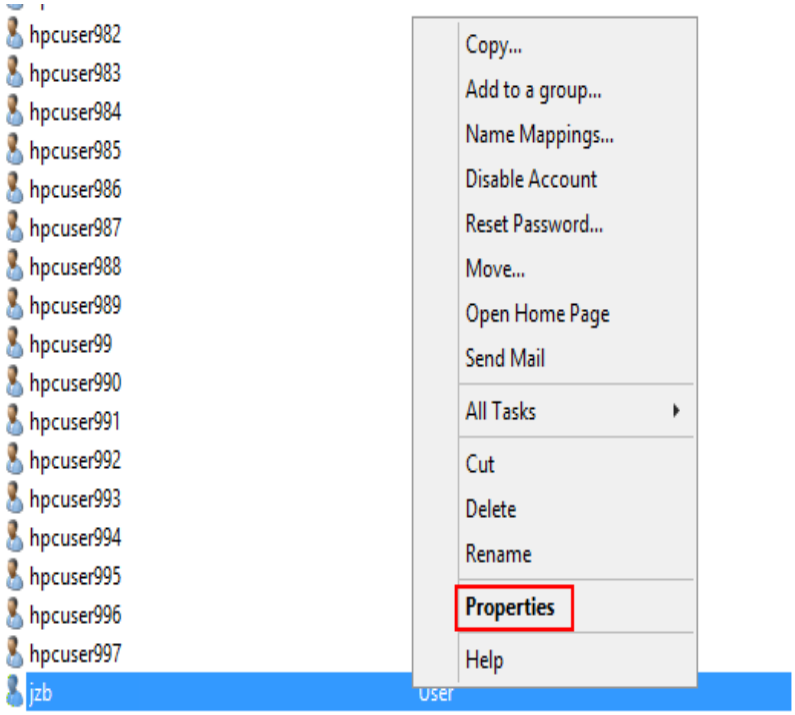
Step 1 Open **Active Directory Users and Computers** and choose **View** > **Advanced Features**.

Step 2 Configure the UNIX properties of users.

1. Double-click the user name for which you want to configure UNIX properties.

NOTE

Alternatively, you can right-click a user name (for example, **jzb**) and choose **Properties** from the shortcut menu.

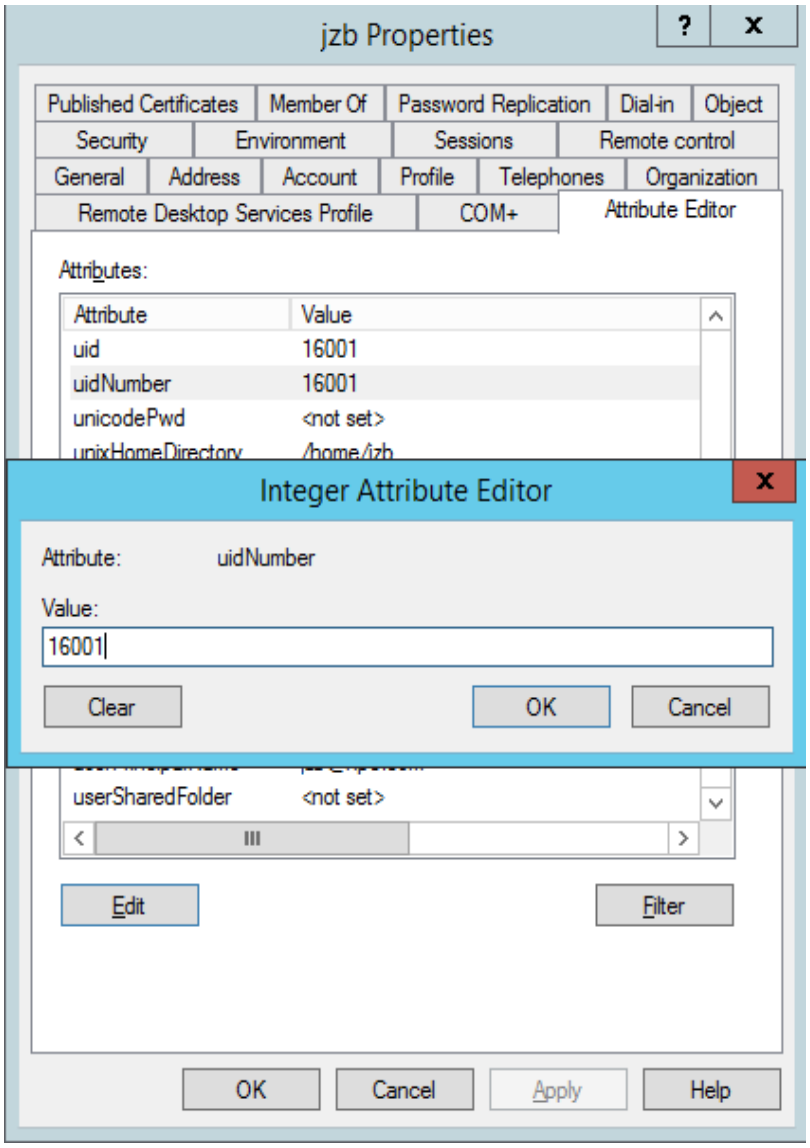


2. In the user properties window, click **Attribute Editor**.

   The user properties to be configured are **uid**, **uidNumber**, **unixHomeDirectory**, **gidNumber**, and **loginshell**. You can double-click the names of the properties to modify them.

   NOTE

   Alternatively, you can select a property name and click **Edit** to modify it.



Step 3 Configure the UNIX properties of user groups.

1. Double-click the user group name for which you want to configure UNIX properties.

   NOTE

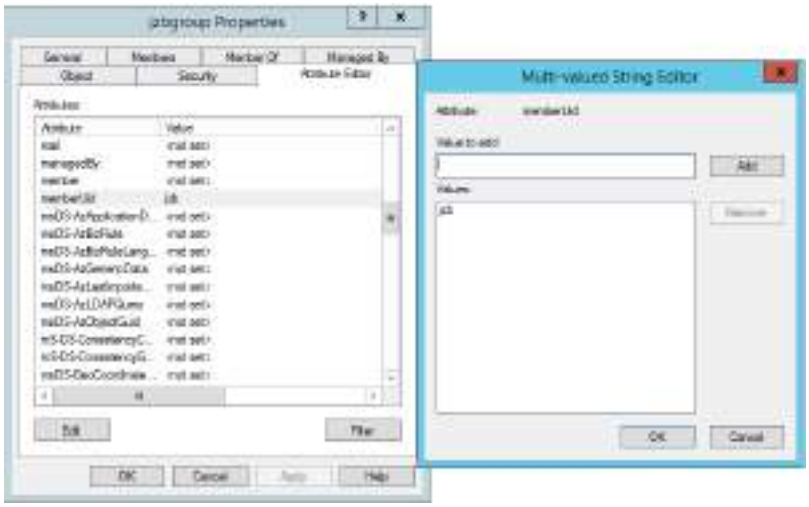
   Alternatively, you can right-click a user group name and choose **Properties** from the shortcut menu.

2. Click **Attribute Editor**.

   The user group properties to be configured are **gidNumber** and **memberUid**. You can double-click the names of the properties to modify them.

   NOTE

   Alternatively, you can select a property name and click **Edit** to modify it.



----End

3.8.2.7 Configuring the Client

The client configuration varies with the OS. The following uses SUSE and CentOS as examples. The configuration of other OSs is similar.

3.8.2.7.1 SUSE Client

On a Linux client, you must set the time zone of the client, change the host name of the client, add the client to the Kerberos realm, configure the Kerberos encryption algorithm for the client, configure DNS resolution records, initialize Kerberos authentication, and enable NFS security authentication. The following uses a SUSE client as an example.

Procedure

Step 1 Install the Zypper management software package on the client to facilitate the installation of Samba and Kerberos components.

NOTE

You can run the **zypper lr** command to check whether the Zypper source has been installed on the client. If the Zypper management software package has been installed on the client, skip this step.

Example:

```
linux-xvat:~ # zypper lr
Repository priorities are without effect. All enabled repositories share the same priority.
# | Alias             | Name              | Enabled | GPG Check | Refresh
--+-------------------+-------------------+---------+-----------+--------
1 | SLES12-SP5-12.5-0 | SLES12-SP5-12.5-0 | Yes     | (r ) Yes  | No
```

1. Use the FTP tool to copy the SUSE ISO image file to the **/mnt/iso** directory on the client.
2. Mount the ISO image file to the **/mnt/iso** directory.

   Example:

   ```
   linux-xvat:mount -o loop /mnt/iso/SLE-12-SP5-Server-DVD-x86_64-GM-DVD1.iso /mnt/iso/
   mount: /dev/loop0 is write-protected, mounting read-only
   ```


3. Configure the Zypper.

```
linux-xvat:~ # zypper ar file:///mnt/iso/ local-sles
Adding repository 'local-sles' ..........[done]
Repository 'local-sles' successfully added
URI         : file:/mnt/iso/
Enabled     : Yes
GPG Check   : Yes
Autorefresh : No
Priority    : 99 (default priority)
Repository priorities are without effect. All enabled repositories share the same priority.
```

4. Delete the local Zypper source and clear the cache.

```
linux-xvat:~ # zypper lr
Repository priorities are without effect. All enabled repositories share the same priority.
# | Alias              | Name               | Enabled | GPG Check | Refresh
--+--------------------+--------------------+---------+-----------+--------
1 | SLES12-SP5-12.5-0 | SLES12-SP5-12.5-0 | Yes     | (r ) Yes  | No
2 | local-sles         | local-sles         | Yes     | ( p) Yes  | No
linux-xvat:~ # cd /etc/zypp/repos.d/
linux-xvat:/etc/zypp/repos.d # ll
total 4
-rw-r--r-- 1 root root 172 Sep  2 22:48 SLES12-SP5-12.5-0.repo
-rw-r--r-- 1 root root   0 Nov  9 17:53 local-sles.repo
linux-xvat:/etc/zypp/repos.d # rm -rf SLES12-SP5-12.5-0.repo
linux-xvat:/etc/zypp/repos.d # zypper clean
All repositories have been cleaned up.
linux-xvat:/etc/zypp/repos.d # zypper ref
Retrieving repository 'local-sles' metadata ----------------------------------------
Wadning: The gpg key signing file 'content' has expired.
  Repository:local-sles
  Key Name:          Suse Package Signing Key <build@suse.de>
  Key Fingerprints:  FEAB5025 XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX
  Key Created:       Wed Dec  7 18:57:35 XXXX
  Key Expires:       Sun Dec  7 18:57:35 XXXX
  Rpm Name:          gpg-pubkey-xxxxxxxx-xxxxxxxx
Retrieving repository 'local-sles' metadata ----------------------------------------
Building Repository 'local-sles' cache ---------------------------------------
All repositories have been refreshed.
```

Step 2 Change the time zone and time of the client to be consistent with those of the Kerberos realm controller server. The maximum time difference is 5 minutes.

Step 3 Change the host name of the client, for example, **CLIENT_112_70**. The host name of the client can be used to configure DNS resolution records. Restart the client for the modification to take effect.

```
vi /etc/hostname
export HOSTNAME=CLIENT_112_70
/etc/rc.d/boot.local start
```

Step 4 Add the client to the Kerberos realm. The Windows AD domain is used as an example.

1. Run the **zypper -n install samba-winbind** command to install the Samba-Winbind component.
2. Run the **vi /etc/krb5.conf** command to configure the **krb5.conf** file.

   The following is an example of the **krb5.conf** file content. Replace the information in bold with the domain name of the AD domain. **AD1** must be replaced with the device name of the KDC server.

```
[libdefaults]
    default_realm = JZB.COM
    clockskew = 300
    forwardable = false
    proxiable = false
    noaddress = false
    dns_lookup_realm = true
    dns_lookup_kdc = true
```



```
    allow_weak_crypto = false
    default_keytab_name = /etc/krb5.keytab
    default_tgs_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 des3-cbc-sha1 arcfour-
hmac-md5 camellia256-cts-cmac camellia128-cts-cmac des-cbc-crc des-cbc-md5 des-cbc-md4
    default_tkt_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 des3-cbc-sha1 arcfour-
hmac-md5 camellia256-cts-cmac camellia128-cts-cmac des-cbc-crc des-cbc-md5 des-cbc-md4
    permitted_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 des3-cbc-sha1 arcfour-
hmac-md5 camellia256-cts-cmac camellia128-cts-cmac des-cbc-crc des-cbc-md5 des-cbc-md4


[logging]
    kdc = FILE:/var/log/krb5/krb5kdc.log
    admin_server = FILE:/var/log/krb5/kadmind.log
    default = SYSLOG:NOTICE:DAEMON

[realms]
        JZB.COM = {
                kdc = AD1.jzb.com
                admin_server = AD1.jzb.com
                master_kdc = AD1.jzb.com
        }

[domain_realm]
    .JZB.COM = JZB.COM
    JZB.COM = JZB.COM
[appdefaults]
    pam = {
        ticket_lifetime = 1d
        renew_lifetime = 1d
        forwardable = true
        proxiable = false
        minimum_uid = 1
    }
```

3. Run the **vi /etc/resolv.conf** command to configure the DNS.

   The following is an example. **nameserver** is the IP address of the DNS server, and **search** is the AD domain name.

   ```
   nameserver x.x.x.x
   search jzb.com
   ```

4. Run the **vi /etc/samba/smb.conf** command to configure the **samba.conf** file.

   The following is an example of the **samba.conf** file content. Replace the information in bold with the AD domain name.

   ```
   # smb.conf is the main Samba configuration file. You find a full commented
   # version at /usr/share/doc/packages/samba/examples/smb.conf.SUSE if the
   # samba-doc package is installed.
   [global]
       workgroup = JZB.COM
       usershare allow guests = NO
       idmap config * : backend = tdb
       idmap config * : range = 1000000-1999999
       idmap config ADSERVER155 : backend = rid
       idmap config ADSERVER155 : range = 5000000-5999999
       kerberos method = secrets and keytab
       realm = JZB.COM
       security = ADS
       template homedir = /home/%D/%U
       template shell = /bin/bash
       winbind offline logon = yes
       winbind refresh tickets = yes
   [homes]
       comment = Home Directories
       valid users = %S, %D%w%S
       browseable = No
       read only = No
       inherit acls = Yes
   [profiles]
       comment = Network Profiles Service
   ```



```
    path = %H
    read only = No
    store dos attributes = Yes
    create mask = 0600
    directory mask = 0700
[users]
    comment = All users
    path = /home
    read only = No
    inherit acls = Yes
    veto files = /aquota.user/groups/shares/
[groups]
    comment = All groups
    path = /home/groups
    read only = No
    inherit acls = Yes
[printers]
    comment = All Printers
    path = /var/tmp
    printable = Yes
    create mask = 0600
    browseable = No
[print$]
    comment = Printer Drivers
    path = /var/lib/samba/drivers
    write list = @ntadmin root
    force group = ntadmin
    create mask = 0664
    directory mask = 0775
```

5. Run the **vi /etc/nsswitch.conf** command to configure the **nsswitch.conf** file.

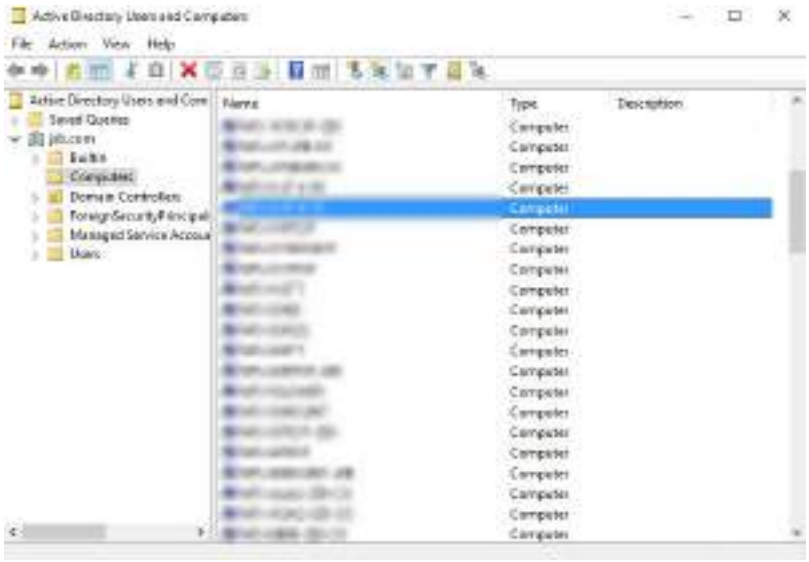
   The following is an example of the **nsswitch.conf** file content.

```
passwd:    compat winbind
group:    compat winbind
shadow: compat winbind

hosts:    files dns
networks:    files dns

services:    files nis
protocols:    files
rpc:    files
ethers:    files
netmasks:    files
netgroup:    files nis
publickey:    files

bootparams:    files
automount:    files nis ldap
aliases:    files nis
sudoers:    ldap
shadow:    compat
```

6. Run the **net ads join -U administrator** command to add the client to the AD domain.

```
linux-xvat:net ads join -U administrator
Enter administrator's password:
Using short domain name -- JZB
Joined 'linux-xvat' to dns domain 'jzb.com'
No DNS domain configured for linux-xvat. Unable to perform DNS Update.
DNS update failed: NT_STATUS_INVALID_PARAMETER
```

   After the client has been added to the AD domain, you can view the added computer name in the AD domain.



7. On the client, run the **systemctl restart winbind nscd** and **systemctl enable winbind nscd** commands to start the **winbind nscd** service, and run the **wbinfo -u** command to check whether AD domain users can be viewed. If AD domain users are displayed, the client has been successfully added to the domain.

Step 5 Log in to the KDC server and open the command line tool (for example, Windows PowerShell). Run the **Set-ADComputer** *Computer_Name* **-KerberosEncryptionType AES128,AES256** command to set the Kerberos encryption algorithm of the client.

Computer_Name is the computer name generated on the KDC server after the client has been added to the Kerberos realm, for example, **CLIENT_112_70**.

Example:

```
Set-ADComputer CLIENT_112_70 -KerberosEncryptionType AES128,AES256
```

NOTE

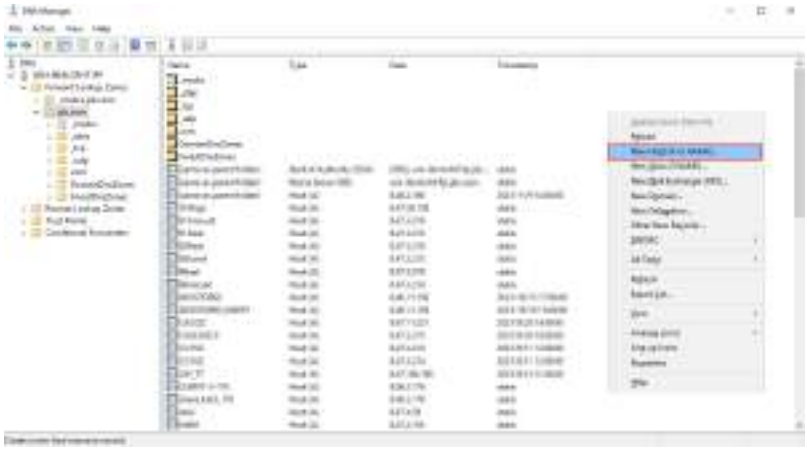
- Windows Server 2012 is used as an example. The commands may vary with the host OS.
- At least one of the Kerberos encryption algorithms configured on the KDC server must be the same as that configured in **3.8.2.5.2 Configuring the Kerberos Encryption Algorithm for the Storage System**.
- After the setting is complete, run the **Get-ADComputer -Properties *** *Computer_Name* command and check the **KerberosEncryptionType** field in the command output, which is the Kerberos encryption algorithm.

Step 6 On the client, run the **zypper install krb5-client** command to install **krb5-client**, and then run the **kinit administrator** command to initialize Kerberos authentication and generate a ticket for interaction between the client and KDC.

Step 7 On the client, run the **net ads keytab create -U administrator** command to generate a keytab file.

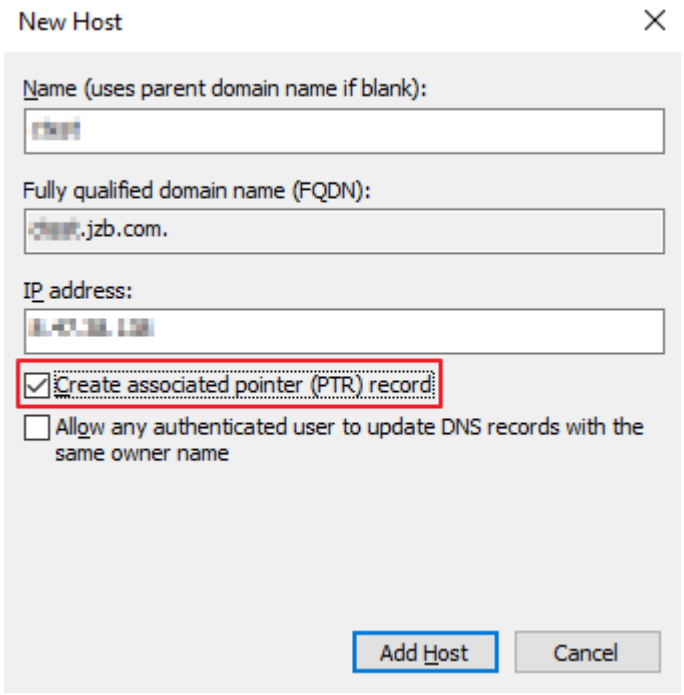
```
CLIENT_112_70:~ # net ads keytab create -U administrator
Enter administrator's password:
CLIENT_112_70:~ # cd /etc/
CLIENT_112_70:/etc # ls /etc/krb5.
krb5.conf    krb5.keytab
```


Step 8 Log in to the DNS server. On the **DNS Manager** page, click **Forward Lookup Zones** and select a domain name, for example, **jzb.com**. Right-click in the blank area on the right and choose **New Host (A or AAAA)** from the shortcut menu.



In the **New Host** dialog box, set the following parameters:

- **Name**: host name, for example, **CLIENT_112_70**.
- **Fully qualified domain name (FQDN)**: automatically generated based on the **Name** parameter and domain name, for example, **CLIENT_112_70.jzb.com**.
- **IP address**: IP address of the client.
- **Create associated pointer (PTR) record**: Select this option to ensure that the DNS can generate forward and reverse resolution records.



After the configuration is complete, run the **nslookup CLIENT_112_70** command on the client to check whether the configuration has taken effect.

Step 9 Enable NFS security authentication on the client.


```
CLIENT_112_70:~ # systemctl enable nfs-client.target
CLIENT_112_70:~ # systemctl start nfs-client.target
```

----End

3.8.2.7.2 CentOS Client

On a Linux client, you must set the time zone of the client, change the host name of the client, add the client to the Kerberos realm, configure the Kerberos encryption algorithm for the client, configure DNS resolution records, initialize Kerberos authentication, and enable NFS security authentication. The following uses a CentOS client as an example.

Procedure

Step 1 Change the time zone and time of the client to be consistent with those of the Kerberos realm controller server. The maximum time difference is 5 minutes.

Step 2 On the client, run the **yum -y install realmd sssd oddjob oddjob-mkhomedir adcli samba-common krb5-workstation** command to install the krb library.

Step 3 On the client, run the **vi /etc/hostname** command to change the host name (for example, **CLIENT_112_70**). Restart the client for the change to take effect.

Step 4 Add the client to the Kerberos realm. The Windows AD domain is used as an example.

1. Run the **vi /etc/resolv.conf** command to configure the DNS.

   The following is an example. **nameserver** is the IP address of the DNS server, and **search** is the AD domain name.

   ```
   nameserver x.x.x.x
   search jzb.com
   ```

   After the DNS configuration is complete, run the **nslookup CLIENT_112_70** command to check whether the configuration has taken effect.
2. Run the **realm discover jzb.com** command to discover the KDC realm, for example, **jzb.com**.
3. Run the **realm join jzb.com** command to add the client to the KDC realm.

Step 5 Log in to the KDC server and open the command line tool (for example, Windows PowerShell). Run the **Set-ADComputer** *Computer_Name* **-KerberosEncryptionType AES128,AES256** command to set the Kerberos encryption algorithm of the client.

Computer_Name is the computer name generated on the KDC server after the client has been added to the Kerberos realm, for example, **CLIENT_112_70**.

Example:

```
Set-ADComputer CLIENT_112_70 -KerberosEncryptionType AES128,AES256
```


NOTE

- Windows Server 2012 is used as an example. The commands may vary with the host OS.
- At least one of the Kerberos encryption algorithms configured on the KDC server must be the same as that configured in **3.8.2.5.2 Configuring the Kerberos Encryption Algorithm for the Storage System**.
- After the setting is complete, run the **Get-ADComputer -Properties *** *Computer_Name* command and check the **KerberosEncryptionType** field in the command output, which is the Kerberos encryption algorithm.

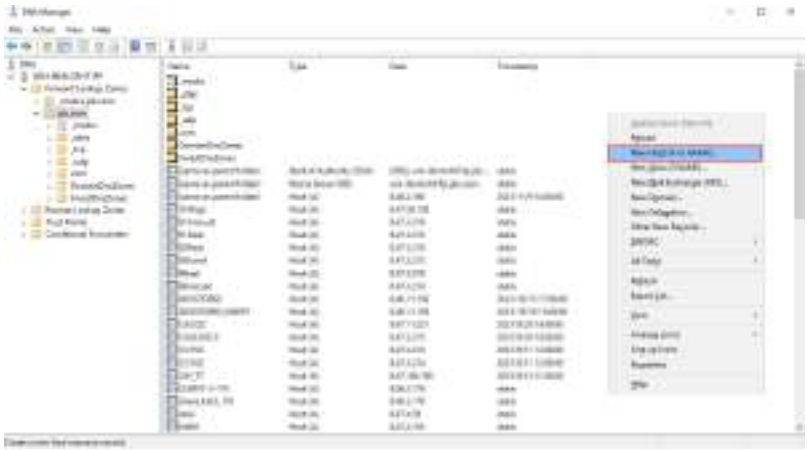
Step 6 Run the **vi /etc/krb5.conf** command on the client to configure the **krb5.conf** file.

The following is an example of the **krb5.conf** file content. Replace the information in bold with the AD domain name, for example, **jzb.com**.

```
includedir /etc/krb5.conf.d/

[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 dns_lookup_realm = false
 ticket_lifetime = 24h
 renew_lifetime = 7d
 forwardable = true
 rdns = false
 default_realm = JZB.COM
 default_ccache_name = KEYRING:persistent:%{uid}

[realms]
# EXAMPLE.COM = {
#  kdc = kerberos.example.com
#  admin_server = kerberos.example.com
# }

[domain_realm]
 .jzb.com = JZB.COM
 jzb.com = JZB.COM
```

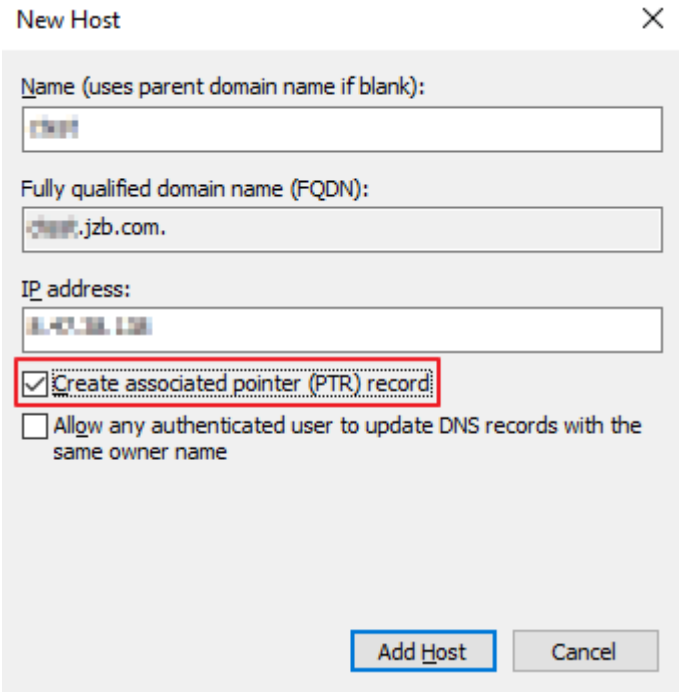
Step 7 On the client, run the **kinit administrator** command to initialize Kerberos authentication and generate a ticket for the interaction between the client and KDC.

Step 8 Log in to the DNS server. On the **DNS Manager** page, click **Forward Lookup Zones** and select a domain name, for example, **jzb.com**. Right-click in the blank area on the right and choose **New Host (A or AAAA)** from the shortcut menu.



In the **New Host** dialog box, set the following parameters:

- **Name**: host name, for example, **CLIENT_112_70**.
- **Fully qualified domain name (FQDN)**: automatically generated based on the **Name** parameter and domain name, for example, **CLIENT_112_70.jzb.com**.
- **IP address**: IP address of the client.
- **Create associated pointer (PTR) record**: Select this option to ensure that the DNS can generate forward and reverse resolution records.



After the configuration is complete, run the **nslookup CLIENT_112_70** command on the client to check whether the configuration has taken effect.

Step 9 Enable NFS security authentication on the client.

```
[root@CLIENT_112_70 ~]# systemctl enable nfs-client.target
[root@CLIENT_112_70 ~]# systemctl start nfs-client.target
```

----End

3.8.2.7.3 (Optional) Configuring an LDAP Domain on the Client

To use LDAP domain users, you must configure the LDAP domain users on the client. The following uses a SUSE client as an example. Before performing the following operations, configure the client by following instructions in **3.8.2.7.1 SUSE Client**.

NOTE

This document describes the configuration of the NFS Kerberos service. LDAP domain users use the LDAP service provided by the AD domain.

Procedure

Step 1 Log in to the SUSE client.

Step 2 Run the **vi /etc/openldap/ldap.conf** command to configure the **ldap.conf** file.

The following is an example of the **ldap.conf** file content, where **ad1** is the device name of the AD domain server and **hpc** is the AD domain name.

```
URI ldap://ad1.hpc.com
BASE dc=hpc,dc=com
```

Step 3 Run the **ldapsearch sAMAccountName=jzb** command (assume that the LDAP domain user is **jzb**) to search for the LDAP domain user. The following is an example. Check that the UNIX properties in bold are correct.

```
kerberos16:~ # ldapsearch sAMAccountName=jzb
SASL/GSSAPI authentication started
SASL username: administrator@HPC.COM
SASL SSF: 56
SASL data security layer installed.
# extended LDIF
#
# LDAPv3
# base <dc=hpc,dc=com> (default) with scope subtree
# filter: sAMAccountName=jzb
# requesting: ALL
#

# jzb, hpcuser, hpc.com
dn: CN=jzb,OU=hpcuser,DC=hpc,DC=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: jzb
givenName: jzb
distinguishedName: CN=jzb,OU=hpcuser,DC=hpc,DC=com
instanceType: 4
whenCreated: 20220422085338.0Z
whenChanged: 20220424021519.0Z
displayName: jzb
uSNCreated: 1499307
uSNChanged: 1522212
name: jzb
objectGUID:: vDpDZDHorE2EonpO8zyddw==
userAccountControl: 512
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 132952584322127201
lastLogoff: 0
lastLogon: 132953266939582841
pwdLastSet: 132950942831525923
primaryGroupID: 513
objectSid:: AQUAAAAAAAUVAAAAX8yEGTCvXnYMwKmnaxoAAA==
accountExpires: 9223372036854775807
logonCount: 6
sAMAccountName: jzb
sAMAccountType: 805306368
userPrincipalName: jzb@hpc.com
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=hpc,DC=com
dSCorePropagationData: 16010101000000.0Z
lastLogonTimestamp: 132950920445062939
uid: 16001
uidNumber: 16001
gidNumber: 16001
unixHomeDirectory: /home/jzb
loginShell: /bin/bash
```



```
# search reference
ref: ldap://ForestDnsZones.hpc.com/DC=ForestDnsZones,DC=hpc,DC=com

# search reference
ref: ldap://DomainDnsZones.hpc.com/DC=DomainDnsZones,DC=hpc,DC=com

# search reference
ref: ldap://hpc.com/CN=Configuration,DC=hpc,DC=com

# search result
search: 5
result: 0 Success

# numResponses: 5
# numEntries: 1
# numReferences: 3
kerberos16:~ #
```

Step 4 Configure the Pluggable Authentication Module (PAM) to use SSSD to authenticate users.

```
kerberos16:~ # pam-config --add --sss
kerberos16:~ # pam-config --add --mkhomedir
```

Step 5 Run the **vi /etc/sssd/sssd.conf** command to configure the **sssd.conf** file.

The following is an example of the **sssd.conf** file content. Replace the information in bold with the AD domain name.

```
[sssd]
 domains = hpc.com
 config_file_version = 2
 services = nss, pam

[domain/hpc.com]
ad_domain = hpc.com
krb5_realm = HPC.COM
realmd_tags = manages-system joined-with-samba
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = false
use_fully_qualified_names = False
fallback_homedir = /home/%u@%d
access_provider = simple
simple_allow_groups = RootUser,NonRootUser
```

Step 6 Enable the SSSD service on the client.

```
kerberos16:~ # systemctl enable sssd.service
kerberos16:~ # systemctl start sssd.service
```

Step 7 View the LDAP domain user. In this example, the LDAP user name is **jzb**.

```
kerberos16:~ # id jzb
uid=16001(jzb) gid=16001(jzbgroup) groups=16001(jzbgroup)
```

----End

3.8.2.8 Creating and Accessing an NFS Share

After the preceding configurations are complete, you can verify the NFS share access.

3.8.2.8.1 Creating an NFS Share

After an NFS share is created, clients can access the shared file system over the network.

Prerequisites

A file system has been created.

Procedure

Step 1 Choose **Services** > **File Service** > **Shares** > **NFS Shares**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left.

Step 3 Click **Create**.

The **Create NFS Share** page is displayed on the right.

NOTE

The screenshot is for reference only and the actual GUI may vary.

For some device models, you can click  in the upper right corner of the page to enable SmartGUI. SmartGUI mines users' historical operation data and builds a configuration parameter recommendation model based on user profiles to recommend configuration parameters for the block service and file service. After SmartGUI is enabled, the system presets the **File System** and **Permission** parameters based on recommendations when you create an NFS share. You can directly use the parameters or modify them as required.

Step 4 Set basic NFS share parameters.

Table 3-38 Basic NFS share parameters

Parameter	Description
File System	File system for which you want to create an NFS share. **NOTE** When the global root directory **/** is selected for **File System**, you can create an NFS global namespace (GNS) share. ● Each vStore can only create one GNS. ● You must add an independent share for a file system. After the share is added, this file system will not be displayed if a host is only authorized to access **/** but not the file system. ● GNS root directory **/** is read-only. You cannot create, modify, and delete directories or files under **/** and you cannot modify directory attributes of **/**. Once the directory of a file system is entered, the permission will change to the share permission of the file system. ● If no GNS is created, root directory **/** cannot be mounted to an NFSv3 client. Only shared file systems can be viewed when **/** is mounted to an NFSv4 directory. ● When creating an NFS GNS share, you can only set the description for the share. ● If you want to create a HyperMetro or HyperReplication vStore pair and a GNS has been created for the primary vStore, the version of the secondary storage system must be the same as that of the primary storage system. If a vStore pair has been created, you can create a GNS share only when the versions of the primary and secondary storage systems are the same and support GNSs. [Example] FileSystem001 **NOTICE** If the selected file system is the secondary storage system in a remote replication pair or remote storage system in a HyperMetro pair, data in the file system is probably being modified when it is accessed. Before performing this operation, confirm that the application allows possible data inconsistency.

Parameter	Description
Dtree	Dtree for which you want to create an NFS share. If you do not select a dtree, the NFS share is created for the entire file system. [Example] Dtree_test
Share Path	Share path of the file system, which is generated based on the **File System** and **Dtree** parameters. [Example] /Filesystem001/Dtree_test
Description	Description of the NFS share. [Value range] The description can be left blank or contain up to 255 characters.

Parameter	Description
Character Encoding	Clients communicate with the storage system using codes. Codes configured on the NFS share must be the same as that of the clients. These codes apply to names and metadata of shared files, but do not change the codes of file data. Codes include: • UTF-8 International code set • EUC-JP euc-j*[ja] code set • JIS JIS code set • S-JIS cp932*[ja_jp.932] code set • ZH Simplified Chinese code set, in compliance with GB 2312 • GBK Simplified Chinese code set, in compliance with GB 2312 • EUC-TW Traditional Chinese code set, in compliance with CNS 11643 • BIG5 cp950 traditional Chinese code set • DE German character set, in compliance with ISO 8859-1 • PT Portuguese character set, in compliance with ISO 8859-1 • ES Spanish character set, in compliance with ISO 8859-1 • FR French character set, in compliance with ISO 8859-1 • IT Italian character set, in compliance with ISO 8859-1 • KO cp949 Korean code set • AR Arabic character set, in compliance with ISO 8859-6 • CS Czech character set, in compliance with ISO 8859-2 • DA Danish character set, in compliance with ISO 8859-1 • FI Finnish character set, in compliance with ISO 8859-1 • HE Hebrew character set, in compliance with ISO 8859-8

Parameter	Description
	• HR Croatian character set, in compliance with ISO 8859-2 • HU Hungarian character set, in compliance with ISO 8859-2 • NO Norwegian character set, in compliance with ISO 8859-1 • NL Dutch character set, in compliance with ISO 8859-1 • PL Polish character set, in compliance with ISO 8859-2 • RO Romanian character set, in compliance with ISO 8859-2 • RU Russian character set, in compliance with ISO 8859-5 • SK Slovak character set, in compliance with ISO 8859-2 • SL Slovenian character set, in compliance with ISO 8859-2 • SV Swedish character set, in compliance with ISO 8859-1 • TR Turkish character set, in compliance with ISO 8859-9 • EN-US English character set, in compliance with ISO 8859-1 **NOTE** • Method of querying character encoding on clients (for example, in Linux): Run the **locale** command to view character encoding of the current system. • NFSv4 supports only UTF-8. If NFSv4 is used, ensure that the host uses UTF-8 character encoding.
Show Snapshot	This function allows clients to show and traverse snapshot directories.

NOTE

Description and **Character Encoding** are hidden parameters. To display hidden parameters, click **Advanced**.

Step 5 Configure access permissions for the NFS share.

Click **Add** to add a client. For details, see **3.8.2.8.2 Adding an NFS Share Client**.

NOTE

- When **Type** is set to **Host**, the system automatically detects whether the LDAP domain, NIS domain, or DNS has been configured. To add a client by specifying the host name, configure at least one of them.
- When **Type** is set to **Network group**, the system automatically detects whether the LDAP domain or NIS domain has been configured. You must configure at least one of them.
- You can click **More** on the right of a client and select **Modify** to modify its information.
- You can select one or more clients and click **Remove**, or click **More** on the right of a client and select **Remove**, to remove clients.

Step 6 Click **OK**.

----End

3.8.2.8.2 Adding an NFS Share Client

An NFS share client allows the client users to access shared file systems over the network.

Prerequisites

- You have obtained required data for configuring an NFS share.
- You have created a host name available on the DNS if you need to add a client whose **Type** is **Host**.
- You have created a network group name available on the LDAP or NIS server if you need to add a client whose **Type** is **Network group**.

Procedure

Step 1 Choose **Services** > **File Service** > **Shares** > **NFS Shares**.

Step 2 Select the vStore to which the desired NFS share belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Click **More** on the right of the desired NFS share and select **Add Client**.

The **Add Client** page is displayed.

NOTE

Alternatively, perform either of the following operations to add a client:

- Click the path of the desired NFS share. On the page that is displayed, click **Add** in the **Permissions** area.
- Click the path of the desired NFS share. In the upper right corner of the page that is displayed, click **Operation** and select **Add Client**.

NOTE

For some device models, you can click  in the upper right corner of the page to enable SmartGUI. SmartGUI mines users' historical operation data and builds a configuration parameter recommendation model based on user profiles to recommend configuration parameters for the block service and file service. After SmartGUI is enabled, the system presets the **Type** and **Permission** parameters based on recommendations when you add a client. You can directly use the parameters or modify them as required.

Step 4 Set client attributes.

Table 3-39 describes the parameters.

Table 3-39 Client parameters

Parameter	Description
Type	Client type of the NFS share. [Value range] • Host • Network group **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 > network segment > wildcard > network group > *. • When **Type** is set to **Network group** and the vStore to which the share belongs is configured with the DNS service, add the reverse lookup zones of the network segments where the client IP addresses reside on the DNS server. Otherwise, the host I/O latency may increase.

Parameter	Description
Clients	When **Type** is set to **Host**, enter client host names (FQDNs are recommended), IP addresses, or IP address segments, or use the asterisk (*) to represent IP addresses of all clients. When **Type** is set to **Network group**, enter the network group names configured in the LDAP or NIS domain. **NOTE** • When **Type** is set to **Host**, the system automatically detects whether the LDAP domain, NIS domain, or DNS has been configured. To add a client by specifying the host name, configure at least one of them. • When **Type** is set to **Network group**, the system automatically detects whether the LDAP domain or NIS domain has been configured. You must configure at least one of them. [Value range] You can enter multiple host names, IP addresses, or network group names of the clients separated by semicolons (;), spaces, or carriage returns. For host names: • A host name contains 1 to 255 characters and cannot contain spaces. • A host name cannot start with a hyphen (-). For IP addresses: • You can enter client IP addresses, client IP address segments, or an asterisk (*) to represent IP addresses of all clients. • IPv4 addresses, IPv6 addresses, or the combination of IPv4 and IPv6 addresses are supported. • The mask of an IPv4 address ranges from 1 to 32. The prefix of an IPv6 address ranges from 1 to 128. A network group name: • Contains 1 to 254 characters. • The value can contain only letters, digits, underscores (_), periods (.), and hyphens (-).
UNIX Permission	Indicates the permission level for a UNIX client to access the NFS share. Possible options are: • **Read-only**: The client can only read files in the share. • **Read-write**: The client can read and write files in the share. • **None**: No operation is allowed on the share.

Parameter	Description
Kerberos5 Permission	Indicates the permission level for the Kerberos5 client to access the NFS share. Possible options are: ● **Read-only**: The client can only read files in the share. ● **Read-write**: The client can read and write files in the share. ● **None**: No operation is allowed on the share. This parameter applies only to the scenario where the NFS Kerberos service is configured.
Kerberos5i Permission	Indicates the permission level for the Kerberos5i client to access the NFS share. Possible options are: ● **Read-only**: The client can only read files in the share. ● **Read-write**: The client can read and write files in the share. ● **None**: No operation is allowed on the share. This parameter applies only to the scenario where the NFS Kerberos service is configured.
Kerberos5p Permission	Indicates the permission level for the Kerberos5p client to access the NFS share. Possible options are: ● **Read-only**: The client can only read files in the share. ● **Read-write**: The client can read and write files in the share. ● **None**: No operation is allowed on the share. This parameter applies only to the scenario where the NFS Kerberos service is configured.
root Permission Constraint	Controls the **root** permission of the clients. ● **root_squash**: does not allow a client to access the share as user **root**. Otherwise, the client will be mapped as an anonymous user. ● **no_root_squash**: allows a client to access the share as user **root** that has full control and access permissions for shared directories. **NOTE** ● If a VM needs to be created in the NFS share, select **no_root_squash**. Otherwise, the VM may run abnormally. ● For a file system or dtree whose security mode is UNIX, the default UNIX permission is **755**. If **root_squash** is enabled for the NFS share permission of the file system or dtree, user **root** only has the read and execute permissions. You can run the **change file_system general file_system_id=? unix_permissions=?** or **change dtree dtree_id=? unix_permissions=?** command to modify the UNIX permission of the file system or dtree.

NOTE

In the NFS Kerberos service application scenario, the settings of **Kerberos5 Permission**, **Kerberos5i Permission**, and **Kerberos5p Permission** in the preceding table must match the **sec** field specified when an NFS share is mounted on a client. 00

For example, if the **sec** field is set to **krb5i** when an NFS share is mounted to a client, at least **Kerberos5i Permission** must be set for the client.

Step 5 Set advanced client parameters. Select **Advanced** in the upper right corner.

Table 3-40 describes the parameters.

Table 3-40 Advanced client parameters

Parameter	Description
Permission Constraint	Indicates whether to retain the user ID (UID) and group ID (GID) of a shared directory. • **all_squash**: The UID and GID of a shared directory are mapped to user **nobody**, which is applicable to public directories. • **no_all_squash**: retains the UID and GID of a shared directory. [Default value] **no_all_squash**
Source Port Verification Constraint	Indicates whether to enable source port verification. • **secure**: allows clients to access the NFS share using ports 1 to 1023. • **insecure**: allows clients to access the NFS share using any port. [Default value] **insecure**
Anonymous User ID	Indicates the UID and GID of a user who accesses the shared directory after the user is mapped as an anonymous user. [Default value] 65534 **NOTE** Only 6.1.5 and later versions support this parameter.

Step 6 Click **OK**.

----End

3.8.2.8.3 Configuring a Kerberos-to-UNIX Mapping

Set the Kerberos-to-UNIX mapping for the NFS Kerberos service and set the mapping rule between the source and target users as required.

Procedure

Step 1 Choose **Services** > **File Service** > **Authentication Users** > **User Mappings**.

Step 2 Select the vStore for which you want to create a user mapping from the **vStore** drop-down list in the upper left.

Step 3 Click **Create**.

The **Create User Mapping** page is displayed on the right.

Step 4 Set basic user mapping parameters.

Table 3-41 describes the parameters.

Table 3-41 Basic user mapping parameters

Parameter	Description
Mapping Mode	User mapping mode related to the operating system, including: • **Windows to UNIX**: When accessing UNIX shares using Windows, a Windows user has all the permissions granted to the target user. • **UNIX to Windows**: When accessing Windows shares using UNIX, a UNIX user has all the permissions granted to the target user. • **Kerberos to UNIX**: When a client accesses UNIX shares through Kerberos authentication, the Kerberos user has all the permissions granted to the target user. For the NFS Kerberos service, set the mapping mode to **Kerberos to UNIX**.
Source User	Source user of the mapping. For the NFS Kerberos service, you are advised to set this parameter as follows: • If **KDC Vendor** is set to **Non-Windows**, set this parameter to client host name + Kerberos realm name, for example: kdcclient10.lxj_krb5.com. • If **KDC Vendor** is set to **Windows**, set this parameter to client host name (in uppercase) + $, for example: CLIENT_112_70$.

Parameter	Description
Target User	Target user of the mapping. In the NFS Kerberos service, you are advised to set the target user to **root**. The target users can be: ● UNIX local user on the storage system: Map the permissions of the source user to the UNIX local user on the storage system. If no local UNIX user exists, create one. ● LDAP or NIS domain user: Map the permissions of source user to the LDAP or NIS domain user. **NOTE** ● System_vStore does not have the local user **root**. You need to create it first. ● vStores other than System_vStore has the local user **root** by default. You do not need to create it.
Priority	Priority of the mapping. A smaller value indicates a higher priority. When multiple mappings share the same source user, the system uses the mapping with the highest priority. [Value range] 1~32

Step 5 Click **Add to Mapping List** to add the mapping to the list below.

NOTE

You can add multiple user mappings to the list.

Step 6 Click **OK**.

----End

3.8.2.8.4 Mounting an NFS Share to a Client

This section describes how to mount an NFS share created on the storage system to a client of the NFS Kerberos service.

Prerequisites

- The NFSv4.0 or NFSv4.1 service has been enabled on the storage system.
- The storage system has been added to the Kerberos realm correctly.
- An NFS share has been created and an NFS share client has been added.
- A Kerberos-to-UNIX mapping has been configured.

Context

The storage system must use the NFSv4.0 or NFSv4.1 protocol to support the Kerberos service.

Precautions

When a file system is mounted using NFSv4.0 or NFSv4.1, ensure that the same domain name is configured for both the host and storage. (Generally, the default domain name is **localdomain** on both the host and storage device.) Otherwise, when files created by a host user are queried on the storage, the information about the user and group to which the files belong is incorrectly displayed. For example, user **root** is displayed as **nobody** on the storage.

- On the host, query the domain name in the configuration file of the idmapd service. For example, in the SUSE operating system, you can run the **vi /etc/idmapd.conf** command to query or edit the value of **Domain**.
- On the storage, run the **change vstore view id=***?* command to enter the vStore view. You can run the **show vstore** command to query the value of **id**. Then run the **show service nfs_config** command in developer mode to query the domain name. The default domain name is **localdomain**. To change the domain name on the storage, run the **change service nfs_config domain_name=***?* command.

Procedure

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

Step 2 Run the **showmount -e** *FQDN* command to view all NFS shares in the storage system.

FQDN is the instance of the service principal. For example, if the SPN of the logical port on the storage system is **nfs/ctest.jzb.com@JZB.COM**, the value of *FQDN* is **ctest.jzb.com**.

```
#showmount -e ctest.jzb.com
Export list for ctest.jzb.com
/nfstest *
#
```

NOTE

/nfstest in the output represents the share path of the NFS share created in the storage system.

Step 3 Run the **mount -t nfs -o sec=x,vers=n,proto=m,rsize=o,wsize=p,hard,intr,timeo=q** *FQDN*:*sharepath* *mountpoint* command to mount the NFS share. **Table 3-42** describes the parameters.

- *FQDN* is the instance of the service principal. For example, if the SPN of the logical port on the storage system is **nfs/ctest.jzb.com@JZB.COM**, the value of *FQDN* is **ctest.jzb.com**.
- *sharepath* is the share path of the NFS share created in the storage system, for example, **/nfstest**.
- *mountpoint* indicates the path of the client to be mounted, for example, **/mnt**.

Example:

```
mount -t nfs -o sec=krb5,vers=4,minorversion=1,proto=tcp,rsize=262144,wsize=262144,hard,intr,timeo=50
ctest.jzb.com:/nfstest /mnt
```


Table 3-42 Parameters for mounting an NFS share

Parameter	Description	Setting
o	Mounting mode of the NFS share. Possible values are **ro** and **rw**. • **ro**: mounts a share that is read-only. • **rw**: mounts a share that can be read and written.	The default value is **rw**.
sec	Security option for Kerberos authentication.	Possible values are: • **sys**: uses the UNIX UID and GID for identity authentication, and does not perform Kerberos encryption. • **krb5**: uses Kerberos v5 for identity authentication. • **krb5i**: uses Kerberos v5 for identity authentication, and verifies the integrity of NFS operations through security checks to prevent data tampering. • **krb5p**: uses Kerberos v5 for identity authentication and integrity check, and encrypts NFS traffic to prevent traffic sniffing. This setting provides the highest security but causes more performance overhead. The performance of Kerberos authentication in descending order is **krb5** > **krb5i** > **krb5p**. When the NFS Kerberos service is used, the value of **sec** must match the **Kerberos5 Permission**, **Kerberos5i Permission**, and **Kerberos5p Permission** set in section "**Adding an NFS Share Client**". For example, if the value of **sec** is set to **krb5i** during NFS mounting, at least **Kerberos5i Permission** must be set for the client.
vers	NFS protocol version.	• If the client mounts the share using NFSv4.0, set **vers** to **4**. • If the client mounts the share using NFSv4.1, set **vers** to **4** and specify **minorversion=1**.
proto	Transfer protocol.	Set this parameter to **tcp**.

Parameter	Description	Setting
rsize	Size of the transport block for read, in bytes.	The recommended value is **262144**.
wsize	Size of the transport block for write, in bytes.	The recommended value is **262144**.
timeo	Interval for retransmission upon timeout. The unit is 0.1 second.	• The default value is **600**. • If there is a high requirement on the service recovery time, you are advised to set this parameter to **50**.

NOTE

You are advised to use the recommended parameter settings.

Step 4 Run the **mount** command to verify that the NFS share has been mounted to the local computer.

----End

3.8.2.8.5 Accessing an NFS Share from a Client

This section describes how to access an NFS share.

NOTE

If the message **Permission denied** is displayed when a client accesses an NFS share, run the **change file_system general file_system_id=? unix_permissions=?** or **change dtree dtree_id=? unix_permissions=?** command to modify the Unix permission of the file system or dtree, and then access the NFS share.

Using the Root User to Access an NFS Share

After an NFS share is mounted to a client, you can use the root user to access the NFS share. The procedure is as follows:

Step 1 Log in to the client.

Step 2 Use the root user to access the share. In the following example, the mounted client path is **/mnt**.

```
kerberos16:~ # id root
uid=0(root) gid=0(root) groups=0(root)
kerberos16:~ # su root
kerberos16:~ # cd /mnt
kerberos16:/mnt # mkdir testroot
kerberos16:/mnt # ll
total 556
drwxr-xr-x 2 jzb  jzbgroup   4096 Apr 24 15:13 16001
drwxr-xr-x 2 root root   4096 Apr 25 10:22 17001
drwxr-xr-x 8 root root 544768 Apr 22 15:21 .snapshot
drwxr-xr-x 2 jzb  jzbgroup   4096 Apr 24 15:28 test
drwxr-xr-x 2 root root   4096 Apr 25 10:23 test01
drwxr-xr-x 2 jzb  jzbgroup   4096 Apr 25 10:16 test0425
```



```
drwxr-xr-x 2 root root   4096 Apr 25  2022 testroot
kerberos16:/mnt #
```

----End

(Optional) Using the LDAP Domain User to Access an NFS Share

You can use an LDAP user to access an NFS share on the client. The following is an example of using an LDAP user to access an NFS share from a SUSE client.

Step 1 Switch to the LDAP domain user.

Go to the mount path and switch to the LDAP domain user.

For example, the mounted client path is **/mnt** and the LDAP domain user name is **jzb**.

```
kerberos16:~ # cd /mnt
kerberos16:/mnt # su jzb
jzb@kerberos16:/mnt>
```

Step 2 Run the **kinit** command to initialize the LDAP domain user and enter the user password as prompted.

```
jzb@kerberos16:/mnt> kinit
Password for jzb@HPC.COM:
jzb@kerberos16:/mnt>
```

Step 3 Create a run directory for the LDAP domain user.

Run the **id** *user name* command to view the IDs of the LDAP domain user and user group. Then create a run directory with the value of **uid**.

In this example, the user name is **jzb**.

```
jzb@kerberos16:/mnt> id jzb
uid=16001(jzb) gid=16001(jzbgroup) groups=16001(jzbgroup)
jzb@kerberos16:/mnt>mkdir 16001
```

Step 4 Use the LDAP domain user to access the share.

On the SUSE client, use the LDAP domain user to access the share. The following is an example.

```
jzb@kerberos16:/mnt> cd /mnt
jzb@kerberos16:/mnt> mkdir test
jzb@kerberos16:/mnt> ll
total 8
drwxr-xr-x 2 jzb jzbgroup 4096 Apr 24 15:13 16001
drwxr-xr-x 2 jzb jzbgroup 4096 Apr 24 15:28 test
jzb@kerberos16:/mnt>
```

----End

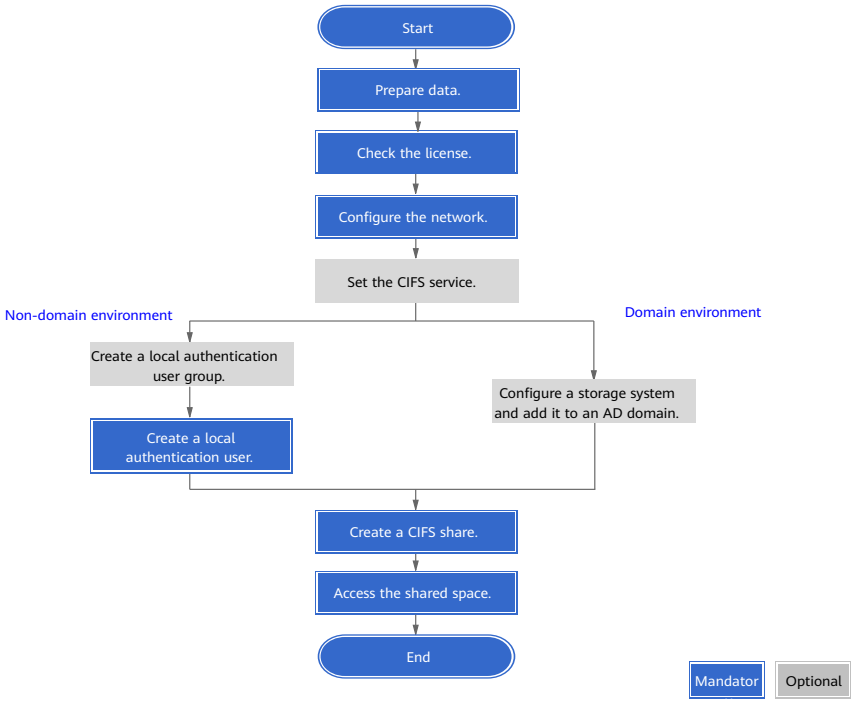
3.8.3 Configuring a CIFS Share

This section describes how to configure a CIFS share.

3.8.3.1 Configuration Process

Figure 3-5 shows the CIFS share configuration process.

Figure 3-5 CIFS share configuration process



3.8.3.2 Preparing Data

Before configuring a CIFS share in a storage system, plan and collect required data to facilitate follow-up service configurations.

You need to prepare the following data:

- Logical IP address

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

  File system or its dtree configured as a CIFS share.
- Name of a CIFS share
- Permission

  Permission of a user or user group to access a CIFS share, including:
  - Full control: The user can fully control the CIFS share.
  - Read-only: The user can only read the CIFS share.
  - Read and write: The user can read and write the CIFS share.
  - Forbidden: The user cannot access the CIFS share.
- Local authentication user

  Users for local authentication of the storage system in a non-domain environment.
- AD domain information

- DNS

  IP address of the DNS server.

NOTE

You can contact your network administrator to obtain desired data.

3.8.3.3 Checking the License

Before configuring CIFS, ensure that the license grants the use of NAS Foundation.

Procedure

Step 1 Choose **Settings** > **License Management**.

Step 2 In the middle function pane, verify that **NAS Foundation** is displayed in the feature list.

NOTE

- If no license file has been imported, import a license file by referring to the initialization guide.
- If **NAS Foundation** is not displayed in the feature list, contact technical support engineers.

----End

3.8.3.4 Configuring the Network

Before configuring shared services, plan and configure the network properly for accessing and managing file services.

3.8.3.4.1 (Optional) Creating a Bond Port

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

Prerequisites

The IP addresses of the Ethernet ports you want to bond have been cleared. Ethernet ports that have IP addresses cannot be bonded.

Context

Port bonding provides more bandwidth and higher redundancy for links. Although ports are bonded, each session still transmits data through a single port and the total bandwidth can be increased only when there are multiple sessions. Determine whether to bond ports based on site requirements.

Port bonding on the storage system has the following restrictions:

- Only Ethernet ports that have the same rate and are on the same controller can be bonded. Ports cannot be bonded across controllers. Non-Ethernet ports cannot be bonded.
- Link aggregation (IEEE 802.3ad) is supported.
- For OceanStor 5310, OceanStor 5510 and OceanStor 5610:

  - GE interface modules (not supporting TOE) support port bonding across modules by default.
  - 10GE, 25GE, 40GE, and 100GE interface modules (supporting TOE) do not support port bonding across modules by default. They support port bonding across modules after TOE is disabled.

    NOTICE

    To disable the TOE function of a port, contact Huawei technical support.

  - The onboard network ports of OceanStor 5310 can be bonded across interface modules and the port rates must be the same.
- For OceanStor 6810, OceanStor 18510, and OceanStor 18810, interface modules in the same quadrant can be bonded across interface modules, and the TOE function of the ports to be bonded must be disabled.

  NOTICE

  To disable the TOE function of a port, contact Huawei technical support.

  For OceanStor 6810, OceanStor 18510, and OceanStor 18810, each interface module can use only one bonding mode. That is, an interface module does not allow bonding across modules and bonding within the module at the same time.

- Read-only users are not allowed to bond Ethernet ports.
- Each Ethernet port can be added to only one bond port.
- A member port of a port group cannot be added to a bond port.
- Management network ports cannot be bonded.
- Member ports in the same bond port cannot connect to different switch networks.
- After Ethernet ports are bonded, their MTU changes to the default value and you need to configure the switch port mode. Take Huawei switches as an example. You must set the ports on the Huawei switches to work in static LACP mode.

  NOTICE

  The link aggregation modes vary with switch manufacturers. If a switch from another vendor is used, contact technical support of the switch manufacturer for specific link aggregation configurations.

Port bonding on the host has the following restriction:

If the TOE function is enabled on the storage system and the host port connecting to the switch must be bonded, the bonding mode must be set to 4.

NOTE

If the preceding restriction cannot be met, disable the TOE function of the port.

Procedure

Step 1 Choose **Services** > **Network** > **Ethernet Network** > **Bond Ports**.

Step 2 Click **Create**.

The **Create Bond Port** page is displayed on the right.

Step 3 Set a bond name and select ports you want to bond.

1. Specify a name for the bond port in **Name**.

   NOTE

   The name must meet the following requirements:

   - The value can contain only letters, digits, underscores (_), hyphens (-), and periods (.).
   - The name contains 1 to 31 characters.

2. Select the controller where the bond port resides.
3. In **Available Ports**, select one or more ports you want to bond.

Step 4 Click **OK**.

Confirm your operation as prompted.

----End

3.8.3.4.2 (Optional) Creating a VLAN

This section describes how to create VLANs for Ethernet ports or bond ports.

Prerequisites

VLANs cannot be created on the Ethernet ports that are configured with IP addresses or used for networking.

Procedure

Step 1 Choose **Services** > **Network** > **Ethernet Network** > **VLANs**.

Step 2 Click **Create**.

The **Create VLAN** page is displayed on the right.

Step 3 In the **Port Type** drop-down list, select the type of the ports used to create VLANs.

Possible values are **Ethernet Port** and **Bond Port**.

Step 4 In the **Home Port** list, select a home port.

Step 5 In **ID**, specify the ID of a VLAN, and then click **Add**.

NOTE

- The VLAN ID ranges from 1 to 4094. You can specify multiple VLAN IDs one by one or in a batch. When creating multiple VLANs and specifying VLAN IDs in a batch, the VLAN IDs are in the following format: Start VLAN ID-End VLAN ID.
- To delete a VLAN ID, click × next to it.

Step 6 Click **OK**.

----End

Follow-up Procedure

When creating a logical port based on a VLAN, ensure that the port type is VLAN and the home port is the VLAN's home port.

3.8.3.4.3 (Optional) Creating a DNS Zone

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

Context

It is recommended that a DNS zone be associated with only logical ports with the same IP address type (IPv4 or IPv6).

If the host interface card supports both IPv4 and IPv6 protocols, the DNS client initiates IPv4 and IPv6 resolution requests. If the storage system is associated with both IPv4 and IPv6 logical ports in the same DNS zone and the host interface card is configured with only IPv4 addresses, the host may fail to access the domain name.

Procedure

Step 1 Choose **Services** > **vStore Service** > **vStores**.

Step 2 Click the name of the desired vStore. On the details page that is displayed on the right, click the **File Service** tab and click **Configure** in the **DNS Zone** area.

The **Configure DNS Zone** page is displayed on the right.

Step 3 Configure a DNS zone.

- Add a DNS zone.
  a. Click **Add**.
  b. In **Name**, enter the name of the DNS zone to be added.

NOTE

The name complexity requirements are as follows:

- A name contains 1 to 255 characters and consists of multiple labels separated by periods (.).
- A label contains 1 to 63 characters including letters, digits, hyphens (-), and underscores (_), and must start and end with a letter or a digit.
- A name must be unique.

c. If a HyperMetro vStore pair has been created for the vStore and **Working Mode** of the selected HyperMetro domain is **Active-active mode**, you need to set the owning site of the DNS zone. In normal cases, the host can access the logical port that belongs to the local site through the domain name of the local site. DNS zones with owning sites are mainly used when the active-active sites are far away from each other. In this case, hosts can access the nearest site to ensure access performance.

- Modify a DNS zone.

  In **Name**, modify the name of the desired DNS zone.

  NOTE

  The name complexity requirements are as follows:
  - A name contains 1 to 255 characters and consists of multiple labels separated by periods (.).
  - A label contains 1 to 63 characters including letters, digits, hyphens (-), and underscores (_), and must start and end with a letter or a digit.
  - A name must be unique.

- Remove a DNS zone.

  In the row that contains the desired DNS zone, click **Remove**.

Step 4 Click **Save**.

----End

3.8.3.4.4 Creating a Logical Port

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

Context

When configuring a CIFS share, set **Role** to **Service** for the logical port, and set **Data Protocol** to **CIFS** or **NFS + CIFS** for the logical port.

Precautions

- It is recommended that you create no more than 64 logical ports for each controller. If more than 64 logical ports are created for one controller, the logical ports will fail over to a few available physical ports in the event that a large number of physical ports fail, decreasing service performance.
- In the case of file access across network segments, if a Remote Authentication Dial-In User Service (RADIUS) server is used for network device

authentication in the data center and IP address failover occurs on a logical port, the IP address of the logical port will be re-registered on the RADIUS server. In this process, the IP address is not available. File services will be restored after the IP address becomes available.

Procedure

Step 1 Choose **Services** > **Network** > **Logical Ports**.

Step 2 Click **Create**.

The **Create Logical Port** page is displayed on the right.

Step 3 Set the parameters listed in **Table 3-43**.

Table 3-43 Logical port parameters

Parameter	Description
Name	Name of the logical port. The name must meet the following requirements: • The name must be unique. • The name can contain only letters, digits, underscores (_), hyphens (-), and periods (.). • The name contains 1 to 255 characters.
Role	Role of the logical port. Possible values are: **Management**: A port of this role is used by a vStore administrator to log in to the system for management. **Service**: A port of this role is used to access services, such as accessing CIFS shares of file systems. **Management + service**: A port of this role is used to access services or for a vStore administrator to log in to the storage system for system management. **Replication**: A port of this role is used for replication link connection in remote replication or HyperMetro, or for quorum link connection in HyperMetro.
Data Protocol	Data protocol of a logical port. Possible values are **NFS**, **CIFS**, **NFS + CIFS**, **iSCSI**, and **NVMe over RoCE**. **NOTE** • **NFS**, **CIFS**, and **NFS + CIFS** are applicable to file service configuration. **iSCSI** and **NVMe over RoCE** are applicable to block service configuration. • This parameter is displayed only when **Role** is set to **Service** or **Management + service**.
Owning vStore	vStore to which the logical port belongs. **NOTE** This parameter is displayed only when **Role** is set to **Service**, **Management**, or **Management + service**.

Parameter	Description
Owning Site	Site to which a logical port belongs. If a HyperMetro vStore pair has been created for the owning vStore, the configuration information of the front-end service logical port at the local site is automatically synchronized to the remote site, and the logical port at the owning site processes service access. The logical port is in connected state at the owning site and is in to-be-working state at the non-owning site. After the logical port creation is complete, its owning site cannot be modified. If a fault occurs for the port, the logical port at the non-owning site is used to process service access. **NOTE** This parameter is displayed only when a HyperMetro vStore pair has been created for the owning vStore and **Working Mode** of the HyperMetro domain of the HyperMetro vStore pair is **Active-active mode**.
IP Address Type	IP address type of the logical port, which can be **IPv4** or **IPv6**.
IP Address	IPv4 or IPv6 address of the logical port.
Subnet Mask	Subnet mask of the logical port's IPv4 address. **NOTE** This parameter is available only when **IP Address Type** is set to **IPv4**.
Prefix	Prefix length of the logical port's IPv6 address. **NOTE** This parameter is available only when **IP Address Type** is set to **IPv6**.
Gateway	Gateway of a logical port's IP address.
Port Type	Type of the port to which the logical port belongs. Possible values are **Ethernet port**, **Bond port**, **VLAN**, and **RoCE port**. **NOTE** • When **Data Protocol** is **NFS**, **CIFS**, **NFS + CIFS**, or **iSCSI**, you can select an Ethernet port, bond port, or VLAN. • When **Data Protocol** is **NVMe over RoCE**, you can select a VLAN or RoCE port. • Only 6.1.5 and later versions support RoCE ports.
Home Port	Ethernet port, bond port, VLAN, or RoCE port to which the logical port belongs. **NOTE** If **Port Type** is **RoCE port**, the system displays only the RoCE ports with a trust mode of DSCP.

Parameter	Description
Activation Status	Determine whether to activate the logical port. **NOTE** This parameter is available only when **Data Protocol** is set to **NFS**, **CIFS**, or **NFS + CIFS**.

Step 4 When **Role** is set to **Management**, **Service**, or **Management + service**, select **Advanced** in the upper right corner and set the advanced attributes of the logical port.

NOTE

If **Role** is set to **Service**, you can set advanced attributes only when **Data Protocol** is set to **NFS**, **CIFS**, or **NFS + CIFS**.

Table 3-44 describes the parameters.

Table 3-44 Advanced logical port parameters

Parameter	Description
Failover Group	Name of a failover group. **NOTE** • This parameter is available only when **Data Protocol** is set to **NFS**, **CIFS**, or **NFS + CIFS**. • If a failover group is specified, services on the failed home port will be taken over by an available port in the specified failover group. • If no failover group is specified, services on the failed home port will be taken over by an available port in the default failover group. • It is recommended that the logical ports of the same vStore use the same failover group. This ensures that the fault domains of the logical ports are the same.
IP Address Failover	After IP address failover is enabled, services on the failed home port will be taken over by other available ports in the failover group. In the entire process, the IP address used by services remains unchanged. **NOTE** • This parameter is available only when **Data Protocol** is set to **NFS**, **CIFS**, or **NFS + CIFS**. • Shares of file systems do not support the multipathing mode. They use IP address failover to improve the reliability of links.

Parameter	Description
Failback Mode	After the fault of the home port is rectified, services fail back to the home port. Possible values are **Automatic** and **Manual**. **NOTE** • This parameter is available only when **Data Protocol** is set to **NFS**, **CIFS**, or **NFS + CIFS**. • If **Failback Mode** is **Manual**, ensure that the link to the home port is normal before the failback. You can manually switch services back to the home port only when the link to the home port keeps normal for over five minutes. • If **Failback Mode** is **Automatic**, ensure that the link to the home port is normal before the failback. Services will automatically fail back to the home port only when the link to the home port keeps normal for over five minutes.
Listen for DNS Query	With this function enabled, external NEs can access the DNS service provided by the storage system by using the IP address of this logical port. **NOTE** This parameter is available only when **Data Protocol** is set to **NFS**, **CIFS**, or **NFS + CIFS**.
DNS Zone	Name of a DNS zone. **NOTE** • This parameter is available only when **Data Protocol** is set to **NFS**, **CIFS**, or **NFS + CIFS**. • If the value is blank, the logical port is not used for DNS-based load balancing. • One logical port can be associated with only one DNS zone. One DNS zone can be associated with multiple logical ports. • It is recommended that **Listen for DNS Query** be enabled for at least one logical port of each DNS zone. • It is recommended that a DNS zone be associated with only logical ports with the same IP address type (IPv4 or IPv6). If the host interface card supports both IPv4 and IPv6 protocols, the DNS client initiates IPv4 and IPv6 resolution requests. If the storage system is associated with both IPv4 and IPv6 logical ports in the same DNS zone and the host interface card is configured with only IPv4 addresses, the host may fail to access the domain name. • The load balancing effect varies with the distribution of logical ports associated with a DNS zone. To obtain a better load balancing effect, ensure that logical ports associated with a DNS zone are evenly distributed among controllers. • If a HyperMetro vStore pair has been created for the owning vStore, you can only select the DNS zones with the same owning site.

Step 5 Click **OK**.

----End

3.8.3.4.5 (Optional) Configuring DNS Load Balancing Parameters

The DNS load balancing feature can detect loads on various IP addresses on a storage system in real time and use a proper IP address as the DNS response to achieve load balancing among IP addresses.

Prerequisites

- If the storage system connects to an external DNS server, the external DNS server has been configured and is running properly.
- If the storage system directly connects to a host, DNS client configurations have been set on the host.
- Port 53 for the TCP/UDP protocol between the storage system and the DNS server or host is enabled.

Context

- DNS load balancing applies to scenarios where a large number of NAS service IP addresses or NAS clients are involved. If only a small number of (for example, less than 20) NAS service IP addresses or NAS clients are involved, you are advised to directly use service IP addresses to mount shares.
- Working principle:
  a. When a host accesses the NAS service of a storage system using a domain name, the host first sends a DNS request to the built-in DNS server and the DNS server obtains the IP address according to the domain name.
  b. If the domain name contains multiple IP addresses, the storage system selects the IP address with a light load as the DNS response based on the configured load balancing policy and returns the DNS response to the host.
  c. After receiving the DNS response, the host sends a service request to the target IP address.
- When DNS load balancing resolves a domain name, a specific domain name resolution record is added. The following records are supported:
  – A record: added if a domain name points to an IPv4 address (for example, 192.168.20.10).
  – AAAA record: added if a host name (or domain name) points to an IPv6 address (for example, ff03:0:0:0:0:0:0:c1).
  – PTR record: reverse of an A or AAAA record for implementing reverse DNS lookups.
- DNS load balancing supports only the UDP protocol for domain name resolution.

Procedure

Step 1 Choose **Settings** > **Basic Information** > **DNS Service**.

Step 2 Enable **File Service DNS Load Balancing**.

1. Set the DNS load balancing policy. The storage system supports the following load balancing policies:

NOTE

- **Weighted round robin** applies to scenarios where the load of storage devices is light or unknown, for example, in the scenario where shares are initially mounted to a large number of NAS clients.
- Other policies apply to scenarios where users want to balance loads based on a certain indicator (such as CPU usage, port bandwidth, number of connections, and overall loads) of running services, for example, in the scenario where shares are mounted to NAS clients in batches during capacity expansion of client applications.

- **Weighted round robin**: IP addresses which process loads and are under the same domain name are randomly selected for processing.
- **CPU usage**: The CPU usage of each node determines the weight. The storage system uses the weight to select a node to process client services.
- **Port bandwidth usage**: The total bandwidth usage of each node determines the weight. The storage system uses the weight to select a node to process client services.
- **Connections**: The NAS connections of each node determine the weight. The storage system uses the weight to select a node to process client services.
- **Overall loads**: The overall load of CPU usage, bandwidth usage, and number of NAS connections determines node selection. Less loaded nodes are more likely to be selected.

2. Click **Save**.

----End

Follow-up Procedure

After associating logical ports with a DNS zone, configuring logical ports to listen to DNS requests, setting a DNS load balancing policy, and enabling DNS load balancing, you need to configure DNS server addresses on clients. For details about how to configure and use DNS load balancing, see **5.1 How Can I Configure and Use DNS Load Balancing?**

3.8.3.4.6 (Optional) Managing the Routes of a Logical Port

When configuring share access, ensure that the logical port can ping the IP addresses of the domain controller, DNS server, and clients. If the ping test fails, add routes from the IP address of the logical port to the network segment of the domain controller, DNS server, or clients.

Prerequisites

A logical port has been configured with an IP address.

Procedure

Step 1 Choose **Services** > **Network** > **Logical Ports**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Select the desired logical port and click **Manage Route**.

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

NOTE

Alternatively, perform either of the following operations to go to the **Manage Route** page:

- Click **More** on the right of the desired logical port and select **Manage Route**.
- Click the name of the desired logical port. In the upper right corner of the page that is displayed, click **Manage Route** from the **Operation** drop-down list.

Step 4 Configure the route information for the logical port.

1. In the **IP Address** drop-down list, select the IP address of the logical port for which you want to add a route.
2. Click **Add**.
3. Set the parameters listed in **Table 3-45**.

Table 3-45 Route parameters

Parameter	Description
Type	Three types of routes are available: – **Default route** A route through which data is forwarded by default if no preferred route is available. The destination address and mask (IPv4) or prefix (IPv6) of the default route are automatically set to 0. To use this option, you only need to add a gateway. – **Host route** A route to a host. The destination mask (IPv4) or prefix (IPv6) of the host route are automatically set to 255.255.255.255 or 128. To use this option, you only need to add the destination address and gateway. – **Network segment route** A route to a network segment. You must add the destination address, destination mask (IPv4) or prefix (IPv6), and gateway.
Destination Address	IPv4 address, IPv6 address, or network segment of the destination service network port on the application server or destination logical port on another storage system.
Subnet Mask/ Prefix	Subnet mask of the IPv4 address or prefix of the IPv6 address for the destination service network port on the application server or destination logical port on another storage system.
Gateway	Gateway where the local logical port's IP address resides. **NOTE** The IP address of the gateway must be different from all internal heartbeat IP addresses. Otherwise, routing will fail.

4. Click ✓. The route information is added to the list.

NOTE

Click 🗑 on the right of a desired route to delete it.

Step 5 Click **Close**.

----End

3.8.3.5 (Optional) Configuring the CIFS Service

This section describes how to configure CIFS service parameters.

Context

The configured CIFS service parameters take effect for all CIFS shares of a vStore. If the configuration of a single CIFS share is inconsistent with that of the vStore, the vStore parameters prevail.

Procedure

Step 1 Choose **Settings** > **File Service** > **CIFS Service**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Click **Modify** in the upper right corner of the page.

Step 4 Set basic parameters for the CIFS service.

Table 3-46 describes the parameters.

Table 3-46 Basic parameters of the CIFS service

Parameter	Description
SMB3 Encryption	Specifies whether to enable SMB3 encryption. After this function is enabled, the system encrypts the shares to ensure data security, but the performance deteriorates. **NOTICE** Enabling this function affects SMB3 service performance. Check whether this function needs to be enabled. **NOTE** After SMB3 encryption is enabled, only SMB3 clients can access shares by default.
Unencrypted Client Access	After this function is enabled, clients that do not have encryption capabilities can access the shares. **NOTICE** After this function is enabled, clients of earlier versions (for example, Windows 7) are allowed to access shares where SMB3 encryption is enabled in plaintext. Check whether this function needs to be enabled. **NOTE** This function takes effect only after the SMB3 encryption function is enabled.
Symbolic Link	After this function is enabled, CIFS clients can access symbolic links created on UNIX clients (for example, symbolic links created through NFS clients). However, performance may deteriorate after this function is enabled.

Parameter	Description
Notify	After this function is enabled, a client's operations on a directory, such as adding a directory, adding a file, modifying the directory, and modifying a file, can be detected by other clients that are accessing this directory or the parent directory of this directory. The created or modified directories and files are visible after the page automatically refreshes. **NOTE** Only 6.1.5 and later versions support this parameter.
Oplock	Oplock: a mechanism. It is used to dynamically adjust cache policies of clients to improve 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. **NOTE** Only 6.1.5 and later versions support this parameter.
Signature Enforcement	After this function is enabled, servers forcibly use the signature function no matter whether clients enable the signature function, enhancing CIFS share access security. **NOTE** Only 6.1.5 and later versions support this parameter.
ABSE	After access based share enumeration (ABSE) has been enabled, when users view the CIFS share information, the system displays only the CIFS shares that the users have permissions to access. **NOTE** ● It takes 10 to 20 minutes to load the CIFS share permission information after the storage system is powered on. During this period, the function does not take effect. ● You are advised to enable this function. If this function is disabled, users can find all shares (including the shares for which the users do not have access permission), which may cause security threats to other shares. ● Only 6.1.5 and later versions support this parameter.

Parameter	Description
Guest	After this function is enabled, users can access shared directories without entering usernames or passwords and have the permission of the Everyone user group that has been added when the CIFS shares were created. **NOTE** • After this function is enabled, unauthorized users can access shared directories as guest users, which may cause information security risks. You are advised to disable this function. • Only 6.1.5 and later versions support this parameter.

Step 5 Click **Save**.

----End

3.8.3.6 Configuring a Local Authentication User (Group)

In a non-domain environment, you must configure a local authentication user (group). The storage system enables you to allocate different share access permissions to different users (groups).

3.8.3.6.1 (Optional) Creating a Local Authentication User Group

This section describes how to create a local authentication user group. Local authentication user groups are used to control the share access permissions of specific local authentication users.

Context

A system has nine local authentication user groups that are automatically created. The nine user groups are reserved for the system and cannot be modified or deleted:

- **Administrators** is the administrator group. When the group members access a shared namespace in the storage system, they do not need to be authenticated by share-level ACLs and NT ACLs. They can operate any file in any share with administrator permissions without the need to be authenticated.
- Other user groups are common user groups. When the group members access a shared file system of the storage system, they can have the corresponding permissions only after being authenticated.

NOTE

An access control list (ACL) is a collection of permissions that are authorized to users or user groups to operate shared files. ACL permissions are classified into ACL storage permissions and ACL authentication permissions. After a user logs in to a share, the system determines the user's permissions on the share, reads the ACL permissions, and then determines whether the user can read and write files. For ACL storage permissions, each ACL permission is called an Access Control Entry (ACE). After a share is mounted to a Windows client, the client sends NT ACLs to the server (storage system that provides the share).

Procedure

Step 1 Choose **Services** > **File Service** > **Authentication Users** > **Windows Users** > **Local Authentication User Groups**.

Step 2 Select the vStore for which you want to create a local authentication user group from the **vStore** drop-down list in the upper left corner.

Step 3 Click **Create**.

The **Create Local Windows Authentication User Group** page is displayed on the right.

Step 4 Set basic parameters for the local authentication user group.

Table 3-47 describes the parameters.

Table 3-47 Basic local authentication user group parameters

Parameter	Description
Name	Name of the local authentication user group. [Value range] • The name must be unique. • The name cannot contain "/[]:|<>+=;?*@, or control characters, and cannot end with a period (.). If the name starts or ends with a space, the space is not displayed after the name is created. • The name can contain case-insensitive letters. For example, **aa** and **AA** cannot be created at the same time. • The user group name cannot be the same as the name of a local authentication user. • The name contains 1 to 256 characters.
Description	Description of the local authentication user group. [Value range] The description can be left blank or contain up to 256 characters.

Step 5 Select privileges for the local authentication user group. You can view details about the privileges in the description.

Step 6 Click **OK**.

----End

3.8.3.6.2 Creating a Local Authentication User

This section describes how to create a local authentication user. For applications that use local authentication, local authentication users are used to access shares. You can add a local authentication user to a user group for authentication and access a share as the user group.

Procedure

Step 1 Choose **Services** > **File Service** > **Authentication Users** > **Windows Users** > **Local Authentication Users**.

Step 2 Select the vStore for which you want to create a local authentication user from the **vStore** drop-down list in the upper left corner.

Step 3 Click **Create**.

The **Create Local Windows Authentication User** page is displayed on the right.

Step 4 Set basic parameters for the local authentication user.

Table 3-48 describes the parameters.

Table 3-48 Basic local authentication user parameters

Parameter	Description
Name	Name of the local authentication user. [Value range] • The name must be unique. • The name cannot contain "/\][:;|=,+*?<>@, spaces, or control characters, and cannot end with a period (.). • The name can contain case-insensitive letters. For example, **aaaaaaaa** and **AAAAAAAA** cannot be created at the same time. • The name cannot be the same as the name of a local authentication user group. • The name contains 3 to 20 characters. **NOTE** You can modify the minimum length of the user name on the **Set Security Policy** page.

Parameter	Description
Password	Password of the local authentication user. [Value range] • The password contains 8 to 32 characters. • The password must contain at least one of the following types: special characters, uppercase letters, lowercase letters, and digits. Special characters include !"#$%&'()*+,-./:;<=>?@[\]^`{_|}~ and spaces. • The password cannot contain three consecutive identical characters. • The password cannot be the same as the user name or the user name spelled backward. **NOTE** You can set security policies for the password of a local authentication user on the **Set Security Policy** page. If **Validity Period** is **0**, the password will never expire. For the security purpose, you are advised to set a specific password validity period. After the password expires, you cannot access shares, but you can set a password again or modify the password security policy on the **Set Security Policy** page.
Confirm Password	Confirms the password for consistency.
Status	Indicates whether to enable the user.
Description	Description of the local authentication user. [Value range] The description can be left blank or contain up to 256 characters.
Owning Groups	Groups to which the local authentication user belongs. Click ▸ on the right of **Owning Groups**. In the **Available Groups** list, select the desired groups and add them to **Selected Groups**.

NOTE

You cannot configure privileges for local authentication users separately on DeviceManager. Instead, you can configure privileges for local authentication users on the CLI.

Step 5 Click **OK**.

----End

3.8.3.7 Adding a Storage System to an AD Domain

After a storage system is added to an AD domain, domain users can access CIFS shares that are allocated to the domain. This section describes how to add a storage system to an AD domain.

3.8.3.7.1 Preparing AD Domain Configuration Data

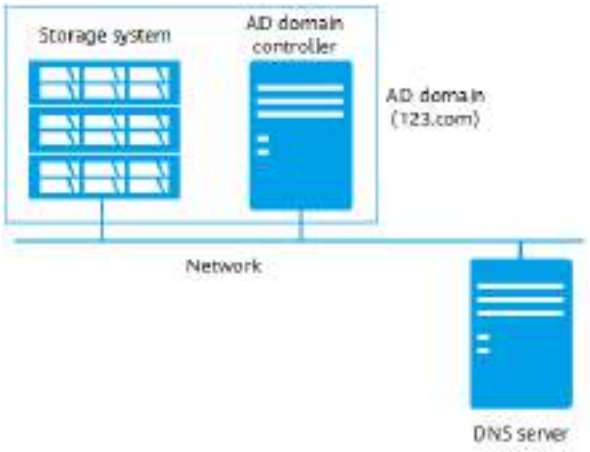
Why AD Domains?

In Windows shared mode, every device that provides shares is an independent node. The account and permission information about users allowed to access shares are stored on each node. As a result, the information maintenance is complex and uncontrollable.

If an AD domain is used, however, the domain controller manages all the user configuration information and authenticates the access to the domain. The domain controller incorporates a database that stores information about the domain account, password, and nodes in the domain. A user can access all the shared content in the domain after passing the authentication by the domain controller.

Working Principles

Figure 3-6 Network diagram of AD domain server authentication



1. The DNS server provides a full domain name (123.com for example) for the AD domain.
2. The storage system is added into the AD domain and provides share services.
3. Users can access shares after logging in to hosts in the AD domain using domain accounts.

Data Preparation

To smoothly add a storage system to an AD domain, prepare or plan the required data based on the site requirements. Collect **Domain Administrator**, **Password**, **Full Domain Name**, **Organization Unit** (optional), and **System Name**. For details about how to obtain the data, see **3.8.3.7.3 Configuring AD Domain Authentication Parameters**.

3.8.3.7.2 Connecting a Storage System to a DNS Server

After a storage system is connected to a DNS server, the storage system can access the AD domain server using a domain name. This operation enables you to configure the IP address of the DNS service for the file storage service.

Prerequisites

- A DNS server has been configured and is running properly.
- Port 53 for the TCP/UDP protocol between the storage system and the DNS server is enabled.

Context

- A DNS server is used to resolve names of hosts in a domain.
- If you want to configure a standby DNS server, keep the domain names of the active and standby servers consistent.

Procedure

Step 1 Choose **Services** > **vStore Service** > **vStores**.

Step 2 Click the name of the desired vStore. On the details page that is displayed on the right, click the **File Service** tab and click **Configure** in the **DNS Service** area.

The **Configure DNS Service** page is displayed on the right.

Step 3 Configure an IP address for the DNS service.

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

   NOTE

   Set **Standby DNS IP Address 1** first and then **Standby DNS IP Address 2**.
4. (Optional) Test the connectivity between the DNS server and the storage system.
   - You can click **Test** next to a DNS IP address to test its availability.
   - You can click **Test All** to test the connectivity between the DNS server and the storage system.

Step 4 Set DNS domain names.

NOTE

Domain names are used in sequence. A maximum of six domain names are supported.

- Adding a domain name
  a. Click **Add**.
  b. Set a domain name.

NOTE

The domain name must comply with the following rules:

- The domain name is case insensitive and must be unique.
- The domain name contains 1 to 255 characters, including only letters (a to z and A to Z), digits (0 to 9), periods (.), underscores (_), and hyphens (-).
- A domain name is separated by periods into several segments. Each segment cannot exceed 63 characters and must start or end with a letter or digit.

- Modifying a domain name
  a. Click the domain name to be modified.
  b. Set a domain name.

NOTE

The domain name must comply with the following rules:

- The domain name is case insensitive and must be unique.
- The domain name contains 1 to 255 characters, including only letters (a to z and A to Z), digits (0 to 9), periods (.), underscores (_), and hyphens (-).
- A domain name is separated by periods into several segments. Each segment cannot exceed 63 characters and must start or end with a letter or digit.

- Removing a domain name

  Click on the right of the domain name to be deleted.
- Moving up a domain name

  Click on the right of the domain name to be moved up.
- Moving down a domain name

  Click on the right of the domain name to be moved down.

Step 5 Click **OK**. Confirm your operation as prompted.

----End

3.8.3.7.3 Configuring AD Domain Authentication Parameters

If an AD domain server is deployed on a customer's network, a storage device must join the AD domain. Then, CIFS clients need to be authenticated by the AD domain server when they attempt to access shared resources on the storage device. The administrator can manage the share access permissions and quotas of domain users. If the storage device does not join an AD domain, domain users cannot use share services provided by the storage device.

Prerequisites

- An AD domain has been set up.
- The storage system has been connected to the DNS server.
- The AD domain server and DNS server have time synchronization with the storage system. The time difference must be no larger than 5 minutes.

- Ports 88 (TCP/UDP protocol), 389 (TCP/UDP protocol), 445 (TCP protocol), and 464 (TCP/UDP protocol) are enabled between the storage system and the AD domain.

NOTE

The storage systems can connect to AD domain servers and DNS servers through management network ports or service network ports (logical ports). If a storage system connects to an AD domain server and DNS server through management network ports, ensure that the management network ports on at least two controllers can properly communicate with the AD domain server and DNS server. If a storage system connects to the AD domain server and DNS server through service network ports, it is recommended that the service network ports on at least two controllers can properly communicate with the AD domain server and DNS server. It is recommended that storage systems connect to AD domain servers through service network ports.

Precautions

- Before adding a storage system to an AD domain, ensure that the primary controller of the storage system is connected to the DNS server and AD domain server.
- When **Overwrite System Name** is enabled, if a system name entered exists in the AD domain controller, the information about the current storage system will overwrite the information about the storage system corresponding to the system name on the AD domain controller.
- A simple password may result in security issues. A complex password that contains uppercase letters, lowercase letters, digits, and special characters is recommended.
- You are advised to use physical isolation and end-to-end encryption to ensure security of data transfer between the AD domain server and clients.

Procedure

Step 1 Choose **Settings** > **User and Security** > **Domain Authentication** > **File Service AD Domain**.

Step 2 Select a desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 View AD domain parameters of the file service. **Table 3-49** describes the parameters.

NOTE

- On the file service AD domain management page, click  to refresh file service AD domain information.
- On the file service AD domain management page, click  and select the file service AD domain information you want to view.

Table 3-49 AD domain parameters of the file service

Parameter	Description
Full Domain Name	Indicates the full domain name of the AD domain server.

Parameter	Description
Organization Unit	Indicates the organization unit of a type of directory objects in the domain. These objects include users, computers, and printers.
System Name	Indicates the name of the storage system in the AD domain.
Domain Status	Indicates whether the storage system is added to the domain.

Step 4 Configure the file service AD domain.

1. Select the AD domain to be configured and click **Configure**.

   The **Configure File Service AD Domain** page is displayed on the right.

   NOTE

   Alternatively, choose **Services** > **vStore Service** > **vStores** and click the name of a vStore. On the details page that is displayed on the right, select the **File Service** tab and click **Configure** in the **AD Domain** area.

2. Configure basic information. **Table 3-50** describes the parameters.

Table 3-50 Basic information about the file service AD domain

Parameter	Description
Domain Administrator	Indicates the user name of the AD domain server administrator. The following formats are supported: 1. User name, for example, **test_user1**. 2. NetBIOS name + user name. You can run the **nbtstat -n** command to query the NetBIOS name. For example, **china\test_user1**. **NOTE** This function is supported only in 6.1.5 and later versions. 3. User name + AD domain name, for example, **test_user1@china.com**. **NOTE** This function is supported only in 6.1.5 and later versions. [Value range] A string of 1 to 63 characters. [Example] test_user1
Password	Indicates the password of the AD domain server administrator. [Value range] A string of 1 to 127 characters.

Parameter	Description
Full Domain Name	Indicates the full domain name of the AD domain server. **NOTE** You can click **Test** to test the validity of the full domain name. [Value range] A string of 1 to 127 characters. [Example] abc.com
Organization Unit	Indicates the organization unit of a type of directory objects in the domain. These objects include users, computers, and printers. After an object joins the domain, it will be a member in the organization unit. If this parameter is left empty, objects join the **Computers** organization unit by default. [How to obtain] 1. On the Windows AD domain server, open **Active Directory Users and Computers** or **ADSI Edit**. 2. Select the directory on the left, right-click the directory, and choose **Properties**. 3. In the **Properties** dialog box that is displayed, click **Attribute Editor**. The value of **distinguishedName** is the organization unit. [Example] cn=xxx,dc=abc,dc=com
System Name	Indicates the name of the storage system in the AD domain. After the storage system is added to the domain, the client can use the name to access the storage system. **NOTE** – If the system name used for joining the domain exists in the domain controller and the **Overwrite System Name** function is disabled in the storage system, joining the AD domain will fail. – Special characters ~!$%^&{}`' are not recommended because the domain name of the DNS server does not support these characters. – English characters and digits are recommended. [Value range] A string of 1 to 15 characters. [Example] test2021

Parameter	Description
Overwrite System Name	If a storage system with the same name exists in the domain controller, enabling this function will overwrite the original storage system information. **NOTICE** After this function is enabled, information about the storage system with the same system name in the domain controller will be overwritten. As a result, the authentication between the storage system and domain controller corresponding to the system name will be affected.
Domain Status	Indicates whether the storage system is added to the domain.

3. Click **Join Domain**.
4. If you want to remove a storage system from an AD domain, perform the following operations:
   a. Set **Domain Administrator** and **Password**.
   b. Click **Exit Domain**.
      Confirm your operation as prompted.
5. Click **Close**.

----End

Follow-up Procedure

- After adding a storage system to an AD domain that has multiple domain controllers, you are advised to wait about 2 minutes for these domain controllers to synchronize configurations and then access shares as a domain user.
- After the storage system is removed from the AD domain, you are advised to wait for about 2 minutes before adding the storage system to the AD domain.

3.8.3.8 Creating a CIFS Share

This section describes how to share file systems in CIFS mode so that users can access the file systems.

Procedure

Step 1 Choose **Services** > **File Service** > **Shares** > **CIFS Shares**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Click **Create**.

The **Create CIFS Share** page is displayed on the right.

NOTE

The screenshot is for reference only and the actual displayed information may vary.

For some device models, you can click in the upper right corner of the page to enable SmartGUI. SmartGUI mines users' historical operation data and builds a configuration parameter recommendation model based on user profiles to recommend configuration parameters for the block service and file service. After SmartGUI is enabled, the system presets the **File System** and **Share Name** parameters based on recommendations when you create a CIFS share. You can directly use the parameters or modify them as required.

Step 4 Set basic CIFS share parameters.

Table 3-51 describes the parameters.

Table 3-51 Basic CIFS share parameters

Parameter	Description
File System	File system for which you want to create a CIFS share. **NOTE** If the selected file system is the secondary storage system in a remote replication pair or remote storage system in a HyperMetro pair, data in the file system is probably being modified when it is accessed. Before performing this operation, confirm that the application allows possible data inconsistency. [Example] Filesystem001
Dtree	Dtree for which you want to create a CIFS share. If you do not select a dtree, the CIFS share is created for the entire file system. [Example] Dtree_test
Share Name	Name of the share, which is used by users to access shared resources. [Value range] • The name must be unique. • The name cannot contain characters " / \ [ ] : | < > + ; , ? * =, and cannot be **ipc$**, **autohome**, **~**, or **print$** reserved by the system. • The name contains 1 to 80 characters. [Example] share_for_user1
Share Path	Share path of the file system, which is generated based on the **File System** and **Dtree** parameters. [Example] /Filesystem001/Dtree_test

Step 5 Set advanced properties of the CIFS share. Select **Advanced** in the upper right corner.

Table 3-52 describes the parameters.

Table 3-52 Advanced parameters of a CIFS share

Parameter	Description
Description	Indicates the description of a CIFS share. **NOTE** The description can be left blank or contain up to 255 characters.

Parameter	Description
Notify	Determine whether to enable **Notify**. After this function is enabled, a client's operations on a directory, such as adding a sub-directory, adding a file, modifying the directory, and modifying a file, can be detected by other clients that are accessing this directory or the parent directory of this directory. The created or modified directories and files are visible after the page automatically refreshes.
Continuously Available	Determine whether to enable **Continuously Available**. This option provides the SMB continuous availability feature. This feature depends on Oplock which is enabled by default. If Oplock is disabled, choose **Settings** > **File Service** > **CIFS Service** to enable it.
SMB3 Encryption	Specifies whether to enable SMB3 encryption. After this function is enabled, the system encrypts the share to ensure data security, but the performance deteriorates. **NOTICE** Enabling this function affects SMB3 service performance. Check whether this function needs to be enabled. **NOTE** • After SMB3 encryption is enabled, only SMB3 clients can access shares by default. • Only 6.1.3 and later versions support this parameter.
Unencrypted Client Access	After this function is enabled, clients that do not have encryption capabilities can access the share. **NOTICE** After this function is enabled, clients of earlier versions (for example, Windows 7) are allowed to access shares where SMB3 encryption is enabled in plaintext. Check whether this function needs to be enabled. **NOTE** • This function takes effect only after the SMB3 encryption function is enabled. • Only 6.1.3 and later versions support this parameter.
ABE	After ABE is enabled, files and folders that users have no access permission are not displayed. **NOTE** • SMB2 and SMB3 support this function but SMB1 does not. • Only 6.1.3 and later versions support this parameter.
Show Snapshot	This function allows clients to show and traverse snapshot directories. **NOTE** Only 6.1.3 and later versions support this parameter.

Step 6 Select user or user groups that can access the CIFS share.

1. In the **Permissions** area, click **Add**.

The **Add User or User Group** page is displayed.

2. Select the type of the users or user groups.

   The value can be **Everyone**, **Local Windows authentication user**, **Local Windows authentication user group**, **AD domain user**, or **AD domain user group**.

   - If you select **Local Windows authentication user** or **Local Windows authentication user group**, select the users or user groups to be added from the list.

     NOTE

     You can click **Create** to create a local Windows authentication user or local Windows authentication user group.

   - If you select **AD domain user** or **AD domain user group**, enter the names of the users or user groups in **Name**.

     NOTE

     - If you select **AD domain user** or **AD domain user group**, the system automatically detects whether the AD domain has been configured. If no AD domain is configured, the system prompts you to configure an AD domain first.
     - A domain user name is in the format of *Domain name*|*Domain user name* and a domain user group name is in the format of *Domain name*|*Domain user group name*.
     - **Name** contains 1 to 256 characters. An AD domain user name cannot start with an at sign (@).
     - You can also enter multiple names separated by pressing **Enter**.

3. In **Permission**, select the permission granted for the users or user groups.

   Table 3-53 describes the permissions.

Table 3-53 CIFS share permissions

Permission	Forbidden	Read-Only	Read-Write	Full Control
Viewing files and subdirectories	X[a]	√[b]	√	√
Viewing file contents	X	√	√	√
Running executable files	X	√	√	√
Adding files or subdirectories	X	-[c]	√	√

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

NOTE

- The permission priority from high to low is **Forbidden** > **Full control** > **Read-write** > **Read-only**. The highest permission prevails. If a user is granted with a higher permission than its original one, 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 changed to **Full control** and it can access the CIFS share immediately without re-authentication.
- You can run the **change service cifs administrators_privilege=?** command on the CLI to modify permissions of members in the **Administrators** user group. For details about the command, see *Command Reference* of the desired version. In the command, the value of the **administrators_privilege** parameter can be **admin** (default), **default_group**, or **owner**.

  For local authentication users whose primary user group is **Administrators**, users with different **administrators_privilege** values have different permissions.

  - **admin**: When members in the **Administrators** user group access a shared file system in the storage system, they do not need to be authenticated by share-level ACLs and NT ACLs. They can operate any file in any share with administrator permissions without the need to be authenticated.
  - **default_group**: Members in the **Administrators** user group have the same permissions as members in the **default_group** user group.
  - **owner**: Members in the **Administrators** user group have the permissions to query and set file or directory ACLs and modify file or directory owners. When the group members access shared file systems, they need to be authenticated by directory- or file-level NT ACLs, but do not need to be authenticated by share-level ACLs.

  Modified permissions take effect only after users are re-authenticated on clients.

  You can run the **show service cifs** command on the CLI and check permissions of the **Administrators** user group in the **Administrators Privilege** field.

4. Click **OK**.

   The system adds the selected users or user groups to the **Permissions** list.

Step 7 Click **OK**.

----End

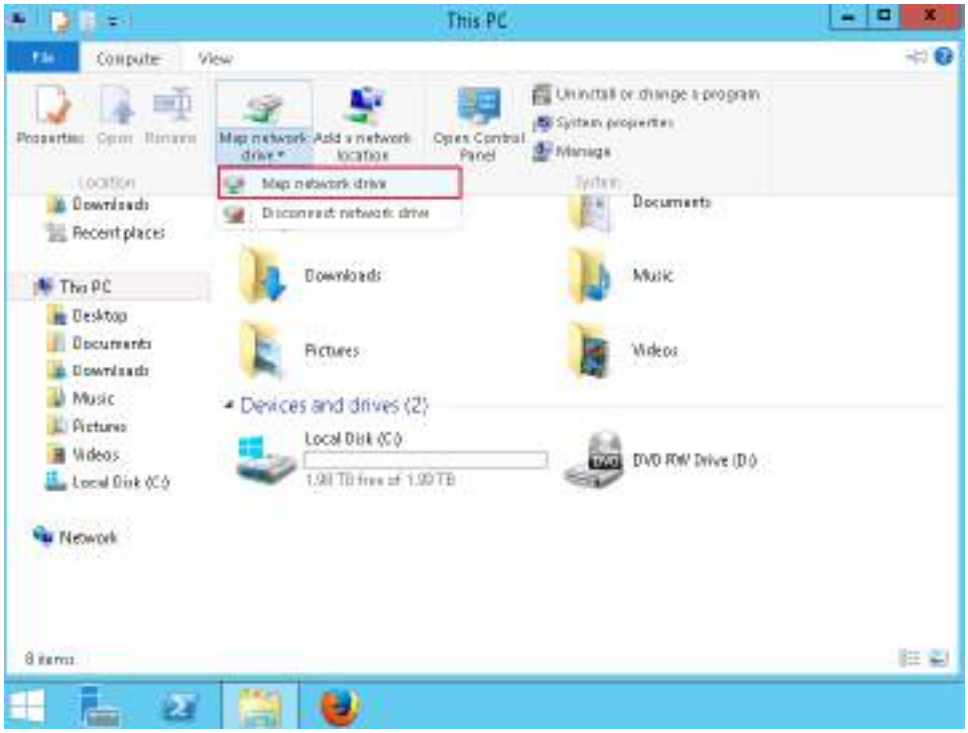
3.8.3.9 Accessing a CIFS Share

By accessing a CIFS share, different users can access the shared directories that they have permission to access.

Procedure

Step 1 Choose **Map network drive** on a Windows client.

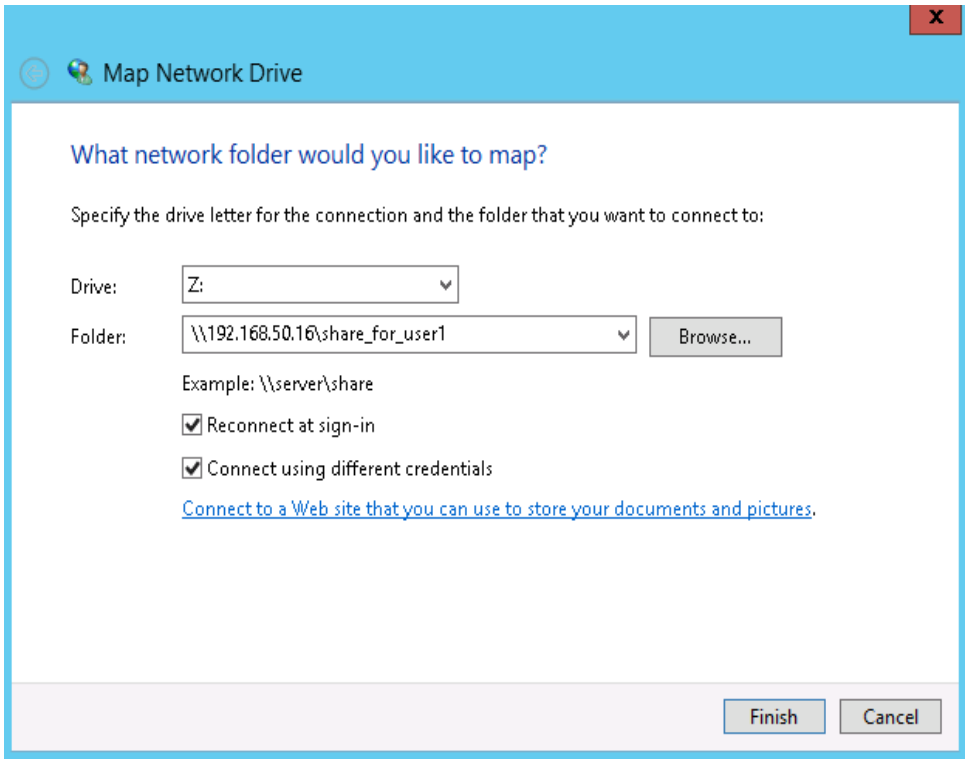
Take Windows Server 2012 as an example. Open **File Explorer** and choose **Computer** > **Map network drive** > **Map network drive**.



NOTE

GUIs may be slightly different for clients running different versions of Windows operating systems. The actual GUIs prevail.

Step 2 In the displayed **Map Network Drive** dialog box, configure the network folder you want to map.

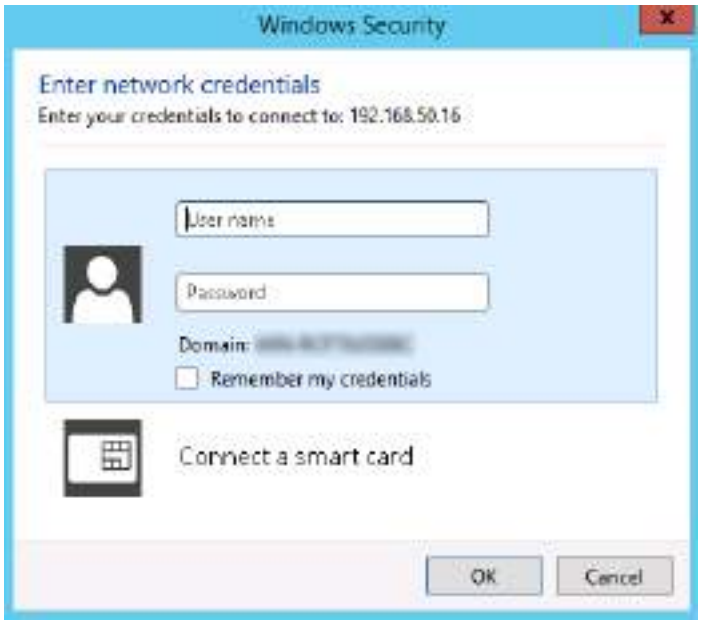


- In **Drive**, specify the drive letter for the connection.
- In **Folder**, specify the folder that you want to connect to. Select **Connect using different credentials** and click **Finish**.

  The folder is in the format of ***logical ip address**sharename***.

  Wherein, **logical ip address** indicates the IP address of the storage system's logical port providing the CIFS share, and **sharename** indicates the name of the CIFS share.

Step 3 In the displayed **Windows Security** dialog box, enter the user name and password for accessing the CIFS share.



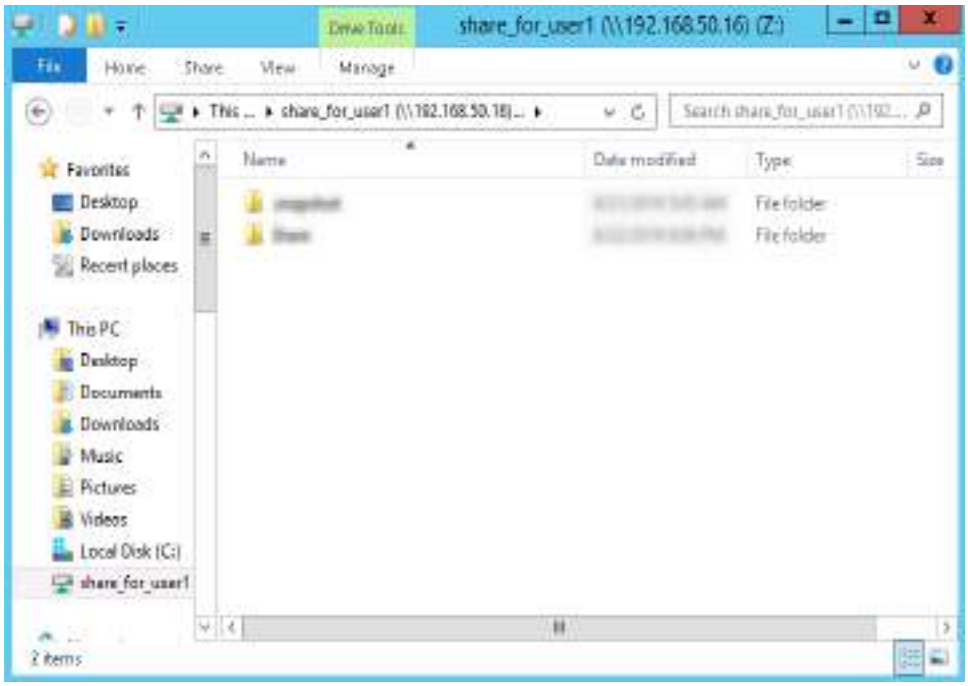
- If you log in as a domain authentication user, enter the domain user name in the *Domain name*|*Domain user name* format and the corresponding password.

NOTE

After CIFS shares are allocated to domain users, do not modify the domain user information. If you do, the CIFS shares cannot be accessed.

- If you log in as a local authentication user, enter the user name and password of the local authentication user.

Step 4 Click **OK**.



NOTE

If errors occur during the access, verify that:

- The storage system is added into a correct AD domain.
- The network between the client and storage system is normal.
- The domain user has the access permission.

----End

3.8.3.10 Connecting Microsoft Management Console to a Storage System

The Microsoft Management Console (MMC) built in a Windows client can manage users, user groups, shares, sessions, and open files for storage systems.

3.8.3.10.1 Introduction

MMC is a Windows tool that can provide a unified and standard management interface and operation platform for Windows administrators. With CIFS used, MMC can manage users, user groups, and shares for storage systems.

In large- and medium-sized NAS applications, multiple NAS servers from different vendors may be deployed. MMC can manage these servers in a unified way, improving management efficiency.

Table 3-54 lists the supported management functions.

Table 3-54 Management function list

Category	Function
CIFS share management	Enumerating shares **NOTE** Operators must have administrator privileges.
	Adding shares **NOTE** Restricted by Windows clients, a share folder path cannot be longer than 255 characters on MMC. If the path is longer than 255 characters, creating shares will fail.
	Viewing shares
	Modifying shares **NOTE** The descriptions, permissions, ACLs, and offline cache configurations of shares can be modified.
	Stopping sharing
User management	Enumerating users
	Viewing user information **NOTE** The user group to which users belong can be viewed.
	Changing the user group to which users belong
User group management	Creating user groups
	Enumerating user groups
	Viewing user group information **NOTE** Group members including domain users can be viewed.
	Changing group members **NOTE** Group members can be added to or removed from user groups.
	Modifying user group descriptions
	Renaming user groups
	Deleting user groups
Session management	Enumerating sessions
	Closing sessions

Category	Function
Open files management	Enumerating open files
	Closing open files

3.8.3.10.2 Logging In to MMC

After logging in to MMC, you can manage users, user groups, and shares.

Precautions

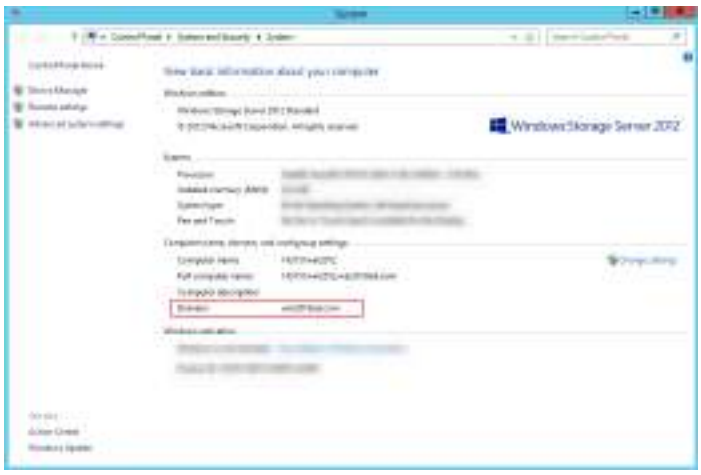
- If you will log in to a Windows client as a local user, ensure that another local user with the same user name and password has been created on the storage system and added to the **Administrators** user group.
- If you will log in to a Windows client as a domain user, ensure that:
  - The Windows client and storage system are added to the same AD domain.
  - The domain user is added to the **Administrators** user group of the Windows client.
  - The domain user is added to the **Administrators** user group of the storage system.

Procedure

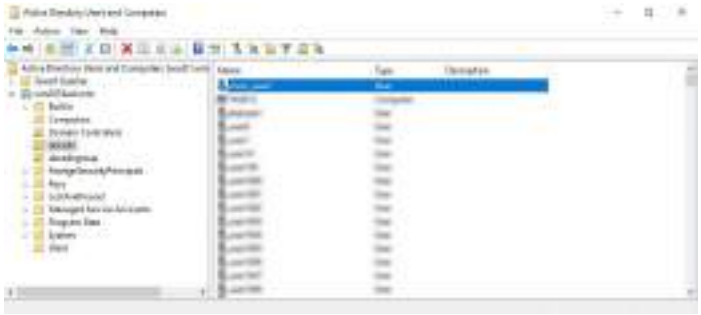
NOTE

The following uses the scenario where a domain user logs in to a Windows client as an example.

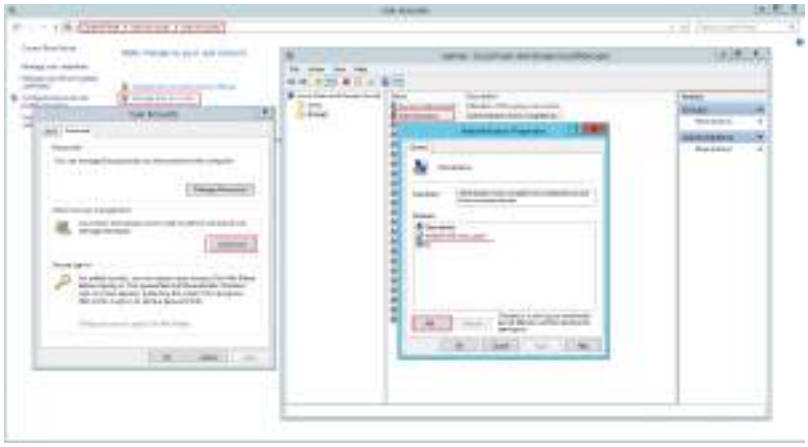
Step 1 Log in to the Windows client as an administrator and add the Windows client to the AD domain.



Step 2 On the AD domain controller, create a domain user (for example, **mmc_user1**).



Step 3 On the Windows client, add the domain user **mmc_user1** to the **Administrators** user group of the Windows client.



Step 4 On DeviceManager, add the storage system to the AD domain where the Windows client resides.

For details, see **3.8.3.7 Adding a Storage System to an AD Domain**.

Step 5 On DeviceManager, add the domain user **mmc_user1** to the **Administrators** user group of the storage system.

1. Choose **Services** > **File Service** > **Authentication Users** > **Windows Users** > **Local Authentication User Groups**.
2. Select the vStore to which the desired local authentication user group belongs from the **vStore** drop-down list in the upper left corner.
3. Click the name of the desired local authentication user group, that is **Administrators**.

The details about the **Administrators** user group are displayed on the right.

4. Click the **Members** tab. On the **AD Domain Users** tab, click **Add**.
   The **Add AD Domain User** page is displayed on the right.
5. In **Name**, enter the AD domain user name.

   NOTE

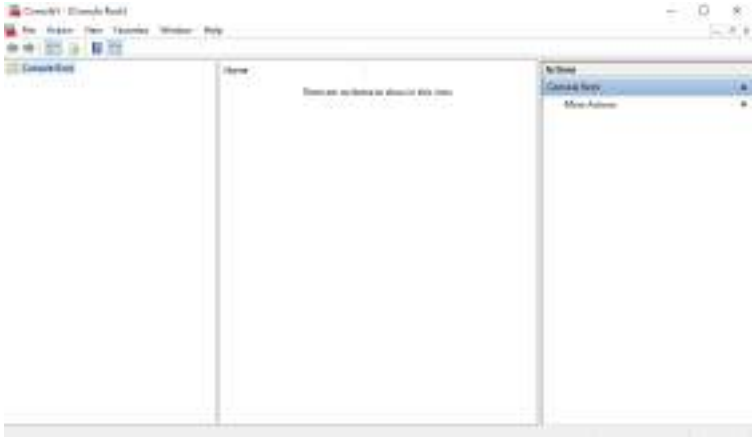
   - The name contains 1 to 256 characters.
   - The name format is *Domain name**Domain user name*.
   - You can enter multiple names separated by commas (,) or carriage returns.

   Example:
   win2019ad.com\mmc_user1
6. Click **OK**.

Step 6 Log in to the Windows client as the domain user **mmc_user1**.

Step 7 Choose **Start** > **Run**. In the text box that is displayed, enter **mmc**. Click the matching search result.

The MMC page is displayed.



NOTE

- Windows clients of different versions have different GUIs. The actual GUI prevails.
- You can also open the MMC console using the command **mmc** in Windows PowerShell.

----End

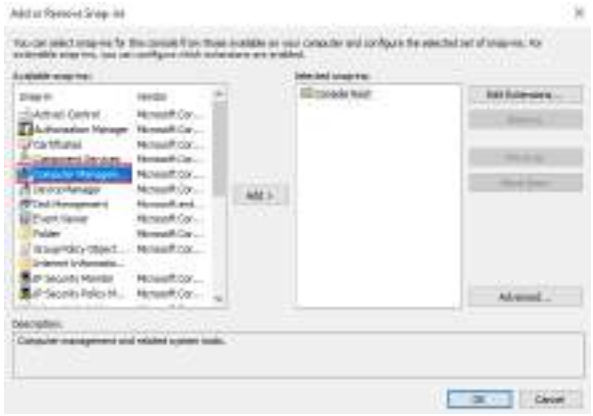
3.8.3.10.3 Adding Snap-ins

After logging in to the MMC, you need to add snap-ins to manage users/user groups and shares.

Method 1: Adding the Computer Management Snap-in

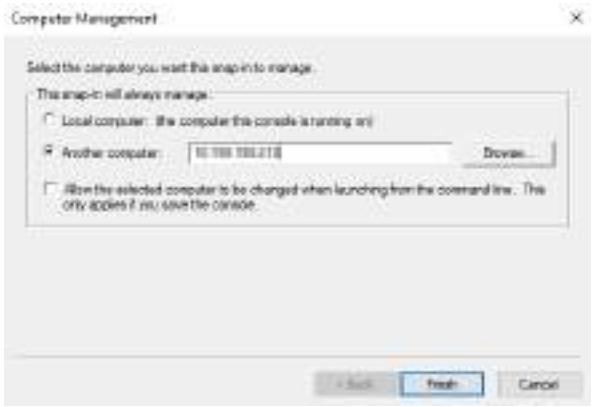
You can add the **Computer Management** snap-in first, and then manage users/user groups and shares through **Shared Folders** and **Local Users and Groups** in **System Tools**.

Step 1 Choose **File** > **Add/Remove Snap-ins**. In the dialog box that is displayed, select **Computer Management** and click **Add**.

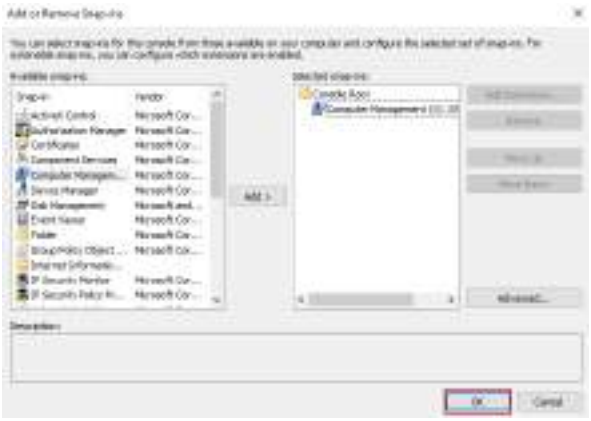


Step 2 In the dialog box that is displayed, select **Another computer**, enter the front-end service IP address of the storage system, and click **Finish**.

- The IP address can be an IPv4 or IPv6 address.
- Alternatively, you can enter **System Name** that is used when the storage system joins the AD domain.



Step 3 Click **OK**.



Step 4 Manage shares of the storage system.

In the navigation tree on the left, choose **Computer Management** > **System Tools**. The **Shared Folders** and **Local Users and Groups** snap-ins are displayed.

----End

NOTE

The **Share Folders** snap-in allows you to manage CIFS shares, sessions, and open files.

- To manage shares, see **3.8.3.10.4 Managing Shares**.
- To manage sessions, see **3.8.3.10.5 Managing Sessions**.
- To manage open files, see **3.8.3.10.6 Managing Open Files**.

The **Local Users and Groups** snap-in allows you to manage users and groups. For details, see **3.8.3.10.7 Managing Users and User Groups**.

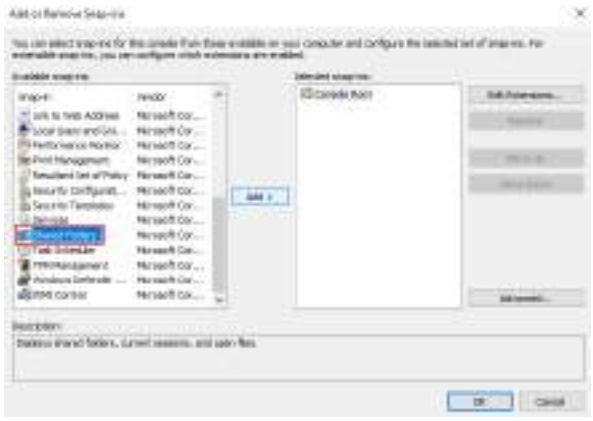
Method 2: Adding the Shared Folders and Local Users and Groups Snap-ins

Alternatively, you can add the **Shared Folders** and **Local Users and Groups** snap-ins to manage users/user groups and shares.

Adding Shared Folders

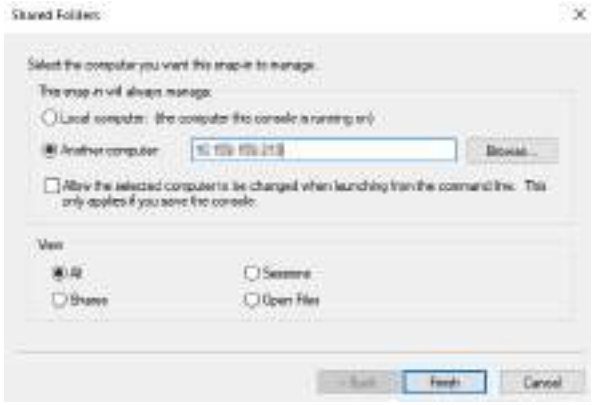
After you add the **Shared Folders** snap-in, you can manage CIFS shares, sessions, and open files.

Step 1 Choose **File** > **Add/Remove Snap-ins**. In the dialog box that is displayed, select **Shared Folders** and click **Add**.

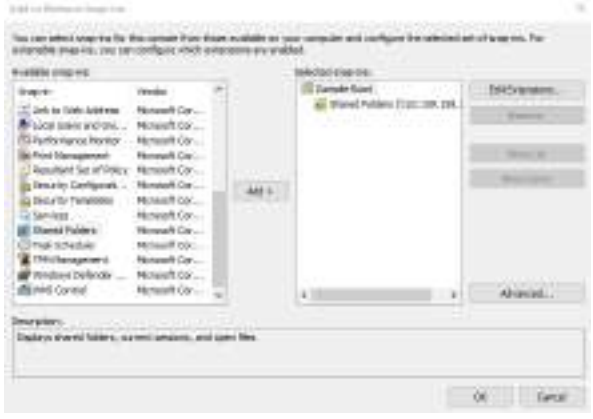


Step 2 In the dialog box that is displayed, select **Another computer**, enter the front-end service IP address of the storage system, and click **Finish**.

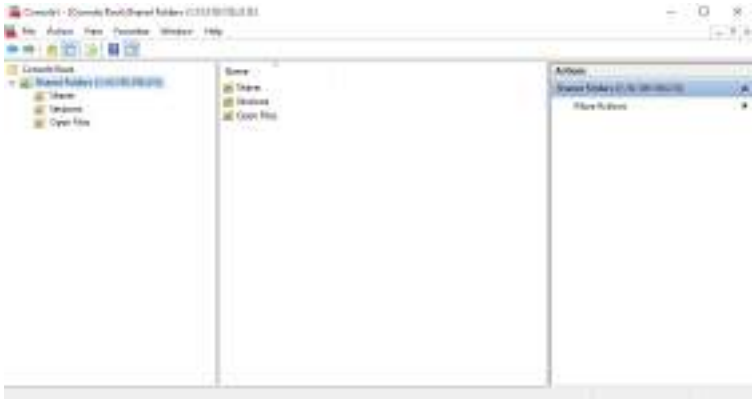
- The IP address can be an IPv4 or IPv6 address.
- Alternatively, you can enter **System Name** that is used when the storage system joins the AD domain.



Step 3 Click **OK**.



Step 4 Manage shares of the storage system.



----End

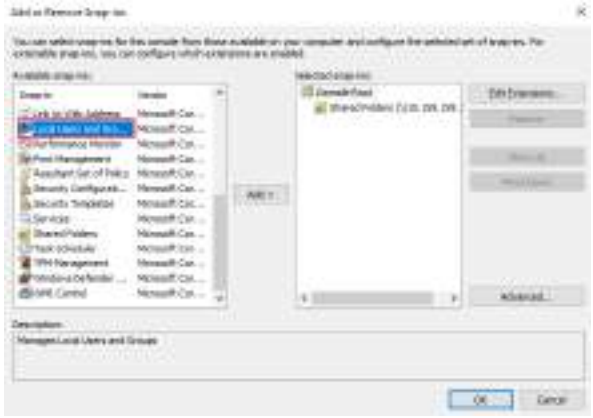
NOTE

- To manage shares, see **3.8.3.10.4 Managing Shares**.
- To manage sessions, see **3.8.3.10.5 Managing Sessions**.
- To manage open files, see **3.8.3.10.6 Managing Open Files**.

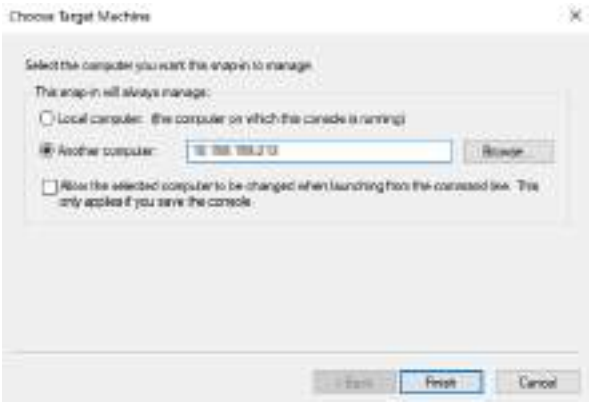
Adding Local Users and Groups

After you add the **Local Users and Groups** snap-in, you can manage users and groups.

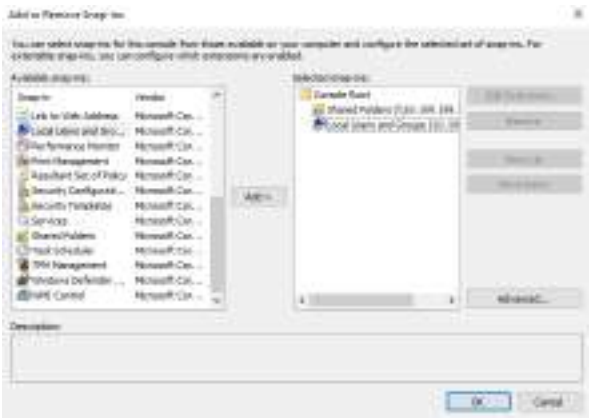
Step 1 Choose **File** > **Add/Remove Snap-ins**. In the dialog box that is displayed, select **Local Users and Groups** and click **Add**.



Step 2 In the dialog box that is displayed, select **Another computer**, enter the front-end service IP address of the storage system, and click **Finish**.



Step 3 Click **OK**.



Step 4 Manage users and user groups.

----End

NOTE

To manage users and groups, see **3.8.3.10.7 Managing Users and User Groups**.

3.8.3.10.4 Managing Shares

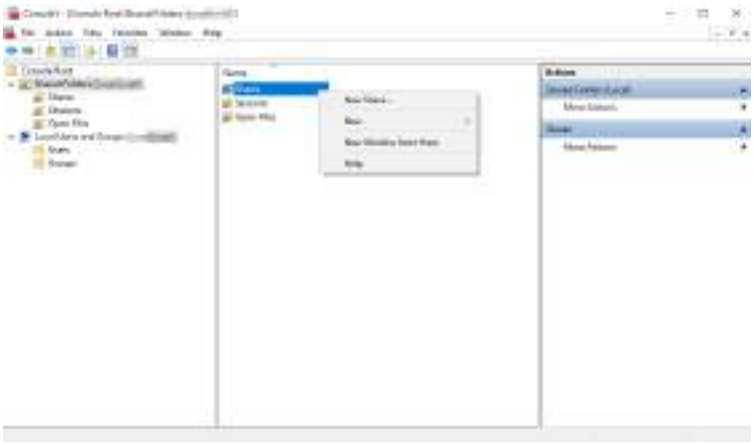
This section describes how to manage shares using MMC.

Prerequisites

- You have logged in to MMC.
- The local administrator account has been disabled on the client.

Procedure

- Create a share.
  a. Double-click **Shared Folders**.
  b. Right-click **Shares** and choose **New Share**.



  c. In the **Create a Shared Folder Wizard** dialog box, select a folder that you want to share from the storage system.
     - Restricted by Windows clients, a share folder path cannot be longer than 255 characters on MMC. If the path is longer than 255 characters, creating shares will fail.
     - You can click **Browse** to select a folder from the storage system.
  d. Click **Next** and enter **Share Name** and **Description**.
  e. Click **Next** and select permissions for the folder.
  f. Click **Finish**. In the **Sharing Was Successful** dialog box, click **Finish**.
     The created folder will be displayed on MMC.
- View a share.
  a. Choose **Shared Folders** > **Shares**.
     - In the right pane, all CIFS shares of the storage system are listed.
     - The client connection count of the share is fixed at 1. The actual value cannot be displayed at present.
  b. Right-click the share that you want to view and choose **Properties**. In the dialog box that is displayed, select **Share Permissions** to view the access permission for the share.
- Modify a share.
  a. Choose **Shared Folders** > **Shares**.
     In the right pane, all CIFS shares of the storage system are listed.
  b. Right-click the share that you want to modify and choose **Properties**.

c. In the dialog box that is displayed, select **General**. Modify **Description**.

NOTE

In the **User limit** area on the **General** tab page, retain the default value of **Maximum allowed**. The value of **Allow this number of users** does not take effect.

d. In the dialog box that is displayed, select **Share Permissions** and modify the permission for the share.

- Stop sharing.
  a. Choose **Shared Folders** > **Shares**.
     In the right pane, all CIFS shares of the storage system are listed.
  b. Right-click the folder that you want to stop sharing and choose **All Tasks** > **Stop Sharing**.
  c. In the dialog box that is displayed, click **Yes**.

3.8.3.10.5 Managing Sessions

You can use MMC to disconnect users and close sessions in shared folders.

Prerequisites

You have logged in to MMC.

Precautions

If you close sessions without notifying users, user data may be lost. Before closing sessions, notify the users.

When you use MMC to enumerate sessions, Windows will use the IP address of each session to parse the session as the corresponding computer name on the DNS server due to Windows restrictions. You must configure the record for the IP address of each session in the reverse lookup zone of the DNS server. Otherwise, MMC refresh will time out and no response will be returned.

Procedure

- View sessions.
  a. Choose **Shared Folders** > **Sessions**.
     Details about all current sessions will be displayed in the right pane.

- Close a session.
  a. Choose **Shared Folders** > **Sessions**.
     Details about all current sessions will be displayed in the right pane.
  b. Right-click the session you want to close and choose **Close Session** from the shortcut menu.
     A confirmation dialog box is displayed.
  c. Click **Yes**.
     The session is closed.

NOTE

If you want to close all sessions, right-click **Sessions** and choose **Disconnect All Sessions** from the shortcut menu.

3.8.3.10.6 Managing Open Files

You can use MMC to close open files in shared folders.

Prerequisites

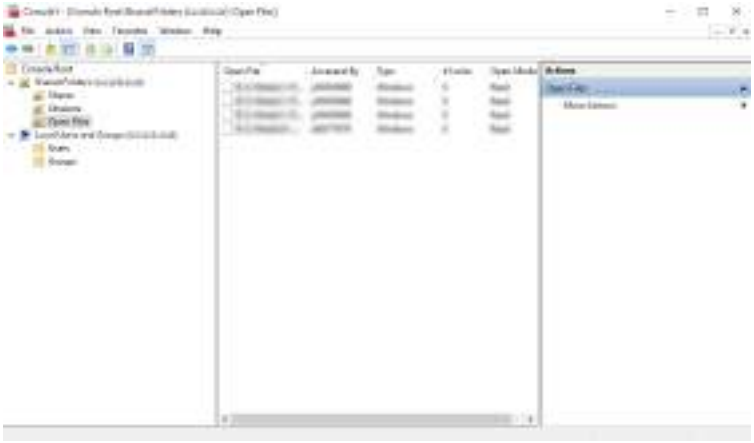
You have logged in to MMC.

Precautions

When you close an open file or folder, the users who connect to the file or folder will be disconnected and user data may be lost. Before closing open files, notify the users.

Procedure

- View open files.
  a. Choose **Shared Folders** > **Open Files**.
     All files that are opened currently will be displayed in the right pane.



- Close an open file.
  a. Choose **Shared Folders** > **Open Files**.
     All files that are opened currently will be displayed in the window on the right.

b. Right-click the file you want to close and choose **Close Open File** from the shortcut menu.

A confirmation dialog box is displayed.

c. Click **Yes**.

The open file is closed.

NOTE

If you want to close all open files, right-click **Open Files** and choose **Disconnect All Open Files** from the shortcut menu.

3.8.3.10.7 Managing Users and User Groups

This section describes how to manage users and user groups using MMC.

Prerequisites

- You have logged in to MMC.
- The local administrator account has been disabled on the client.
- The client and storage system have joined the same AD domain.

Managing Users

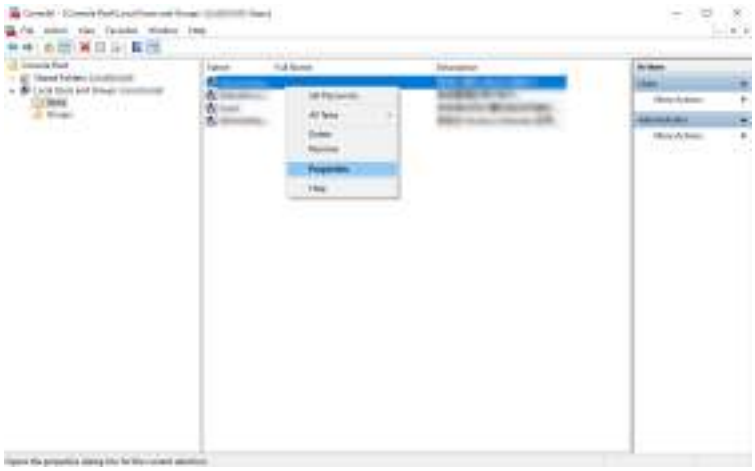
- View the user.
  a. Choose **Local Users and Groups (Local)** > **Users**.

  All users will be displayed in the right pane.

  NOTE

  Users cannot be created on the **Users** page of the MMC.

  b. Right-click the user that you want to view and choose **Properties** to view the user details.

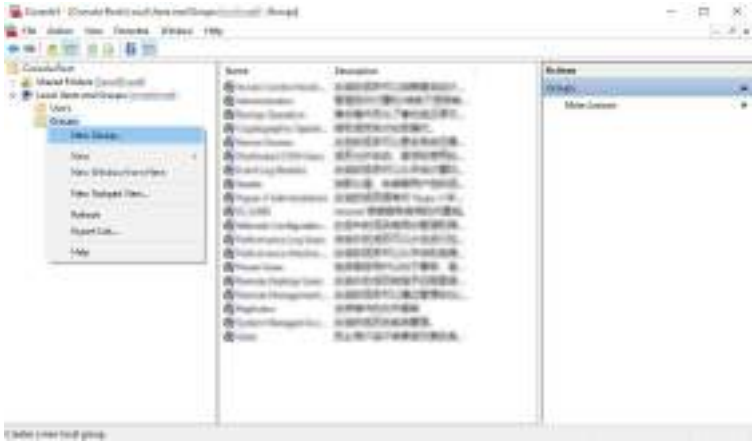


- Modify users.
  a. Choose **Local Users and Groups (Local)** > **Users**.
  b. Right-click the user that you want to modify and choose **Properties** > **Member of**.
  c. Select the user group to which the user belongs and click **Remove**.

d. Click **OK** for the change to take effect.

Managing User Groups

- Create a user group.
  a. Choose **Local Users and Groups (Local)** > **Groups**.
  b. Right-click **Groups** and choose **New Group**. Enter user information as instructed and click **Create**.



NOTE

A Windows reserved account cannot be created via MMC.

- View the user group.
  a. Choose **Local Users and Groups (Local)** > **Groups**.
  All user groups will be displayed in the right pane.
  b. Right-click the user group that you want to view and choose **Properties** to view the user group details.
- Modify user groups.
  a. Choose **Local Users and Groups (Local)** > **Groups**.
  b. Right-click the user group that you want to modify, choose **Properties**, and click **Add** to add users to the user group.
  c. Select the user that you want to remove from the user group and click **Remove**.
  d. Modify **Description**.
  e. Click **OK** for the change to take effect.

NOTE

The description of a Windows reserved user group cannot be modified via MMC.

- Rename user groups.
  a. Choose **Local Users and Groups (Local)** > **Groups**.
  b. Right-click the user group that you want to rename and select **Rename**.
  c. Enter the new user group name.
- Delete user groups.
  a. Choose **Local Users and Groups (Local)** > **Groups**.

b. Right-click the user group that you want to delete and select **Delete**.

c. Read and confirm the risk disclosure statement. In the dialog box that is displayed, click **Yes**.

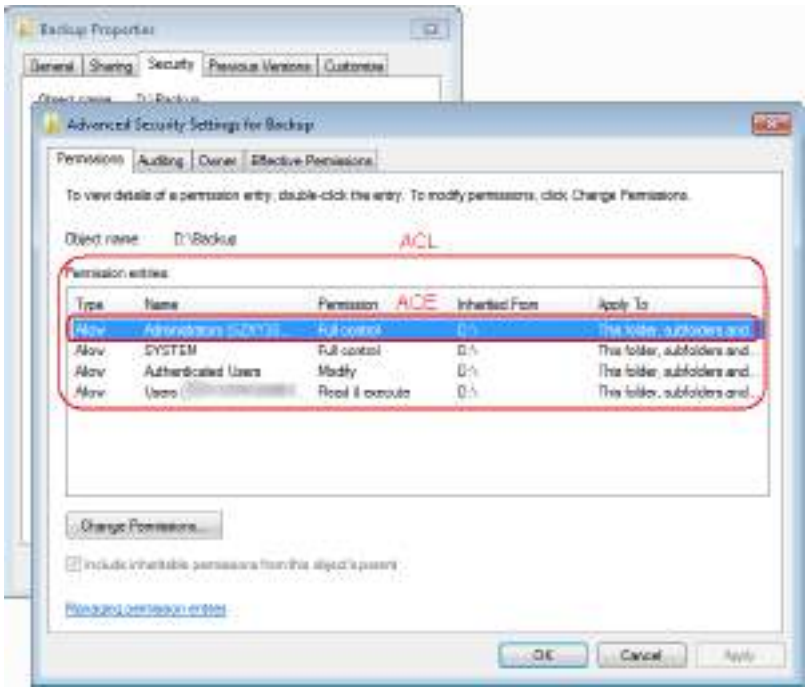
3.8.3.11 Using Windows ACLs

3.8.3.11.1 Overview

What Is a Windows ACL

A Windows access control list (ACL) is a set of access control entries (ACEs) specific to a file or directory in Windows. Each ACE is used to specify whether a specific user or user group can access a file or directory or not. In certain applications, users can access CIFS shares only after manually configuring the ACL.

Figure 3-7 Windows ACL



Windows Permission Control Principles

Table 3-55 describes access control rules.

Table 3-55 Windows access control rules

Rule	Description
Denial prior to allowance	If **User01** belongs both to user group 1 that has read and write permissions and user group 2 that has no read and write permissions, User01 has no read and write permissions.
Permission minimum	If a user's ACE is unavailable, the user permission is determined by **Others**.
Permission inheritance	A subfolder or subdirectory automatically inherits the permissions of its parent folder or directory.
Permission accumulation	If **User01** belongs both to user group 1 that has the write permission and user group 2 that has the read permission, **User01** has read and write permissions.

3.8.3.11.2 Configuring ACLs for Windows Users

You can configure ACLs for users to grant network access permissions on files and folders.

Prerequisites

You have logged in to a Windows client as an administrator and mounted a CIFS share.

Procedure

NOTE

In the following example, you log in to a Windows client as an administrator and configure ACL permissions for user **test_user1** on the **dir_test** subdirectory in the shared directory.

Step 1 Right-click **dir_test** and choose **Properties** from the short-cut menu.

Step 2 In the displayed **dir_test Properties** dialog box, click the **Security** tab.

Step 3 Click **Advanced**.

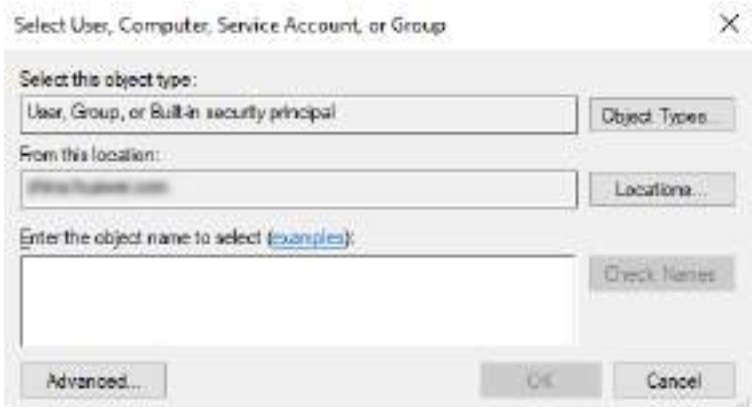
The **Advanced Security Settings for dir_test** dialog box is displayed.

Step 4 Click **Add**.

The **Permission Entry for dir_test** dialog box is displayed.

Step 5 Click **Select a principal**.

The **Select User, Computer, Service Account, or Group** search box is displayed.



Step 6 In the **From this location** and **Enter the object name to select** areas, enter the domain name and user name, and click **OK**.

The **Permission Entry for dir_test** dialog box is displayed.

NOTE

You can also click **Advanced**, query users, and select one in the displayed dialog box.

Step 7 Click **Show advanced permissions**.

Configure ACL permissions for user **test_user1**.

Step 8 Configure the planned ACL permissions as required.

1. Click **OK**.
   The **Advanced Security Settings for dir_test** dialog box is displayed.
2. Click **OK**.
   The **dir_test Properties** dialog box is displayed.
3. Click **OK**.

----End

3.8.3.11.3 Configuring ACLs Using the MMC

If you use the MMC to manage shares, you can configure ACL permissions for shares on the MMC.

NOTE

In the following example, you log in to a Windows client as domain user **mmc_user1** and configure ACLs for shares on the MMC.

Prerequisites

- You have logged in to a Windows client as a domain user and mounted a CIFS share.
- You have started the MMC and added the **Shared Folders** snap-in.

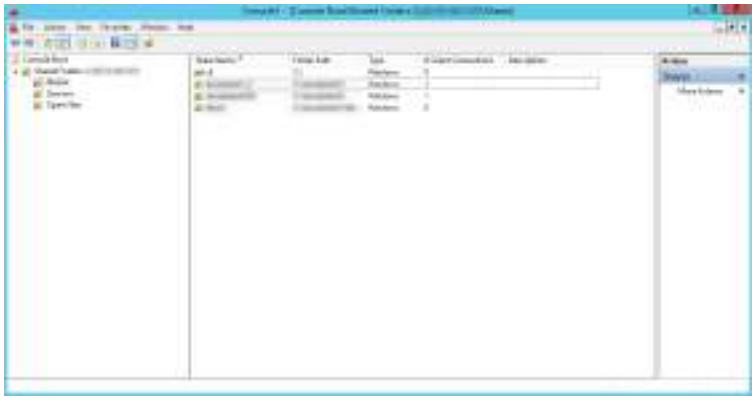
Context

For details about how to log in to the MMC and perform basic management operations, see **3.8.3.10 Connecting Microsoft Management Console to a Storage System**.

Procedure

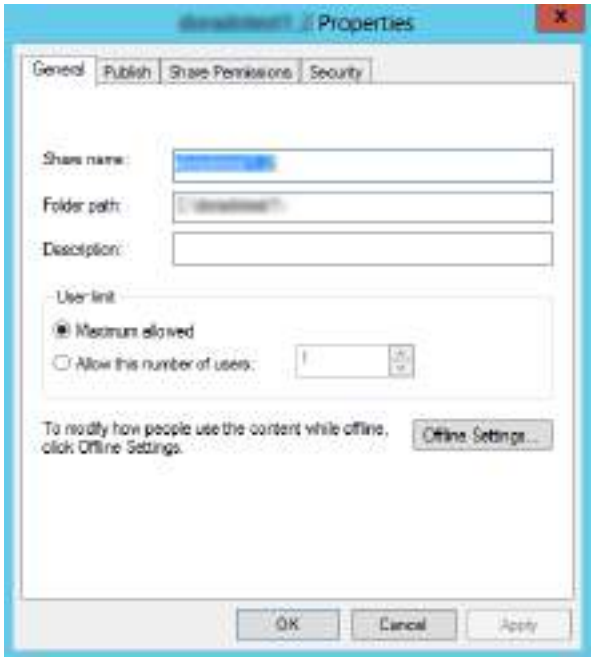
Step 1 Choose **Shared Folders** > **Shares**.

All the current CIFS shares are displayed in the right pane.



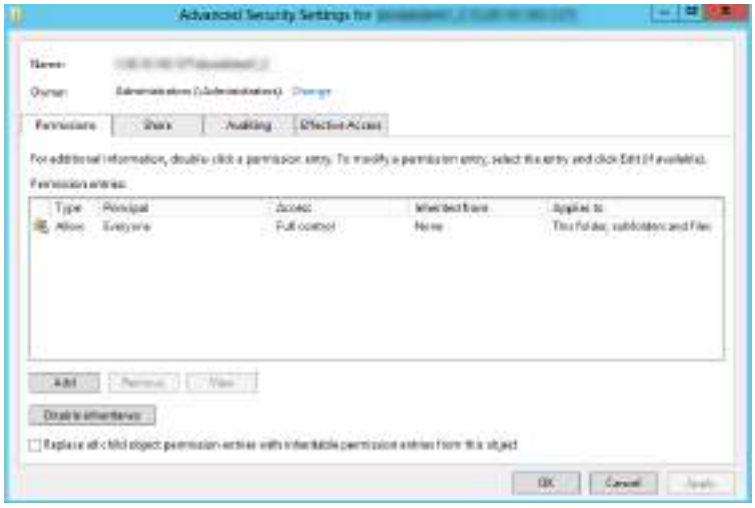
Step 2 Right-click the desired share and choose **Properties** from the shortcut menu.

The **xxx Properties** dialog box is displayed. **xxx** in this section indicates the selected share.



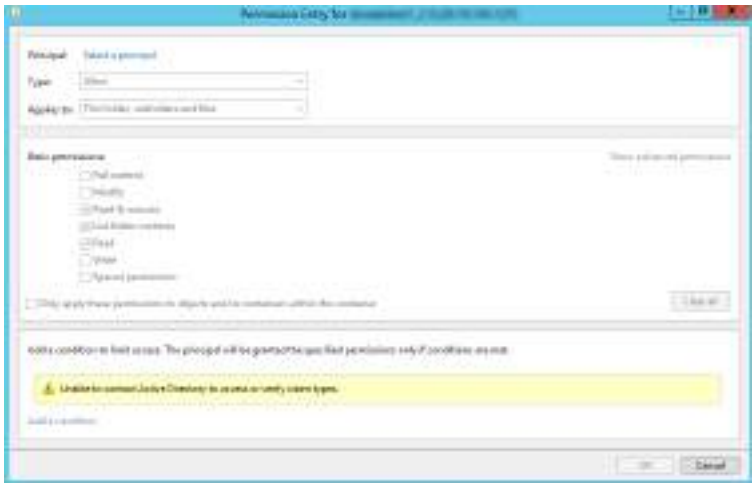
Step 3 Click the **Security** tab.

Step 4 Click **Advanced**.



Step 5 Click **Add**.

The **Permission Entry for xxx** dialog box is displayed.

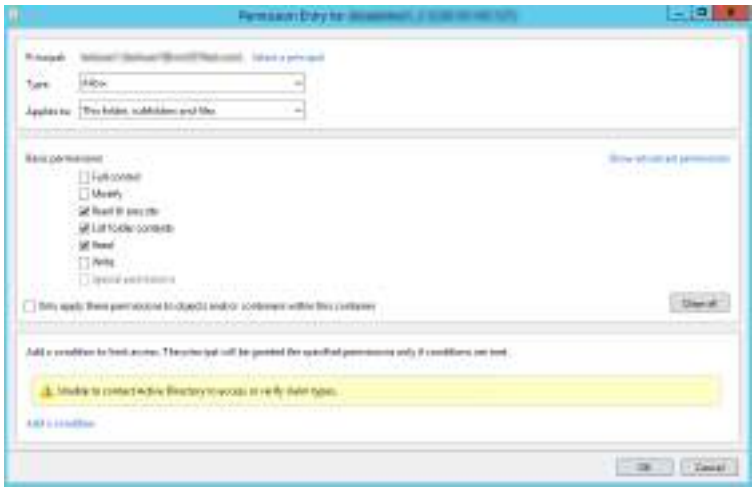


Step 6 Click **Select a principal**.

The **Select User, Computer, Service Account, or Group** search box is displayed.

Step 7 In the **From this location** and **Enter the object name to select** areas, enter the domain name and user name, and click **OK**.

The **Permission Entry for xxx** dialog box is displayed.

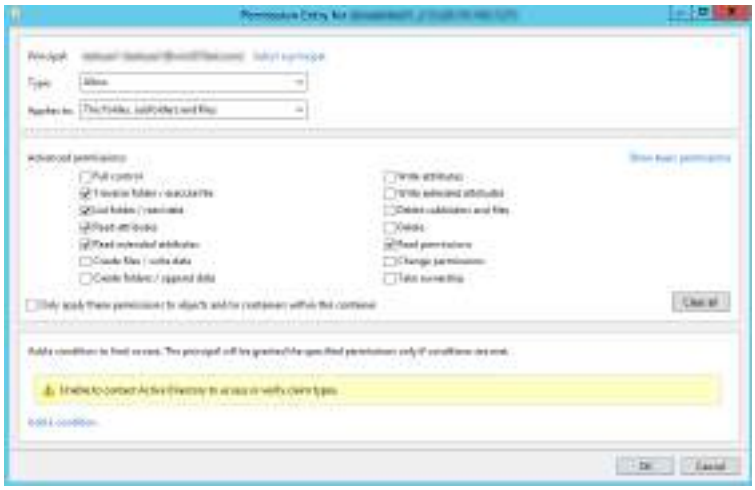


NOTE

You can also click **Advanced**, query users, and select one in the displayed dialog box.

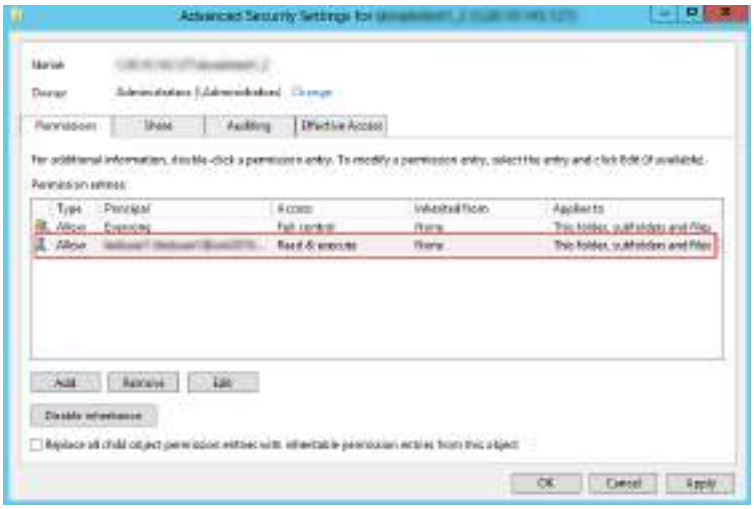
Step 8 Click **Show advanced permissions**.

Configure the ACL properties.



Step 9 Configure the planned ACL permissions as required.

1. Click **OK**.



2. Click **OK**.

3. Click **OK**.

----End

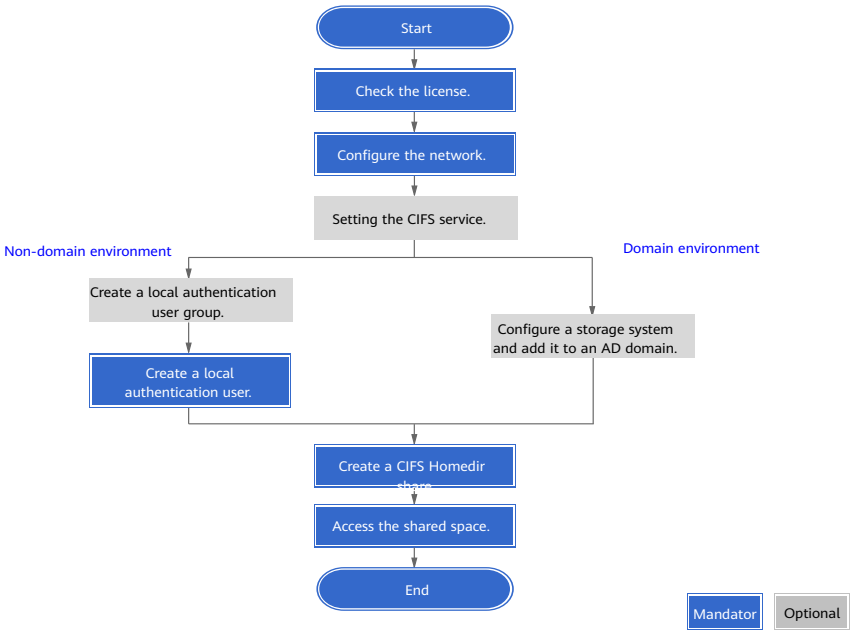
3.8.4 Configuring a CIFS Homedir Share

By configuring a CIFS Homedir share, users can access the shared directory to which they are assigned permissions.

3.8.4.1 Configuration Process

Figure 3-8 shows the flowchart for configuring a CIFS Homedir share.

Figure 3-8 Flowchart for configuring a CIFS Homedir share



3.8.4.2 Checking the License

Before configuring CIFS Homedir, ensure that the license grants the use of NAS Foundation.

Procedure

Step 1 Choose **Settings** > **License Management**.

Step 2 In the middle function pane, verify that **NAS Foundation** is displayed in the feature list.

NOTE

- If no license file has been imported, import a license file by referring to the initialization guide.
- If **NAS Foundation** is not displayed in the feature list, contact technical support engineers.

----End

3.8.4.3 Configuring the Network

Before configuring shared services, plan and configure the network properly for accessing and managing file services.

3.8.4.3.1 (Optional) Creating a Bond Port

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

Prerequisites

The IP addresses of the Ethernet ports you want to bond have been cleared. Ethernet ports that have IP addresses cannot be bonded.

Context

Port bonding provides more bandwidth and higher redundancy for links. Although ports are bonded, each session still transmits data through a single port and the total bandwidth can be increased only when there are multiple sessions. Determine whether to bond ports based on site requirements.

Port bonding on the storage system has the following restrictions:

- Only Ethernet ports that have the same rate and are on the same controller can be bonded. Ports cannot be bonded across controllers. Non-Ethernet ports cannot be bonded.
- Link aggregation (IEEE 802.3ad) is supported.
- For OceanStor 5310, OceanStor 5510 and OceanStor 5610:
  - GE interface modules (not supporting TOE) support port bonding across modules by default.
  - 10GE, 25GE, 40GE, and 100GE interface modules (supporting TOE) do not support port bonding across modules by default. They support port bonding across modules after TOE is disabled.

    NOTICE

    To disable the TOE function of a port, contact Huawei technical support.
  - The onboard network ports of OceanStor 5310 can be bonded across interface modules and the port rates must be the same.
- For OceanStor 6810, OceanStor 18510, and OceanStor 18810, interface modules in the same quadrant can be bonded across interface modules, and the TOE function of the ports to be bonded must be disabled.

  NOTICE

  To disable the TOE function of a port, contact Huawei technical support.

  For OceanStor 6810, OceanStor 18510, and OceanStor 18810, each interface module can use only one bonding mode. That is, an interface module does not allow bonding across modules and bonding within the module at the same time.
- Read-only users are not allowed to bond Ethernet ports.
- Each Ethernet port can be added to only one bond port.
- A member port of a port group cannot be added to a bond port.
- Management network ports cannot be bonded.
- Member ports in the same bond port cannot connect to different switch networks.

- After Ethernet ports are bonded, their MTU changes to the default value and you need to configure the switch port mode. Take Huawei switches as an example. You must set the ports on the Huawei switches to work in static LACP mode.

  NOTICE

  The link aggregation modes vary with switch manufacturers. If a switch from another vendor is used, contact technical support of the switch manufacturer for specific link aggregation configurations.

Port bonding on the host has the following restriction:

If the TOE function is enabled on the storage system and the host port connecting to the switch must be bonded, the bonding mode must be set to 4.

NOTE

If the preceding restriction cannot be met, disable the TOE function of the port.

Procedure

Step 1 Choose **Services** > **Network** > **Ethernet Network** > **Bond Ports**.

Step 2 Click **Create**.

The **Create Bond Port** page is displayed on the right.

Step 3 Set a bond name and select ports you want to bond.

1. Specify a name for the bond port in **Name**.

   NOTE

   The name must meet the following requirements:
   - The value can contain only letters, digits, underscores (_), hyphens (-), and periods (.).
   - The name contains 1 to 31 characters.
2. Select the controller where the bond port resides.
3. In **Available Ports**, select one or more ports you want to bond.

Step 4 Click **OK**.

Confirm your operation as prompted.

----End

3.8.4.3.2 (Optional) Creating a VLAN

This section describes how to create VLANs for Ethernet ports or bond ports.

Prerequisites

VLANs cannot be created on the Ethernet ports that are configured with IP addresses or used for networking.

Procedure

Step 1 Choose **Services** > **Network** > **Ethernet Network** > **VLANs**.

Step 2 Click **Create**.

The **Create VLAN** page is displayed on the right.

Step 3 In the **Port Type** drop-down list, select the type of the ports used to create VLANs.

Possible values are **Ethernet Port** and **Bond Port**.

Step 4 In the **Home Port** list, select a home port.

Step 5 In **ID**, specify the ID of a VLAN, and then click **Add**.

NOTE

- The VLAN ID ranges from 1 to 4094. You can specify multiple VLAN IDs one by one or in a batch. When creating multiple VLANs and specifying VLAN IDs in a batch, the VLAN IDs are in the following format: Start VLAN ID-End VLAN ID.
- To delete a VLAN ID, click × next to it.

Step 6 Click **OK**.

----End

Follow-up Procedure

When creating a logical port based on a VLAN, ensure that the port type is VLAN and the home port is the VLAN's home port.

3.8.4.3.3 (Optional) Creating a DNS Zone

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

Context

It is recommended that a DNS zone be associated with only logical ports with the same IP address type (IPv4 or IPv6).

If the host interface card supports both IPv4 and IPv6 protocols, the DNS client initiates IPv4 and IPv6 resolution requests. If the storage system is associated with both IPv4 and IPv6 logical ports in the same DNS zone and the host interface card is configured with only IPv4 addresses, the host may fail to access the domain name.

Procedure

Step 1 Choose **Services** > **vStore Service** > **vStores**.

Step 2 Click the name of the desired vStore. On the details page that is displayed on the right, click the **File Service** tab and click **Configure** in the **DNS Zone** area.

The **Configure DNS Zone** page is displayed on the right.

Step 3 Configure a DNS zone.

- Add a DNS zone.
  a. Click **Add**.
  b. In **Name**, enter the name of the DNS zone to be added.

  NOTE

  The name complexity requirements are as follows:

  - A name contains 1 to 255 characters and consists of multiple labels separated by periods (.).
  - A label contains 1 to 63 characters including letters, digits, hyphens (-), and underscores (_), and must start and end with a letter or a digit.
  - A name must be unique.

  c. If a HyperMetro vStore pair has been created for the vStore and **Working Mode** of the selected HyperMetro domain is **Active-active mode**, you need to set the owning site of the DNS zone. In normal cases, the host can access the logical port that belongs to the local site through the domain name of the local site. DNS zones with owning sites are mainly used when the active-active sites are far away from each other. In this case, hosts can access the nearest site to ensure access performance.
- Modify a DNS zone.
  In **Name**, modify the name of the desired DNS zone.

  NOTE

  The name complexity requirements are as follows:
  - A name contains 1 to 255 characters and consists of multiple labels separated by periods (.).
  - A label contains 1 to 63 characters including letters, digits, hyphens (-), and underscores (_), and must start and end with a letter or a digit.
  - A name must be unique.
- Remove a DNS zone.
  In the row that contains the desired DNS zone, click **Remove**.

Step 4 Click **Save**.

----End

3.8.4.3.4 Creating a Logical Port

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

Context

When configuring a CIFS Homedir share, set **Role** to **Service** for the logical port, and set **Data Protocol** to **CIFS** or **NFS + CIFS** for the logical port.

Precautions

- It is recommended that you create no more than 64 logical ports for each controller. If more than 64 logical ports are created for one controller, the

logical ports will fail over to a few available physical ports in the event that a large number of physical ports fail, decreasing service performance.

- In the case of file access across network segments, if a Remote Authentication Dial-In User Service (RADIUS) server is used for network device authentication in the data center and IP address failover occurs on a logical port, the IP address of the logical port will be re-registered on the RADIUS server. In this process, the IP address is not available. File services will be restored after the IP address becomes available.

Procedure

Step 1 Choose **Services** > **Network** > **Logical Ports**.

Step 2 Click **Create**.

The **Create Logical Port** page is displayed on the right.

Step 3 Set the parameters listed in **Table 3-56**.

Table 3-56 Logical port parameters

Parameter	Description
Name	Name of the logical port. The name must meet the following requirements: • The name must be unique. • The name can contain only letters, digits, underscores (_), hyphens (-), and periods (.). • The name contains 1 to 255 characters.
Role	Role of the logical port. Possible values are: **Management**: A port of this role is used by a vStore administrator to log in to the system for management. **Service**: A port of this role is used to access services, such as accessing CIFS shares of file systems. **Management + service**: A port of this role is used to access services or for a vStore administrator to log in to the storage system for system management. **Replication**: A port of this role is used for replication link connection in remote replication or HyperMetro, or for quorum link connection in HyperMetro.
Data Protocol	Data protocol of a logical port. Possible values are **NFS**, **CIFS**, **NFS + CIFS**, **iSCSI**, and **NVMe over RoCE**. **NOTE** • **NFS**, **CIFS**, and **NFS + CIFS** are applicable to file service configuration. **iSCSI** and **NVMe over RoCE** are applicable to block service configuration. • This parameter is displayed only when **Role** is set to **Service** or **Management + service**.

Parameter	Description
Owning vStore	vStore to which the logical port belongs. **NOTE** This parameter is displayed only when **Role** is set to **Service**, **Management**, or **Management + service**.
Owning Site	Site to which a logical port belongs. If a HyperMetro vStore pair has been created for the owning vStore, the configuration information of the front-end service logical port at the local site is automatically synchronized to the remote site, and the logical port at the owning site processes service access. The logical port is in connected state at the owning site and is in to-be-working state at the non-owning site. After the logical port creation is complete, its owning site cannot be modified. If a fault occurs for the port, the logical port at the non-owning site is used to process service access. **NOTE** This parameter is displayed only when a HyperMetro vStore pair has been created for the owning vStore and **Working Mode** of the HyperMetro domain of the HyperMetro vStore pair is **Active-active mode**.
IP Address Type	IP address type of the logical port, which can be **IPv4** or **IPv6**.
IP Address	IPv4 or IPv6 address of the logical port.
Subnet Mask	Subnet mask of the logical port's IPv4 address. **NOTE** This parameter is available only when **IP Address Type** is set to **IPv4**.
Prefix	Prefix length of the logical port's IPv6 address. **NOTE** This parameter is available only when **IP Address Type** is set to **IPv6**.
Gateway	Gateway of a logical port's IP address.
Port Type	Type of the port to which the logical port belongs. Possible values are **Ethernet port**, **Bond port**, **VLAN**, and **RoCE port**. **NOTE** • When **Data Protocol** is **NFS**, **CIFS**, **NFS + CIFS**, or **iSCSI**, you can select an Ethernet port, bond port, or VLAN. • When **Data Protocol** is **NVMe over RoCE**, you can select a VLAN or RoCE port. • Only 6.1.5 and later versions support RoCE ports.

Parameter	Description
Home Port	Ethernet port, bond port, VLAN, or RoCE port to which the logical port belongs. **NOTE** If **Port Type** is **RoCE port**, the system displays only the RoCE ports with a trust mode of DSCP.
Activation Status	Determine whether to activate the logical port. **NOTE** This parameter is available only when **Data Protocol** is set to **NFS**, **CIFS**, or **NFS + CIFS**.

Step 4 When **Role** is set to **Management**, **Service**, or **Management + service**, select **Advanced** in the upper right corner and set the advanced attributes of the logical port.

NOTE

If **Role** is set to **Service**, you can set advanced attributes only when **Data Protocol** is set to **NFS**, **CIFS**, or **NFS + CIFS**.

Table 3-57 describes the parameters.

Table 3-57 Advanced logical port parameters

Parameter	Description
Failover Group	Name of a failover group. **NOTE** • This parameter is available only when **Data Protocol** is set to **NFS**, **CIFS**, or **NFS + CIFS**. • If a failover group is specified, services on the failed home port will be taken over by an available port in the specified failover group. • If no failover group is specified, services on the failed home port will be taken over by an available port in the default failover group. • It is recommended that the logical ports of the same vStore use the same failover group. This ensures that the fault domains of the logical ports are the same.
IP Address Failover	After IP address failover is enabled, services on the failed home port will be taken over by other available ports in the failover group. In the entire process, the IP address used by services remains unchanged. **NOTE** • This parameter is available only when **Data Protocol** is set to **NFS**, **CIFS**, or **NFS + CIFS**. • Shares of file systems do not support the multipathing mode. They use IP address failover to improve the reliability of links.

Parameter	Description
Failback Mode	After the fault of the home port is rectified, services fail back to the home port. Possible values are **Automatic** and **Manual**. **NOTE** • This parameter is available only when **Data Protocol** is set to **NFS**, **CIFS**, or **NFS + CIFS**. • If **Failback Mode** is **Manual**, ensure that the link to the home port is normal before the failback. You can manually switch services back to the home port only when the link to the home port keeps normal for over five minutes. • If **Failback Mode** is **Automatic**, ensure that the link to the home port is normal before the failback. Services will automatically fail back to the home port only when the link to the home port keeps normal for over five minutes.
Listen for DNS Query	With this function enabled, external NEs can access the DNS service provided by the storage system by using the IP address of this logical port. **NOTE** This parameter is available only when **Data Protocol** is set to **NFS**, **CIFS**, or **NFS + CIFS**.
DNS Zone	Name of a DNS zone. **NOTE** • This parameter is available only when **Data Protocol** is set to **NFS**, **CIFS**, or **NFS + CIFS**. • If the value is blank, the logical port is not used for DNS-based load balancing. • One logical port can be associated with only one DNS zone. One DNS zone can be associated with multiple logical ports. • It is recommended that **Listen for DNS Query** be enabled for at least one logical port of each DNS zone. • It is recommended that a DNS zone be associated with only logical ports with the same IP address type (IPv4 or IPv6). If the host interface card supports both IPv4 and IPv6 protocols, the DNS client initiates IPv4 and IPv6 resolution requests. If the storage system is associated with both IPv4 and IPv6 logical ports in the same DNS zone and the host interface card is configured with only IPv4 addresses, the host may fail to access the domain name. • The load balancing effect varies with the distribution of logical ports associated with a DNS zone. To obtain a better load balancing effect, ensure that logical ports associated with a DNS zone are evenly distributed among controllers. • If a HyperMetro vStore pair has been created for the owning vStore, you can only select the DNS zones with the same owning site.

Step 5 Click **OK**.

----End

3.8.4.3.5 (Optional) Configuring DNS Load Balancing Parameters

The DNS load balancing feature can detect loads on various IP addresses on a storage system in real time and use a proper IP address as the DNS response to achieve load balancing among IP addresses.

Prerequisites

- If the storage system connects to an external DNS server, the external DNS server has been configured and is running properly.
- If the storage system directly connects to a host, DNS client configurations have been set on the host.
- Port 53 for the TCP/UDP protocol between the storage system and the DNS server or host is enabled.

Context

- DNS load balancing applies to scenarios where a large number of NAS service IP addresses or NAS clients are involved. If only a small number of (for example, less than 20) NAS service IP addresses or NAS clients are involved, you are advised to directly use service IP addresses to mount shares.
- Working principle:
  a. When a host accesses the NAS service of a storage system using a domain name, the host first sends a DNS request to the built-in DNS server and the DNS server obtains the IP address according to the domain name.
  b. If the domain name contains multiple IP addresses, the storage system selects the IP address with a light load as the DNS response based on the configured load balancing policy and returns the DNS response to the host.
  c. After receiving the DNS response, the host sends a service request to the target IP address.
- When DNS load balancing resolves a domain name, a specific domain name resolution record is added. The following records are supported:
  – A record: added if a domain name points to an IPv4 address (for example, 192.168.20.10).
  – AAAA record: added if a host name (or domain name) points to an IPv6 address (for example, ff03:0:0:0:0:0:0:c1).
  – PTR record: reverse of an A or AAAA record for implementing reverse DNS lookups.
- DNS load balancing supports only the UDP protocol for domain name resolution.

Procedure

Step 1 Choose **Settings** > **Basic Information** > **DNS Service**.

Step 2 Enable **File Service DNS Load Balancing**.

1. Set the DNS load balancing policy. The storage system supports the following load balancing policies:

NOTE

- **Weighted round robin** applies to scenarios where the load of storage devices is light or unknown, for example, in the scenario where shares are initially mounted to a large number of NAS clients.
- Other policies apply to scenarios where users want to balance loads based on a certain indicator (such as CPU usage, port bandwidth, number of connections, and overall loads) of running services, for example, in the scenario where shares are mounted to NAS clients in batches during capacity expansion of client applications.

- **Weighted round robin**: IP addresses which process loads and are under the same domain name are randomly selected for processing.
- **CPU usage**: The CPU usage of each node determines the weight. The storage system uses the weight to select a node to process client services.
- **Port bandwidth usage**: The total bandwidth usage of each node determines the weight. The storage system uses the weight to select a node to process client services.
- **Connections**: The NAS connections of each node determine the weight. The storage system uses the weight to select a node to process client services.
- **Overall loads**: The overall load of CPU usage, bandwidth usage, and number of NAS connections determines node selection. Less loaded nodes are more likely to be selected.

2. Click **Save**.

----End

Follow-up Procedure

After associating logical ports with a DNS zone, configuring logical ports to listen to DNS requests, setting a DNS load balancing policy, and enabling DNS load balancing, you need to configure DNS server addresses on clients. For details about how to configure and use DNS load balancing, see **5.1 How Can I Configure and Use DNS Load Balancing?**

3.8.4.3.6 (Optional) Managing the Routes of a Logical Port

When configuring share access, ensure that the logical port can ping the IP addresses of the domain controller, DNS server, and clients. If the ping test fails, add routes from the IP address of the logical port to the network segment of the domain controller, DNS server, or clients.

Prerequisites

A logical port has been configured with an IP address.

Procedure

Step 1 Choose **Services** > **Network** > **Logical Ports**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Select the desired logical port and click **Manage Route**.

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

NOTE

Alternatively, perform either of the following operations to go to the **Manage Route** page:

- Click **More** on the right of the desired logical port and select **Manage Route**.
- Click the name of the desired logical port. In the upper right corner of the page that is displayed, click **Manage Route** from the **Operation** drop-down list.

Step 4 Configure the route information for the logical port.

1. In the **IP Address** drop-down list, select the IP address of the logical port for which you want to add a route.
2. Click **Add**.
3. Set the parameters listed in **Table 3-58**.

Table 3-58 Route parameters

Parameter	Description
Type	Three types of routes are available: – **Default route** A route through which data is forwarded by default if no preferred route is available. The destination address and mask (IPv4) or prefix (IPv6) of the default route are automatically set to 0. To use this option, you only need to add a gateway. – **Host route** A route to a host. The destination mask (IPv4) or prefix (IPv6) of the host route are automatically set to 255.255.255.255 or 128. To use this option, you only need to add the destination address and gateway. – **Network segment route** A route to a network segment. You must add the destination address, destination mask (IPv4) or prefix (IPv6), and gateway.
Destination Address	IPv4 address, IPv6 address, or network segment of the destination service network port on the application server or destination logical port on another storage system.
Subnet Mask/ Prefix	Subnet mask of the IPv4 address or prefix of the IPv6 address for the destination service network port on the application server or destination logical port on another storage system.
Gateway	Gateway where the local logical port's IP address resides. **NOTE** The IP address of the gateway must be different from all internal heartbeat IP addresses. Otherwise, routing will fail.

4. Click ✓. The route information is added to the list.

NOTE

Click 🗑 on the right of a desired route to delete it.

Step 5 Click **Close**.

----End

3.8.4.4 (Optional) Configuring the CIFS Service

This section describes how to configure CIFS service parameters.

Context

The configured CIFS service parameters take effect for all CIFS shares of a vStore. If the configuration of a single CIFS share is inconsistent with that of the vStore, the vStore parameters prevail.

Procedure

Step 1 Choose **Settings** > **File Service** > **CIFS Service**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Click **Modify** in the upper right corner of the page.

Step 4 Set basic parameters for the CIFS service.

Table 3-59 describes the parameters.

Table 3-59 Basic parameters of the CIFS service

Parameter	Description
SMB3 Encryption	Specifies whether to enable SMB3 encryption. After this function is enabled, the system encrypts the shares to ensure data security, but the performance deteriorates. **NOTICE** Enabling this function affects SMB3 service performance. Check whether this function needs to be enabled. **NOTE** After SMB3 encryption is enabled, only SMB3 clients can access shares by default.
Unencrypted Client Access	After this function is enabled, clients that do not have encryption capabilities can access the shares. **NOTICE** After this function is enabled, clients of earlier versions (for example, Windows 7) are allowed to access shares where SMB3 encryption is enabled in plaintext. Check whether this function needs to be enabled. **NOTE** This function takes effect only after the SMB3 encryption function is enabled.
Symbolic Link	After this function is enabled, CIFS clients can access symbolic links created on UNIX clients (for example, symbolic links created through NFS clients). However, performance may deteriorate after this function is enabled.

Parameter	Description
Notify	After this function is enabled, a client's operations on a directory, such as adding a directory, adding a file, modifying the directory, and modifying a file, can be detected by other clients that are accessing this directory or the parent directory of this directory. The created or modified directories and files are visible after the page automatically refreshes. **NOTE** Only 6.1.5 and later versions support this parameter.
Oplock	Oplock: a mechanism. It is used to dynamically adjust cache policies of clients to improve 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. **NOTE** Only 6.1.5 and later versions support this parameter.
Signature Enforcement	After this function is enabled, servers forcibly use the signature function no matter whether clients enable the signature function, enhancing CIFS share access security. **NOTE** Only 6.1.5 and later versions support this parameter.
ABSE	After access based share enumeration (ABSE) has been enabled, when users view the CIFS share information, the system displays only the CIFS shares that the users have permissions to access. **NOTE** ● It takes 10 to 20 minutes to load the CIFS share permission information after the storage system is powered on. During this period, the function does not take effect. ● You are advised to enable this function. If this function is disabled, users can find all shares (including the shares for which the users do not have access permission), which may cause security threats to other shares. ● Only 6.1.5 and later versions support this parameter.

Parameter	Description
Guest	After this function is enabled, users can access shared directories without entering usernames or passwords and have the permission of the Everyone user group that has been added when the CIFS shares were created. **NOTE** • After this function is enabled, unauthorized users can access shared directories as guest users, which may cause information security risks. You are advised to disable this function. • Only 6.1.5 and later versions support this parameter.

Step 5 Click **Save**.

----End

3.8.4.5 Configuring a Local Authentication User (Group)

In a non-domain environment, you must configure a local authentication user (group). The storage system enables you to allocate different share access permissions to different users (groups).

3.8.4.5.1 (Optional) Creating a Local Authentication User Group

This section describes how to create a local authentication user group. Local authentication user groups are used to control the share access permissions of specific local authentication users.

Context

A system has nine local authentication user groups that are automatically created. The nine user groups are reserved for the system and cannot be modified or deleted:

- **Administrators** is the administrator group. When the group members access a shared namespace in the storage system, they do not need to be authenticated by share-level ACLs and NT ACLs. They can operate any file in any share with administrator permissions without the need to be authenticated.
- Other user groups are common user groups. When the group members access a shared file system of the storage system, they can have the corresponding permissions only after being authenticated.

NOTE

An access control list (ACL) is a collection of permissions that are authorized to users or user groups to operate shared files. ACL permissions are classified into ACL storage permissions and ACL authentication permissions. After a user logs in to a share, the system determines the user's permissions on the share, reads the ACL permissions, and then determines whether the user can read and write files. For ACL storage permissions, each ACL permission is called an Access Control Entry (ACE). After a share is mounted to a Windows client, the client sends NT ACLs to the server (storage system that provides the share).

Procedure

Step 1 Choose **Services** > **File Service** > **Authentication Users** > **Windows Users** > **Local Authentication User Groups**.

Step 2 Select the vStore for which you want to create a local authentication user group from the **vStore** drop-down list in the upper left corner.

Step 3 Click **Create**.

The **Create Local Windows Authentication User Group** page is displayed on the right.

Step 4 Set basic parameters for the local authentication user group.

Table 3-60 describes the parameters.

Table 3-60 Basic local authentication user group parameters

Parameter	Description
Name	Name of the local authentication user group. [Value range] • The name must be unique. • The name cannot contain "/[]:|<>+=;?*@, or control characters, and cannot end with a period (.). If the name starts or ends with a space, the space is not displayed after the name is created. • The name can contain case-insensitive letters. For example, **aa** and **AA** cannot be created at the same time. • The user group name cannot be the same as the name of a local authentication user. • The name contains 1 to 256 characters.
Description	Description of the local authentication user group. [Value range] The description can be left blank or contain up to 255 characters.

Step 5 Select privileges for the local authentication user group. You can view details about the privileges in the description.

Step 6 Click **OK**.

----End

3.8.4.5.2 Creating a Local Authentication User

This section describes how to create a local authentication user. For applications that use local authentication, local authentication users are used to access shares. You can add a local authentication user to a user group for authentication and access a share as the user group.

Procedure

Step 1 Choose **Services** > **File Service** > **Authentication Users** > **Windows Users** > **Local Authentication Users**.

Step 2 Select the vStore for which you want to create a local authentication user from the **vStore** drop-down list in the upper left corner.

Step 3 Click **Create**.

The **Create Local Windows Authentication User** page is displayed on the right.

Step 4 Set basic parameters for the local authentication user.

Table 3-61 describes the parameters.

Table 3-61 Basic local authentication user parameters

Parameter	Description
Name	Name of the local authentication user. [Value range] • The name must be unique. • The name cannot contain "/\][:;|=,+*?<>@, spaces, or control characters, and cannot end with a period (.). • The name can contain case-insensitive letters. For example, **aaaaaaaa** and **AAAAAAAA** cannot be created at the same time. • The name cannot be the same as the name of a local authentication user group. • The name contains 3 to 20 characters. **NOTE** You can modify the minimum length of the user name on the **Set Security Policy** page.

Parameter	Description
Password	Password of the local authentication user. [Value range] ● The password contains 8 to 32 characters. ● The password must contain at least one of the following types: special characters, uppercase letters, lowercase letters, and digits. Special characters include !"#$%&'()*+,-./:;<=>?@[\]^`{_|}~ and spaces. ● The password cannot contain three consecutive identical characters. ● The password cannot be the same as the user name or the user name spelled backward. **NOTE** You can set security policies for the password of a local authentication user on the **Set Security Policy** page. If **Validity Period** is **0**, the password will never expire. For the security purpose, you are advised to set a specific password validity period. After the password expires, you cannot access shares, but you can set a password again or modify the password security policy on the **Set Security Policy** page.
Confirm Password	Confirms the password for consistency.
Status	Indicates whether to enable the user.
Description	Description of the local authentication user. [Value range] The description can be left blank or contain up to 256 characters.
Owning Groups	Groups to which the local authentication user belongs. Click ▸ on the right of **Owning Groups**. In the **Available Groups** list, select the desired groups and add them to **Selected Groups**.

NOTE

You cannot configure privileges for local authentication users separately on DeviceManager. Instead, you can configure privileges for local authentication users on the CLI.

Step 5 Click **OK**.

----End

3.8.4.6 Adding a Storage System to an AD Domain

After a storage system is added to an AD domain, domain users can access CIFS shares that are allocated to the domain. This section describes how to add a storage system to an AD domain.

3.8.4.6.1 Preparing AD Domain Configuration Data

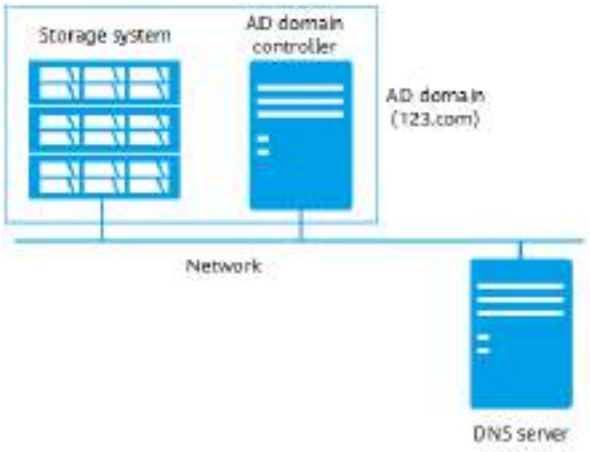
Why AD Domains?

In Windows shared mode, every device that provides shares is an independent node. The account and permission information about users allowed to access shares are stored on each node. As a result, the information maintenance is complex and uncontrollable.

If an AD domain is used, however, the domain controller manages all the user configuration information and authenticates the access to the domain. The domain controller incorporates a database that stores information about the domain account, password, and nodes in the domain. A user can access all the shared content in the domain after passing the authentication by the domain controller.

Working Principles

Figure 3-9 Network diagram of AD domain server authentication



1. The DNS server provides a full domain name (123.com for example) for the AD domain.
2. The storage system is added into the AD domain and provides share services.
3. Users can access shares after logging in to hosts in the AD domain using domain accounts.

Data Preparation

To smoothly add a storage system to an AD domain, prepare or plan the required data based on the site requirements. Collect **Domain Administrator**, **Password**, **Full Domain Name**, **Organization Unit** (optional), and **System Name**. For details about how to obtain the data, see **3.8.4.6.3 Configuring AD Domain Authentication Parameters**.

3.8.4.6.2 Connecting a Storage System to a DNS Server

After a storage system is connected to a DNS server, you can access the storage system through an IP address or a domain name. This operation enables you to configure the IP address of the DNS service for the file storage service.

Prerequisites

- A DNS server has been configured and is running properly.
- Port 53 for the TCP/UDP protocol between the storage system and the DNS server is enabled.

Context

- A DNS server is used to resolve names of hosts in a domain.
- If you want to configure a standby DNS server, keep the domain names of the active and standby servers consistent.

Procedure

Step 1 Choose **Services** > **vStore Service** > **vStores**.

Step 2 Click the name of the desired vStore. On the details page that is displayed on the right, click the **File Service** tab and click **Configure** in the **DNS Service** area.

The **DNS Service** page is displayed on the right.

Step 3 Configure an IP address for the DNS service.

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

   NOTE

   Set **Standby DNS IP Address 1** first and then **Standby DNS IP Address 2**.
4. (Optional) Test the connection between the DNS server and the storage system.
   - You can click **Test** next to a DNS IP address to test its availability.
   - You can click **Test All** to test the connection between the DNS server and the storage system.

Step 4 Click **OK**. Confirm your operation as prompted.

----End

3.8.4.6.3 Configuring AD Domain Authentication Parameters

If an AD domain server is deployed on a customer's network, a storage device must join the AD domain. Then, CIFS clients need to be authenticated by the AD domain server when they attempt to access shared resources on the storage device. The administrator can manage the share access permissions and quotas of domain users. If the storage device does not join an AD domain, domain users cannot use share services provided by the storage device.

Prerequisites

- An AD domain has been set up.
- The storage system has been connected to the DNS server.
- The AD domain server and DNS server have time synchronization with the storage system. The time difference must be no larger than 5 minutes.

- Ports 88 (TCP/UDP protocol), 389 (TCP/UDP protocol), 445 (TCP protocol), and 464 (TCP/UDP protocol) are enabled between the storage system and the AD domain.

NOTE

The storage systems can connect to AD domain servers and DNS servers through management network ports or service network ports (logical ports). If a storage system connects to an AD domain server and DNS server through management network ports, ensure that the management network ports on at least two controllers can properly communicate with the AD domain server and DNS server. If a storage system connects to the AD domain server and DNS server through service network ports, it is recommended that the service network ports on at least two controllers can properly communicate with the AD domain server and DNS server. It is recommended that storage systems connect to AD domain servers through service network ports.

Precautions

- Before adding a storage system to an AD domain, ensure that the primary controller of the storage system is connected to the DNS server and AD domain server.
- When **Overwrite System Name** is enabled, if a system name entered exists in the AD domain controller, the information about the current storage system will overwrite the information about the storage system corresponding to the system name on the AD domain controller.
- A simple password may result in security issues. A complex password that contains uppercase letters, lowercase letters, digits, and special characters is recommended.
- You are advised to use physical isolation and end-to-end encryption to ensure security of data transfer between the AD domain server and clients.

Procedure

Step 1 Choose **Settings** > **User and Security** > **Domain Authentication** > **File Service AD Domain**.

Step 2 Select a desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 View AD domain parameters of the file service. **Table 3-62** describes the parameters.

NOTE

- On the file service AD domain management page, click  to refresh file service AD domain information.
- On the file service AD domain management page, click  and select the file service AD domain information you want to view.

Table 3-62 AD domain parameters of the file service

Parameter	Description
Full Domain Name	Indicates the full domain name of the AD domain server.

Parameter	Description
Organization Unit	Indicates the organization unit of a type of directory objects in the domain. These objects include users, computers, and printers.
System Name	Indicates the name of the storage system in the AD domain.
Domain Status	Indicates whether the storage system is added to the domain.

Step 4 Configure the file service AD domain.

1. Select the AD domain to be configured and click **Configure**.

   The **Configure File Service AD Domain** page is displayed on the right.

   NOTE

   Alternatively, choose **Services** > **vStore Service** > **vStores** and click the name of a vStore. On the details page that is displayed on the right, select the **File Service** tab and click **Configure** in the **AD Domain** area.

2. Configure basic information. **Table 3-63** describes the parameters.

Table 3-63 Basic information about the file service AD domain

Parameter	Description
Domain Administrator	Indicates the user name of the AD domain server administrator. The following formats are supported: 1. User name, for example, **test_user1**. 2. NetBIOS name + user name. You can run the **nbtstat -n** command to query the NetBIOS name. For example, **china\test_user1**. **NOTE** This function is supported only in 6.1.5 and later versions. 3. User name + AD domain name, for example, **test_user1@china.com**. **NOTE** This function is supported only in 6.1.5 and later versions. [Value range] A string of 1 to 63 characters. [Example] test_user1
Password	Indicates the password of the AD domain server administrator. [Value range] A string of 1 to 127 characters.

Parameter	Description
Full Domain Name	Indicates the full domain name of the AD domain server. **NOTE** You can click **Test** to test the validity of the full domain name. [Value range] A string of 1 to 127 characters. [Example] abc.com
Organization Unit	Indicates the organization unit of a type of directory objects in the domain. These objects include users, computers, and printers. After an object joins the domain, it will be a member in the organization unit. If this parameter is left empty, objects join the **Computers** organization unit by default. [How to obtain] 1. On the Windows AD domain server, open **Active Directory Users and Computers** or **ADSI Edit**. 2. Select the directory on the left, right-click the directory, and choose **Properties**. 3. In the **Properties** dialog box that is displayed, click **Attribute Editor**. The value of **distinguishedName** is the organization unit. [Example] cn=xxx,dc=abc,dc=com
System Name	Indicates the name of the storage system in the AD domain. After the storage system is added to the domain, the client can use the name to access the storage system. **NOTE** – If the system name used for joining the domain exists in the domain controller and the **Overwrite System Name** function is disabled in the storage system, joining the AD domain will fail. – Special characters ~!$%^&{}`' are not recommended because the domain name of the DNS server does not support these characters. – English characters and digits are recommended. [Value range] A string of 1 to 15 characters. [Example] test2021

Parameter	Description
Overwrite System Name	If a storage system with the same name exists in the domain controller, enabling this function will overwrite the original storage system information. **NOTICE** After this function is enabled, information about the storage system with the same system name in the domain controller will be overwritten. As a result, the authentication between the storage system and domain controller corresponding to the system name will be affected.
Domain Status	Indicates whether the storage system is added to the domain.

3. Click **Join Domain**.
4. If you want to remove a storage system from an AD domain, perform the following operations:
   a. Set **Domain Administrator** and **Password**.
   b. Click **Exit Domain**.
      Confirm your operation as prompted.
5. Click **Close**.

----End

Follow-up Procedure

- After adding a storage system to an AD domain that has multiple domain controllers, you are advised to wait about 2 minutes for these domain controllers to synchronize configurations and then access shares as a domain user.
- After the storage system is removed from the AD domain, you are advised to wait for about 2 minutes before adding the storage system to the AD domain.

3.8.4.7 Creating a CIFS Homedir Share

Homedir shares are a type of CIFS shares. 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.

Procedure

Step 1 Choose **Services** > **File Service** > **Shares** > **CIFS Shares**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Click **Create Homedir**.

The **Create CIFS Homedir Share** page is displayed on the right.

NOTE

The screenshot is for reference only and the actual displayed information may vary.

Step 4 Set basic parameters for the CIFS Homedir share.

Table 3-64 describes the parameters.

Table 3-64 Basic CIFS Homedir share parameters

Parameter	Description
Share Name	Name used by a user for accessing the shared resources. [Value range] • The name must be unique. • The name cannot contain characters " / \ [ ] : | < > + ; , ? * =, and cannot be **ipc$**, **~**, or **print$** reserved by the system. • The name contains 1 to 80 characters. [Example] share_for_user1

Parameter	Description
Relative Path	Relative path of the user directory. When a user accesses a Homedir share, the actual directory that the user accesses consists of the share path (consisting of the file system and dtree) configured in the mapping rule and the relative path configured here. If the relative path does not exist in the share path and the **Auto Create Path** function is enabled in the mapping rule, the system automatically creates the relative path. Otherwise, manually create the relative path in the share path to ensure that the directory exists when the share is accessed. [Value range] • The relative path cannot contain the following characters: \:*?"<>|. Consecutive slashes (/) are not allowed. • The relative path can contain common characters and special character strings such as %d and %w. %d indicates the domain name, and %w indicates the user name. If the relative path contains special character string **%d/%w**, the domain name and user name of the user are automatically matched. In this way, each user has independent space, and the file system is shared to users as a private directory. For example, if the relative path is **home_%d/%w**, the relative Homedir directory of user **usera** in domain **china** is **home_china/usera/**. Assume that the name of the Homedir share created by the user is **Homedirtest**, and the user name is **usera** and the share path is **fstest/dtreetest** in the mapping rule. When user **usera** accesses the Homedir share, the actual path that user **usera** accesses is **fstest/dtreetest/home_china/usera**. • The relative path contains 1 to 255 characters. [Example] home_%d/%w

Step 5 Set advanced properties of the CIFS share. Select **Advanced** in the upper right corner.

Table 3-65 describes the parameters.

Table 3-65 Advanced parameters of a CIFS share

Parameter	Description
Description	Indicates the description of a CIFS share. **NOTE** The description can be left blank or contain up to 255 characters.

Parameter	Description
Notify	Determine whether to enable **Notify**. After this function is enabled, a client's operations on a directory, such as adding a sub-directory, adding a file, modifying the directory, and modifying a file, can be detected by other clients that are accessing this directory or the parent directory of this directory. The created or modified directories and files are visible after the page automatically refreshes.
Continuously Available	Determine whether to enable **Continuously Available**. This option provides the SMB continuous availability feature. This feature depends on Oplock which is enabled by default. If Oplock is disabled, choose **Settings** > **File Service** > **CIFS Service** to enable it.
SMB3 Encryption	Specifies whether to enable SMB3 encryption. After this function is enabled, the system encrypts the share to ensure data security, but the performance deteriorates. **NOTICE** Enabling this function affects SMB3 service performance. Check whether this function needs to be enabled. **NOTE** • After SMB3 encryption is enabled, only SMB3 clients can access shares by default. • Only 6.1.3 and later versions support this parameter.
Unencrypted Client Access	After this function is enabled, clients that do not have encryption capabilities can access the share. **NOTICE** After this function is enabled, clients of earlier versions (for example, Windows 7) are allowed to access shares where SMB3 encryption is enabled in plaintext. Check whether this function needs to be enabled. **NOTE** • This function takes effect only after the SMB3 encryption function is enabled. • Only 6.1.3 and later versions support this parameter.
ABE	After ABE is enabled, files and folders that users have no access permission are not displayed. **NOTE** • SMB2 and SMB3 support this function but SMB1 does not. • Only 6.1.3 and later versions support this parameter.
Show Snapshot	This function allows clients to show and traverse snapshot directories. **NOTE** Only 6.1.3 and later versions support this parameter.

Step 6 Set the permission of the user or user group for accessing the CIFS Homedir share.

1. In the **Permissions** area, click **Add**.

The **Add User or User Group** page is displayed.

2. Select the type of the users or user groups.

   The value can be **Everyone**, **Local Windows authentication user**, **Local Windows authentication user group**, **AD domain user**, or **AD domain user group**.

   - If you select **Local Windows authentication user** or **Local Windows authentication user group**, select the users or user groups to be added from the list.

     NOTE

     You can click **Create** to create a local Windows authentication user or local Windows authentication user group.

   - If you select **AD domain user** or **AD domain user group**, enter the names of the users or user groups in **Name**.

     NOTE

     - A domain user name is in the format of *Domain name*|*Domain user name* and a domain user group name is in the format of *Domain name*|*Domain user group name*.
     - **Name** contains 1 to 256 characters. An AD domain user name cannot start with an at sign (@).
     - You can also enter multiple names separated by pressing **Enter**.

3. In **Permission**, select the permission granted for the users or user groups.

   Table 3-66 describes the permissions.

Table 3-66 Description of CIFS Homedir share permissions

Permission	Forbidden	Read-Only	Read-Write	Full Control
Viewing files and subdirectories	X[a]	√[b]	√	√
Viewing file contents	X	√	√	√
Running executable files	X	√	√	√
Adding files or subdirectories	X	-[c]	√	√
Modifying file contents	X	-	√	√

Permission	Forbidden	Read-Only	Read-Write	Full Control
Deleting files and subdirectories	X	-	√	√
Renaming	X	-	√	√
Changing ACL permissions of files or directories	X	-	-	√
a: Users do not have the permission. b: Users have the permission. c: The specified permission is not involved.				

NOTE

- The permission priority from high to low is **Forbidden** > **Full control** > **Read-write** > **Read-only**. The highest permission prevails. If a user is granted with a higher permission than its original one, 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 changed to **Full control** and it can access a share immediately without re-authentication.
- You can run the **change service cifs administrators_privilege=?** command on the CLI to modify permissions of members in the **Administrators** user group. For details about the command, see *Command Reference* of the desired version. In the command, the value of the **administrators_privilege** parameter can be **admin** (default), **default_group**, or **owner**.

  For local authentication users whose primary user group is **Administrators**, users with different **administrators_privilege** values have different permissions.

  - **admin**: When members in the **Administrators** user group access a shared file system in the storage system, they do not need to be authenticated by share-level ACLs and NT ACLs. They can operate any file in any share with administrator permissions without the need to be authenticated.
  - **default_group**: Members in the **Administrators** user group have the same permissions as members in the **default_group** user group.
  - **owner**: Members in the **Administrators** user group have the permissions to query and set file or directory ACLs and modify file or directory owners. When the group members access shared file systems, they need to be authenticated by directory- or file-level NT ACLs, but do not need to be authenticated by share-level ACLs.

  Modified permissions take effect only after users are re-authenticated on clients.

  You can run the **show service cifs** command on the CLI and check permissions of the **Administrators** user group in the **Administrators Privilege** field.

4. Click **OK**.

   The system adds the selected users or user groups to the **Permissions** list.

5. Click **Next**.

Step 7 Click **OK**.

----End

3.8.4.8 Adding a Mapping Rule for a CIFS Homedir Share

This section describes how to add a mapping rule for a CIFS Homedir share. Only users matching the mapping rule can access the Homedir shared directory in the file system.

Procedure

Step 1 Choose **Services** > **File Service** > **Shares** > **CIFS Shares**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Click **More** on the right of the desired CIFS Homedir share and select **Add Mapping Rule**.

The **Add Mapping Rule** page is displayed on the right.

NOTE

Alternatively, perform either of the following operations to add a mapping rule:

- Click the name of the desired CIFS Homedir share. On the page that is displayed, click the **Mapping Rules** tab and click **Add**.
- Click the name of the desired CIFS Homedir share. In the upper right corner of the page that is displayed, select **Add Mapping Rule** from the **Operation** drop-down list.

Step 4 In **Username**, specify the user name of the CIFS Homedir mapping rule.

NOTE

- The user name contains 1 to 255 characters.
- The user name can be a common or domain user name. A domain user name uses a backslash (\) to connect the domain name and user name. Only one backslash (\) is allowed, for example, **china\user001**. The domain name can only be a NetBIOS name. You can query the NetBIOS name of a domain by running the **nbtstat -n** command. Alternatively, you can right-click the domain on the **Active Directory Users and Computers** page, choose **Properties** from the shortcut menu, and find the value of **Domain name (pre-Windows 2000)** in the dialog box that is displayed. The value is the NetBIOS name of the domain.
- The user name can contain only one wildcard (*) and the wildcard must be at the end of the user name. For example, **china*** indicates all users in the **china** domain.
- The user name cannot contain "/[]<>+:;,?=| or spaces, cannot start with a backflash (\) and end with a period (.) or backflash (\), and wildcard (*) can only be at the end of the user name. Only one backflash (\) and wildcard (*) is allowed.

Step 5 From the **File System** drop-down list, select the file system for which a mapping rule is to be created.

NOTE

- You can click **Create** to create a file system.
- If **Security Style** of the file system is set to **UNIX**, ensure that the user has the permission to access the relative path of the Homedir share when creating a mapping rule. Otherwise, the user cannot access the Homedir share.

Step 6 From the **Dtree** drop-down list, select the dtree for which a mapping rule is to be created.

Step 7 In **Priority**, set the priority of the mapping rule.

NOTE

- The value of **Priority** ranges from 1 to 1024.
- Mapping rules are sorted in descending order of priorities. A smaller value indicates a higher priority. Rules with the same priority are sorted based on the creation sequence. Users match mapping rules in sequence.

Step 8 Determine whether to enable **Auto Create Path**. After this function is enabled, if a relative path does not exist under the CIFS Homedir share, the system creates the relative path automatically.

NOTE

- When **Auto Create Path** is disabled, if the user path does not exist, the current mapping rule fails to be matched, and the system continues to match the next mapping rule.
- If **Security Style** of the file system is set to **UNIX**, the default UNIX permission of the file system's root directory is **755**. You need to run the **change file_system general file_system_id=? unix_permissions=777** command to modify the UNIX permission so that the **Auto Create Path** function can take effect. Otherwise, users matching this rule cannot access the Homedir share.

Step 9 Click **OK**.

Confirm your operation as prompted.

----End

3.8.4.9 Accessing a CIFS Homedir Share

This section describes how to access CIFS Homedir shares.

Context

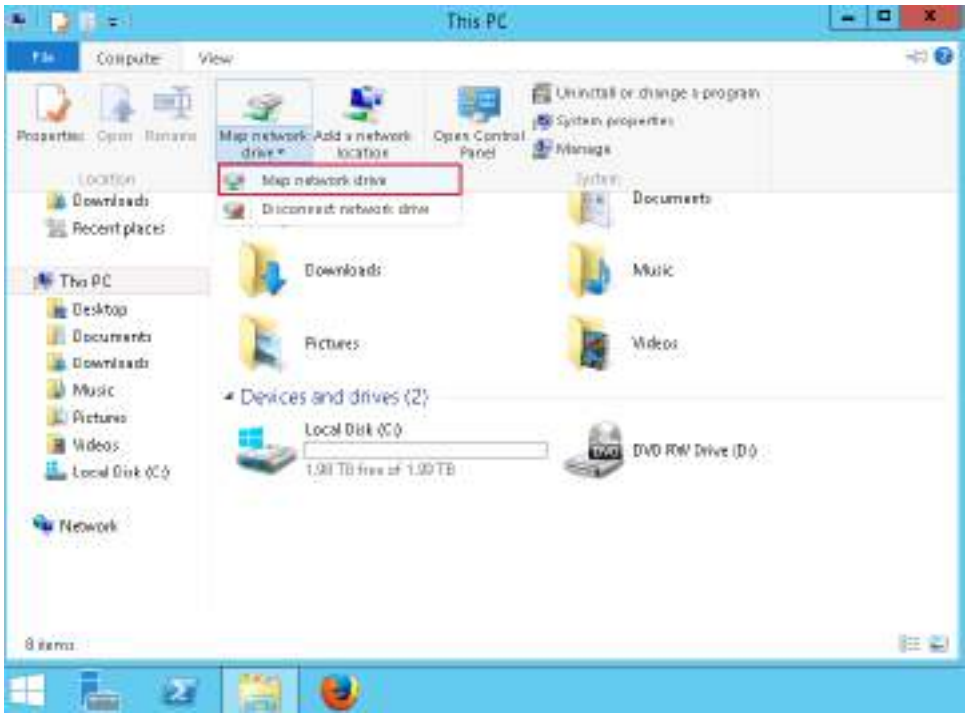
When a user accesses a Homedir share, the actual directory that the user accesses consists of the share path (consisting of the file system and dtree) configured in the mapping rule and the relative path set when the CIFS Homedir share is created. If the configured relative path does not exist in the shared path and the **Auto Create Path** function is enabled in the mapping rule, the system automatically creates the relative path. Otherwise, manually create the relative path in the share path to ensure that the directory exists when the share is accessed.

For example, if the relative path of the CIFS Homedir share is **home_ %d/ %w**, the Homedir relative directory of **usera** in the **china** domain is **home_china/usera/**. Assume that the name of the Homedir share created by the user is **Homedirtest**, the user name is **usera** and the share path is **fstest/dtreetest** in the mapping rule. When user **usera** accesses the Homedir share, the actual path that user usera accesses is **fstest/dtreetest/home_china/usera**. In this way, each user has its own space so that the file system can be shared with users in the form of private directories.

Procedure

Step 1 Choose **Map network drive** on a Windows client.

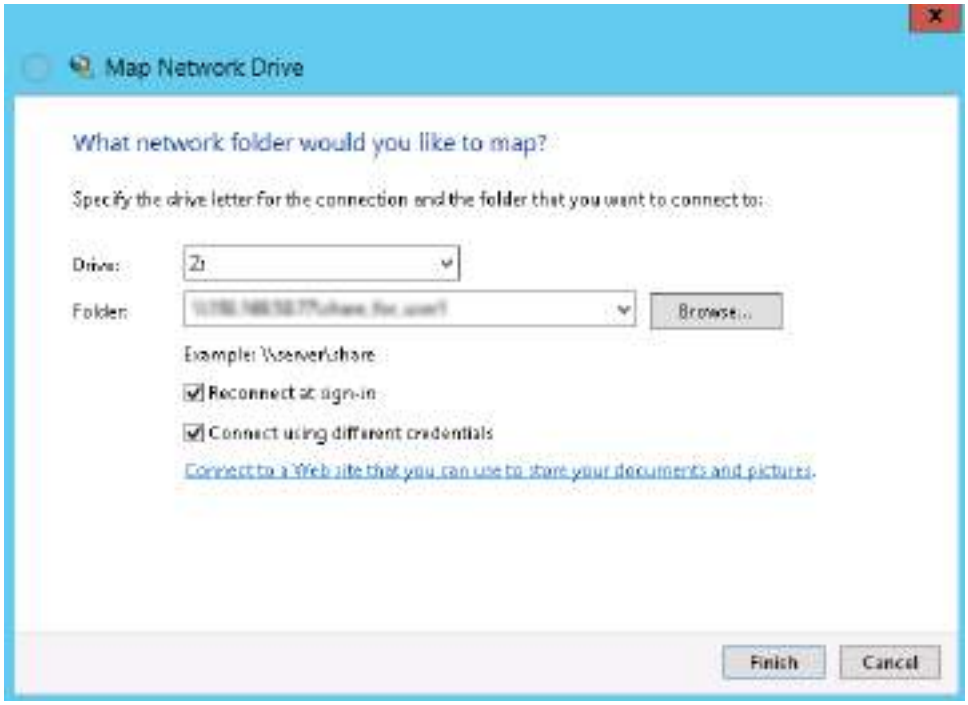
Take Windows Server 2012 as an example. Open **File Explorer** and choose **Computer** > **Map network drive** > **Map network drive**.



NOTE

GUIs may be slightly different for clients running different versions of Windows operating systems. The actual GUIs prevail.

Step 2 In the displayed **Map Network Drive** dialog box, configure the network folder you want to map.



- In **Drive**, specify the drive letter for the connection.
- In **Folder**, specify the folder that you want to connect to. Select **Connect using different credentials** and click **Finish**.

  The folder is in the format of ***\\logical ip address\sharename***.

  Wherein, **logical ip address** indicates the IP address of the storage system's logical port providing the CIFS Homedir share, and **sharename** indicates the name of the CIFS Homedir share.

  NOTE

  If a Homedir share named **autohome** exists in the system, the value of **Folder** can be in the following formats: *logical IP address**username*, *logical IP address**~domain name~domain username*, \|*logical IP address***~**, and *logical IP address***autohome**.

Step 3 In the displayed **Windows Security** dialog box, enter the user name and password for accessing the CIFS Homedir share.

- If you log in as a domain authentication user, enter the domain user name in the *Domain name*|*Domain user name* format and the corresponding password.

  NOTE

  After CIFS shares are allocated to domain users, do not modify the domain user information. If you do, the CIFS shares cannot be accessed.

- If you log in as a local authentication user, enter the user name and password of the local authentication user.

Step 4 Click **OK**.

NOTE

If errors occur during the access, verify that:

- The storage system is added into a correct AD domain.
- The network between the client and storage system is normal.
- The domain user has the access permission.

----End

3.8.5 Configuring an HTTP Share

The procedure for configuring an HTTP share includes preparations, HTTPS service configuration, and HTTP service configuration. The HTTP and HTTPS service configurations differ in listening ports.

- The HTTP service can be enabled when port 80 of the front-end service IP address of the container is listened to.
- The HTTPS service can be enabled when port 443 of the front-end service IP address of the container is listened to.
- Both the HTTP and HTTPS services can be enabled when both ports 80 and 443 of the front-end service IP address of the container are listened to.

With the HTTPS service enabled, you can share a file system in HTTPS mode. After enabling the WebDAV function, you can manage contents in a shared file system.

3.8.5.1 Preparing for the Configuration

Before configuring the HTTPS service, perform the operations in this section to check and configure the environment.

Procedure

Step 1 Check the license. The HTTPS service depends on the license file. Ensure that the imported license file contains SmartContainer License Standard and SmartContainer License Premium.

1. Log in to DeviceManager.
2. On the navigation bar, choose **Settings** > **License Management**.
3. In the middle function pane, verify that **SmartContainer License Standard** and **SmartContainer License Premium** are displayed in the feature list.

   NOTE

   - If no license file has been imported, import a license file by referring to the initialization guide.
   - If **SmartContainer License Standard** or **SmartContainer License Premium** is not displayed in the feature list, contact technical support engineers.

Step 2 Activate the container service. For details, see section "Activating the Container Service" in the *SmartContainer Feature Guide*.

NOTE

The HTTPS service must be deployed based on the container capability provided by the storage system. Before configuring the HTTPS service, you need to activate the container service.

Step 3 Configure the interface module for the HTTPS service. For details, see section "Configuring the Interface Module" in the *SmartContainer Feature Guide*.

NOTE

The interface module used for the HTTPS and FTPS services must be configured as the front-end container mode or back-end container mode. The interface module is exclusively occupied by the container service and cannot be used for other services.

Step 4 Check the certificate. To access the HTTPS service, you need to import an HTTPS certificate. Ensure that the imported certificate contains the HTTPS certificate.

1. Log in to DeviceManager.
2. Choose **Settings** > **Certificates** > **Certificate Management**.
3. In the middle function pane, ensure that **HTTPS certificate** is displayed in the **Scenario** column and the corresponding value in the **Certificate** column is 1.

NOTE

- If the HTTPS certificate fails to be imported, import the certificate by referring to section "Managing the Security Certificate" in the *Security Configuration Guide*.
- To enhance security of links in HTTPS certificate scenarios, you are advised to replace the default security certificates and private keys of the browser and storage system HTTPS service with your security certificates and private keys. For details about how to replace the HTTPS certificate, see section "Managing the Security Certificate" in the *Security Configuration Guide*.

----End

3.8.5.2 Configuring the HTTPS Service (IPv4 Address for Front-End Service)

HTTPS is an application-layer object-oriented protocol. This chapter describes how to use HTTPS services to share directories in a file system.

Prerequisites

The container service has been enabled. Each controller has at least one idle interface module configured to the front-end container mode and only one idle interface module configured to the back-end container mode. The requirements of the interface modules are as follows:

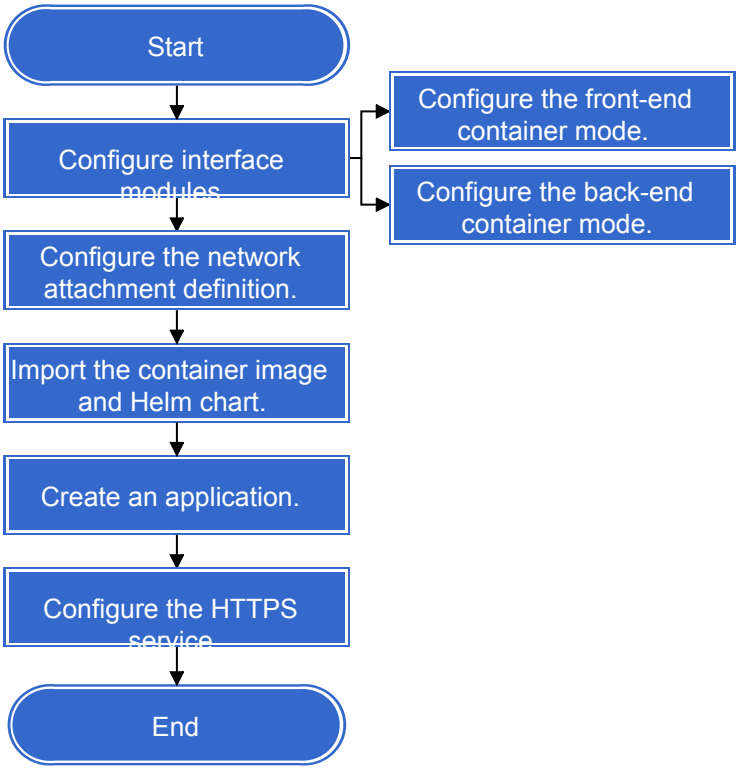
- 10GE electrical interface modules and SmartIO interface modules (with the rate of 10 Gbit/s or 25 Gbit/s) can be configured to the front-end container mode.
- 25 Gbit/s RoCE interface modules can be configured to the back-end container mode.

Configuration Process

The configuration process helps you understand the service configuration logic that needs to be followed during HTTPS service configuration.

Figure 3-10 shows the process of configuring the HTTPS service.

Figure 3-10 HTTPS service configuration process



Configuration Example

The process of configuring the HTTPS service is as follows:

Step 1 Log in to the CLI as an administrator or super administrator.

Step 2 Configure the interface modules.

1. Set the interface modules CTE0.A.IOM2 and CTE0.B.IOM2 to the front-end container mode by running the **change interface_module id=CTE0.A.IOM2,CTE0.B.IOM2 usage_type=container_front_end** command.

   NOTE

   - To obtain the value of **interface_module id**, run the **show interface_module** command without parameters.
   - 10GE electrical interface modules and SmartIO interface modules (with the rate of 10 Gbit/s or 25 Gbit/s) can be configured to the front-end container mode.
   - After an interface module is configured to work in front-end container mode, the interface module can only be used for network communication of container front-end services and does not serve for basic services of the storage system.
   - Before performing this operation, ensure that all services on the interface module have been stopped.

```
developer:/>change interface_module id=CTE0.A.IOM2,CTE0.B.IOM2 usage_type=container_front_end
DANGER: You are about to change the mode of the interface module.
```



```
This operation may cause that the services of all ports on the interface module are interrupted.
Suggestion:
1. Before you perform this operation, ensure that the services of all ports on the interface module are stopped.
2. After performing this operation, the interface module can only be used for network communication of corresponding mode.
Have you read danger alert message carefully?(y/n)y

Are you sure you really want to perform the operation?(y/n)y
Command executed successfully.
```

2. Set the interface modules CTE0.A.IOM3 and CTE0.B.IOM3 to the back-end container mode by running the **change interface_module id=CTE0.A.IOM3,CTE0.B.IOM3 usage_type=container_back_end** command.

   NOTE

   - To obtain the value of **interface_module id**, run the **show interface_module** command without parameters.
   - 25 Gbit/s RoCE interface modules can be configured to the back-end container mode.
   - After an interface module is configured to work in back-end container mode, the interface module can only be used for network communication of container back-end services and does not serve for basic services of the storage system.
   - Before performing this operation, ensure that all services on the interface module have been stopped.

```
developer:/>change interface_module id=CTE0.A.IOM3,CTE0.B.IOM3 usage_type=container_back_end
DANGER: You are about to change the mode of the interface module.
This operation may cause that the services of all ports on the interface module are interrupted.
Suggestion:
1. Before you perform this operation, ensure that the services of all ports on the interface module are stopped.
2. After performing this operation, the interface module can only be used for network communication of corresponding mode.
Have you read danger alert message carefully?(y/n)y

Are you sure you really want to perform the operation?(y/n)y
Command executed successfully.
```

Step 3 Configure the network plane.

1. Create a network plane by running the **create net_plane name=***?* **ipv4_subset_base=***?* **mask=***?* **ipv4_subset_range=***?* **mtu=***?* **failover_enabled=***?* command.

```
admin:/>create net_plane name=net_plane1 ipv4_subset_base=x.x.0.0 mask=255.255.255.0 ipv4_subset_range=x.x.0.13-x.x.0.13 mtu=1500 failover_enabled=yes
Command executed successfully.
```

   NOTE

   In this configuration example, when configuring the network plane for the HTTPS service, pay attention to the following points:

   - If the IP address segment specified by the **ipv4_subset_range** parameter contains only one IP address, this IP address is used for communication between the HTTPS service and the host when an application is created in step **Step 5**.
   - If the IP address segment specified by the **ipv4_subset_range** parameter contains multiple IP addresses, an IP address in the IP address segment is randomly selected for communication between the HTTPS service and the host when an application is created in step **Step 5**.

2. Add ports for the created network plane by running the **add net_plane eth_port net_plane_id=4 port_list=CTE0.A.IOM2.P1,CTE0.A.IOM2.P2,CTE0.B.IOM2.P1,CTE0.B.IOM2.P2** command.

NOTE

The value of **net_plane_id** is the ID of the network plane created in step **Step 3.1**. You can run **show net_plane general** without parameters to obtain the ID.

```
admin:/>add net_plane eth_port net_plane_id=4
port_list=CTE0.A.IOM2.P1,CTE0.A.IOM2.P2,CTE0.B.IOM2.P1,CTE0.B.IOM2.P2
Add ETH port CTE0.A.IOM2.P2 to network plane successfully.
Add ETH port CTE0.B.IOM2.P2 to network plane successfully.
```

Step 4 Import the container image and Helm chart.

1. Obtain the container image and Helm chart.

   Download the container image and Helm chart and save them to a directory on the FTP or SFTP server.

Table 3-67 Software package list

Software Package	Description and How to Obtain
Container image **NOTE** An example of the software name is **OceanStor_*Storage device version*_*Application*_image_signature.tgz**.	The container image version must match the storage device version. – An enterprise user can log in to **http://support.huawei.com/enterprise** to apply for an account and password. Choose **Software Download** > **Centralized Storage**. Click your product model and specify the product version in **Select Version**. Click the desired software in the **Version and Patch** area and then download the corresponding software. – A carrier user can log in to **https://support.huawei.com/carrier**. Search for the product model, click the **Software** tab, and choose the required version to download the corresponding software.

Software Package	Description and How to Obtain
Helm chart **NOTE** An example of the software name is **OceanStor_*Storage device version_Application*_chart_signature.tgz**.	The Helm chart version must match the storage device version. – An enterprise user can log in to **http://support.huawei.com/enterprise** to apply for an account and password. Choose **Software Download** > **Centralized Storage**. Click your product model and specify the product version in **Select Version**. Click the desired software in the **Version and Patch** area and then download the corresponding software. – A carrier user can log in to **https://support.huawei.com/carrier**. Search for the product model, click the **Software** tab, and choose the required version to download the corresponding software.

2. Import the container image named **XXXX_XXX_http_image_signature.tgz** in the **/home/permitdir/** directory by running the following command:

   import container_image ip=x.x.0.14 user=admin password=********** path=/home/permitdir/XXXX_XXX_http_image_signature.tgz**

   NOTE

   Ensure that the container image has been obtained and uploaded to the FTP or SFTP server that can communicate with the management network port of the storage system.

   ```
   admin:/>import container_image ip=x.x.0.14 user=admin password=************ path=/home/permitdir/
   XXXX_XXX_http_image_signature.tgz
   Download package. SUCCESS
   Command executed successfully.
   ```

3. Import the Helm chart named **XXXX_XXX_http_chart_signature.tgz** in the **/home/permitdir/** directory by running the following command:

   import helm_chart ip=x.x.0.14 user=admin password=********** path=/home/permitdir/XXXX_XXX_http_chart_signature.tgz**

   NOTE

   Ensure that the Helm chart has been obtained and uploaded to the FTP or SFTP server that can communicate with the management network port of the storage system.

   ```
   admin:/>import helm_chart ip=x.x.0.14 user=admin password=************ path=/home/permitdir/
   XXXX_XXX_http_chart_signature.tgz
   Download package. SUCCESS
   Command executed successfully.
   ```

Step 5 Create a containerized application to start the HTTPS service by running the following command:

create container_application general app=*?* **version**=*?* **namespace=**? **dynamic_config**=*?*

- **app** indicates the name of the chart package for creating the application. The value of **app** can be obtained from the **Application** field in the command output of the **show helm_chart general** command. An example value is **http-chart**.
- **version** indicates the version of the chart package for creating the application. The value of **version** can be obtained from the **Version** field in the command output of the **show helm_chart general** command.
- **namespace** indicates the application namespace. The value of **namespace** can be obtained from the **namespace** field in the command output of the **show container_application dynamic_config app=? version=?** command. The storage system allows you to access containers whose namespaces are set to **http** and **ftp** to configure and manage the HTTPS and FTPS services.
- **dynamic_config** is the application parameter. You can run the **show container_application dynamic_config app**=*?* **version**=*?* command to obtain the configurable items of **dynamic_config**.

The following is an example command:

```
developer:/>create container_application general app=http-chart version=1.1.0 namespace=http
dynamic_config="netPlaneId=4,storageSize=2Gi"
Command executed successfully.
```

NOTE

- The value of **netPlaneId** is the ID of the network plane created in step **Step 3.1**. You can run **show net_plane general** without parameters to obtain the ID.
- The capacity units supported by **storageSize** are Gi and Ti, which are equivalent to GB and TB (converted based on 1 TB = 1024 GB) used in the storage system.

Step 6 Configure the HTTPS service.

1. Access the container where the HTTPS service is running by running the following command:

   change container_application view pod_name=http-pod-0 namespace=http

   NOTE

   To obtain the value of **pod_name**:

   In versions earlier than 6.1.5, run the **show container_application general name=http-chart** command.

   In 6.1.5 and later versions, run the **show container_application general name=http-chart namespace=http** command.

2. Run the **ifconfig** command to check the front-end service IP address of the container.

   NOTE

   The front-end service IP address of the container is determined by the network segment bound to the network plane during the application creation:

   - In step **Step 3.1**, if the IP segment specified by the **ipv4_subset_range** parameter contains only one IP address, this IP address is the front-end service IP address of the container.
   - In step **Step 3.1**, if the IP segment specified by the **ipv4_subset_range** parameter contains multiple IP addresses, one of these IP addresses is randomly selected as the front-end service IP address of the container.

3. Run the **vi prohttpd/conf/httpd.conf** command to open the configuration file of the HTTPS service.

   a. Press **i** to enter the editing mode.

   b. Change the IP address following **Listen** to the front-end service IP address of the container with a port number specified, and set the port number to **443** used by the HTTPS service.

   c. Type **:wq** and press **Enter** to save the settings and exit.

   The command output is as follows:

```
#Listen 80
#Listen 443

Listen x.x.0.1:80
Listen x.x.0.13:443

#
# Dynamic Shared Object (DSO) Support
```

   NOTE

   - Configure the listening port of the front-end service IP address of the container to control the HTTP and HTTPS services:
     - If port 80 of the front-end service IP address of the container is listened on, the HTTP service can be enabled.
     - If port 443 of the front-end service IP address of the container is listened on, the HTTPS service can be enabled.
     - If ports 80 and 443 of the front-end service IP address of the container are listened on, the HTTP and HTTPS services can be enabled at the same time.
   - As configured in **4.8.3 (Optional) Configuring the Firewall**, the ports allowed by the firewall to be accessed must be consistent with the listening ports of the front-end service IP address of the container.

4. Run the **httpd -k restart** command to enable the modified HTTPS service configuration.

5. Create the **admin** user and set the user password.

   Run the **htpasswd "/mnt/nfs/http/prohttpd/user.passwd" admin** command to create the **admin** user, and set the password as prompted.

   CAUTION

   The password must meet the following requirements:

   - The password contains at least eight characters.
   - The password cannot be the same as the account name.
   - The password must contain at least four types of the following characters: uppercase letters, lowercase letters, digits, and special characters. The special characters include `~!@#$%^&*()-_=+|[{}];:'",<.>/? and spaces.

NOTE

- Common configuration items of the HTTPS service are managed by the files **httpd.conf**, **httpd-ssl.conf**, **http-mpm.conf**, and **httpd-dav.conf**. You can modify these configuration files to manage the HTTPS service.
- The configuration files of the HTTPS service are stored in the **/mnt/nfs/http** directory by default. You can modify the configuration files in this directory to make the configuration result persistent.
- This section describes only some basic configurations of the HTTPS service. For details about the HTTPS service configurations, see related commands of the open-source software httpd.

----End

3.8.5.3 Configuring the HTTPS Service (IPv6 Address for Front-End Service)

HTTPS is an application-layer object-oriented protocol. This chapter describes how to use HTTPS services to share directories in a file system.

Prerequisites

The container service has been enabled. Each controller has at least one idle interface module configured to the front-end container mode and only one idle interface module configured to the back-end container mode. The requirements of the interface modules are as follows:

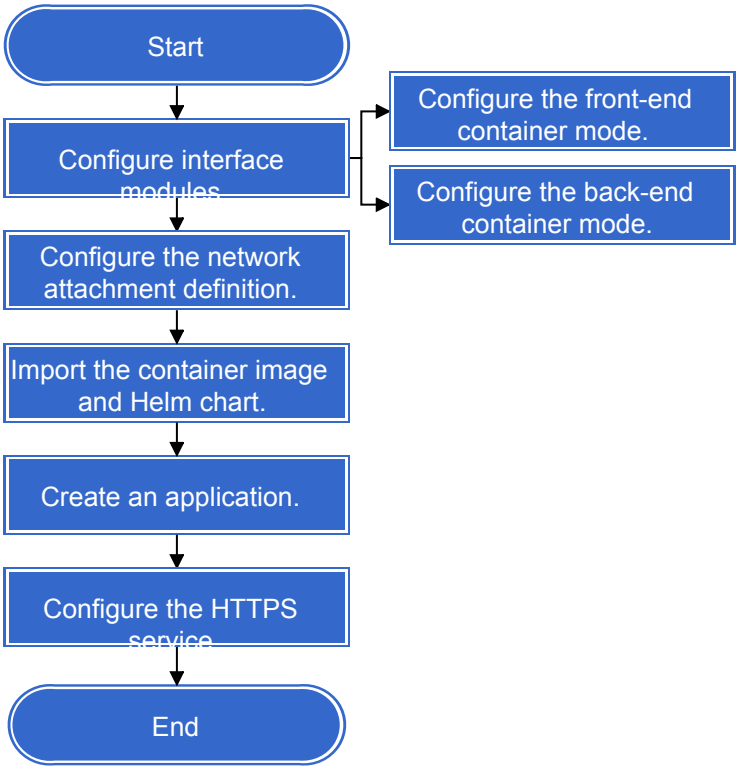
- 10GE electrical interface modules and SmartIO interface modules (with the rate of 10 Gbit/s or 25 Gbit/s) can be configured to the front-end container mode.
- 25 Gbit/s RoCE interface modules can be configured to the back-end container mode.

Configuration Process

The configuration process helps you understand the service configuration logic that needs to be followed during HTTPS service configuration.

Figure 3-11 shows the process of configuring the HTTPS service.

Figure 3-11 HTTPS service configuration process



Configuration Example

The process of configuring the HTTPS service is as follows:

Step 1 Log in to the CLI as an administrator or super administrator.

Step 2 Configure the interface modules.

1. Set the interface modules CTE0.A.IOM2 and CTE0.B.IOM2 to the front-end container mode by running the **change interface_module id=CTE0.A.IOM2,CTE0.B.IOM2 usage_type=container_front_end** command.

   NOTE

   - To obtain the value of **interface_module id**, run the **show interface_module** command without parameters.
   - 10GE electrical interface modules and SmartIO interface modules (with the rate of 10 Gbit/s or 25 Gbit/s) can be configured to the front-end container mode.
   - After an interface module is configured to work in front-end container mode, the interface module can only be used for network communication of container front-end services and does not serve for basic services of the storage system.
   - Before performing this operation, ensure that all services on the interface module have been stopped.

```
developer:/>change interface_module id=CTE0.A.IOM2,CTE0.B.IOM2 usage_type=container_front_end
DANGER: You are about to change the mode of the interface module.
```



```
This operation may cause that the services of all ports on the interface module are interrupted.
Suggestion:
1. Before you perform this operation, ensure that the services of all ports on the interface module are stopped.
2. After performing this operation, the interface module can only be used for network communication of corresponding mode.
Have you read danger alert message carefully?(y/n)y

Are you sure you really want to perform the operation?(y/n)y
Command executed successfully.
```

2. Set the interface modules CTE0.A.IOM3 and CTE0.B.IOM3 to the back-end container mode by running the **change interface_module id=CTE0.A.IOM3,CTE0.B.IOM3 usage_type=container_back_end** command.

   NOTE

   - To obtain the value of **interface_module id**, run the **show interface_module** command without parameters.
   - 25 Gbit/s RoCE interface modules can be configured to the back-end container mode.
   - After an interface module is configured to work in back-end container mode, the interface module can only be used for network communication of container back-end services and does not serve for basic services of the storage system.
   - Before performing this operation, ensure that all services on the interface module have been stopped.

```
developer:/>change interface_module id=CTE0.A.IOM3,CTE0.B.IOM3 usage_type=container_back_end
DANGER: You are about to change the mode of the interface module.
This operation may cause that the services of all ports on the interface module are interrupted.
Suggestion:
1. Before you perform this operation, ensure that the services of all ports on the interface module are stopped.
2. After performing this operation, the interface module can only be used for network communication of corresponding mode.
Have you read danger alert message carefully?(y/n)y

Are you sure you really want to perform the operation?(y/n)y
Command executed successfully.
```

Step 3 Configure the network plane.

1. Create a network plane whose IP address segment is 1::90–1::90 and name is net_plane1 by running the **create net_plane name=net_plane1 ipv6_subset_base=1::0 prefix_length=64 ipv6_subset_range=1::90-1::90 failover_enabled=yes** command.

   NOTE

   In this configuration example, when configuring the network plane for the HTTPS service, pay attention to the following points:

   - If the IP address segment specified by the **ipv6_subset_range** parameter contains only one IP address, this IP address is used for communication between the HTTPS service and the host when an application is created in step **Step 5**.
   - If the IP address segment specified by the **ipv6_subset_range** parameter contains multiple IP addresses, an IP address in the IP address segment is randomly selected for communication between the HTTPS service and the host when an application is created in step **Step 5**.

```
admin:/>create net_plane name=net_plane1 ipv6_subset_base=1::0 prefix_length=64
ipv6_subset_range=1::90-1::90 failover_enabled=yes
Command executed successfully.
```

2. Add ports for the created network plane by running the **add net_plane eth_port net_plane_id=4**

port_list=CTE0.A.IOM2.P1,CTE0.A.IOM2.P2,CTE0.B.IOM2.P1,CTE0.B.IOM2.P2 command.

NOTE

The value of **net_plane_id** is the ID of the network plane created in step **Step 3.1**. You can run **show net_plane general** without parameters to obtain the ID.

```
admin:/>add net_plane eth_port net_plane_id=4
port_list=CTE0.A.IOM2.P1,CTE0.A.IOM2.P2,CTE0.B.IOM2.P1,CTE0.B.IOM2.P2
Add ETH port CTE0.A.IOM2.P2 to network plane successfully.
Add ETH port CTE0.B.IOM2.P2 to network plane successfully.
```

Step 4 Import the container image and Helm chart.

1. Obtain the container image and Helm chart.

   Download the container image and Helm chart and save them to a directory on the FTP or SFTP server.

Table 3-68 Software package list

Software Package	Description and How to Obtain
Container image **NOTE** An example of the software name is **OceanStor_*Storage device version_Application*_image_signature.tgz**.	The container image version must match the storage device version. – An enterprise user can log in to **http://support.huawei.com/enterprise** to apply for an account and password. Choose **Software Download** > **Centralized Storage**. Click your product model and specify the product version in **Select Version**. Click the desired software in the **Version and Patch** area and then download the corresponding software. – A carrier user can log in to **https://support.huawei.com/carrier**. Search for the product model, click the **Software** tab, and choose the required version to download the corresponding software.

Software Package	Description and How to Obtain
Helm chart **NOTE** An example of the software name is **OceanStor_*Storage device version*_*Application*_chart_signature.tgz**.	The Helm chart version must match the storage device version. – An enterprise user can log in to **http://support.huawei.com/enterprise** to apply for an account and password. Choose **Software Download** > **Centralized Storage**. Click your product model and specify the product version in **Select Version**. Click the desired software in the **Version and Patch** area and then download the corresponding software. – A carrier user can log in to **https://support.huawei.com/carrier**. Search for the product model, click the **Software** tab, and choose the required version to download the corresponding software.

2. Import the container image named **XXXX_XXX_http_image_signature.tgz** in the **/home/permitdir/** directory by running the following command:

   import container_image ip=x.x.0.14 user=admin password=********** path=/home/permitdir/XXXX_XXX_http_image_signature.tgz**

   NOTE

   Ensure that the container image has been obtained and uploaded to the FTP or SFTP server that can communicate with the management network port of the storage system.

   ```
   admin:/>import container_image ip=x.x.0.14 user=admin password=************ path=/home/permitdir/XXXX_XXX_http_image_signature.tgz
   Download package. SUCCESS
   Command executed successfully.
   ```

3. Import the Helm chart named **XXXX_XXX_http_chart_signature.tgz** in the **/home/permitdir/** directory by running the following command:

   import helm_chart ip=x.x.0.14 user=admin password=********** path=/home/permitdir/XXXX_XXX_http_chart_signature.tgz**

   NOTE

   Ensure that the Helm chart has been obtained and uploaded to the FTP or SFTP server that can communicate with the management network port of the storage system.

   ```
   admin:/>import helm_chart ip=x.x.0.14 user=admin password=************ path=/home/permitdir/XXXX_XXX_http_chart_signature.tgz
   Download package. SUCCESS
   Command executed successfully.
   ```

Step 5 Create a containerized application to start the HTTPS service by running the following command:

create container_application general app=*?* **version**=*?* **namespace=**? **dynamic_config**=*?*

- **app** indicates the name of the chart package for creating the application. The value of **app** can be obtained from the **Application** field in the command output of the **show helm_chart general** command. An example value is **http-chart**.
- **version** indicates the version of the chart package for creating the application. The value of **version** can be obtained from the **Version** field in the command output of the **show helm_chart general** command.
- **namespace** indicates the application namespace. The value of **namespace** can be obtained from the **namespace** field in the command output of the **show container_application dynamic_config app=? version=?** command. The storage system allows you to access containers whose namespaces are set to **http** and **ftp** to configure and manage the HTTPS and FTPS services.
- **dynamic_config** is the application parameter. You can run the **show container_application dynamic_config app**=*?* **version**=*?* command to obtain the configurable items of **dynamic_config**.

The following is an example command:

```
developer:/>create container_application general app=http-chart version=1.1.0 namespace=http
dynamic_config="netPlaneId=4,storageSize=2Gi"
Command executed successfully.
```

NOTE

- The value of **netPlaneId** is the ID of the network plane created in step **Step 3.1**. You can run **show net_plane general** without parameters to obtain the ID.
- The capacity units supported by **storageSize** are Gi and Ti, which are equivalent to GB and TB (converted based on 1 TB = 1024 GB) used in the storage system.

Step 6 Configure the HTTPS service.

1. Access the container where the HTTPS service is running by running the following command:

   change container_application view pod_name=http-pod-0 namespace=http

   NOTE

   To obtain the value of **pod_name**:

   In versions earlier than 6.1.5, run the **show container_application general name=http-chart** command.

   In 6.1.5 and later versions, run the **show container_application general name=http-chart namespace=http** command.

2. Run the **ifconfig** command to check the front-end service IP address of the container.

   NOTE

   The front-end service IP address of the container is determined by the network segment bound to the network plane during the application creation:

   - In step **Step 3.1**, if the IP segment specified by the **ipv6_subset_range** parameter contains only one IP address, this IP address is the front-end service IP address of the container.
   - In step **Step 3.1**, if the IP segment specified by the **ipv6_subset_range** parameter contains multiple IP addresses, one of the IP addresses is randomly selected as the front-end service IP address of the container.

3. Run the **vi prohttpd/conf/httpd.conf** command to open the configuration file of the HTTPS service.
   a. Press **i** to enter the editing mode.
   b. Change the IP address following **Listen** to the front-end service IP address of the container with a port number specified, and set the port number to **443** used by the HTTPS service.
   c. Type **:wq** and press **Enter** to save the settings and exit.

      The command output is as follows:

      ```
      #Listen 80
      #Listen 443

      Listen 127.0.0.1:80
      Listen [1::99]:443

      #
      # Dynamic Shared Object (DSO) Support
      ```

      NOTE

      - Configure the listening port of the front-end service IP address of the container to control the HTTP and HTTPS services:
        - If port 80 of the front-end service IP address of the container is listened on, the HTTP service can be enabled.
        - If port 443 of the front-end service IP address of the container is listened on, the HTTPS service can be enabled.
        - If ports 80 and 443 of the front-end service IP address of the container are listened on, the HTTP and HTTPS services can be enabled at the same time.
      - As configured in **4.8.3 (Optional) Configuring the Firewall**, the ports allowed by the firewall to be accessed must be consistent with the listening ports of the front-end service IP address of the container.
4. Run the **httpd -k restart** command to enable the modified HTTPS service configuration.
5. Run the **vi /mnt/nfs/http/net_cnet_firewall.ini** command to configure IPv6 port 443 for the firewall. Press **i** to enter the editing mode and set parameters. Then, type **:wq** and press **Enter** to save the settings and exit.

   The command output is as follows:

   ```
   #such as:"21,53,200:300,305"
   tcp_allow_ports="443"
   udp_allow_ports=""
   tcp_allow_ports_ipv6="443"
   udp_allow_ports_ipv6=""
   ```
6. Run the **sh /http/startup.sh firewall** command to make the firewall configuration changes to take effect.
7. Create the **admin** user and set the user password.

   Run the **htpasswd "/mnt/nfs/http/prohttpd/user.passwd" admin** command to create the **admin** user, and set the password as prompted.

CAUTION

The password must meet the following requirements:

- The password contains at least eight characters.
- The password cannot be the same as the account name.
- The password must contain at least four types of the following characters: uppercase letters, lowercase letters, digits, and special characters. The special characters include `~!@#$%^&*()-_=+|[{}];:'",<.>/? and spaces.

NOTE

- Common configuration items of the HTTPS service are managed by the files **httpd.conf**, **httpd-ssl.conf**, **http-mpm.conf**, and **httpd-dav.conf**. You can modify these configuration files to manage the HTTPS service.
- The configuration files of the HTTPS service are stored in the **/mnt/nfs/http** directory by default. You can modify the configuration files in this directory to make the configuration result persistent.
- This section describes only some basic configurations of the HTTPS service. For details about the HTTPS service configurations, see related commands of the open-source software httpd.

----End

3.8.5.4 Accessing the HTTPS Shared Space

This section describes how to access an HTTPS shared space.

Context

The WebDAV function is enabled by default. The WebDAV shared space corresponds to the storage resources in the **mnt/nfs/http/prohttp/uploads** directory of the container.

Using Cadaver Software

Cadaver is a common CLI-based WebDAV client in Linux and UNIX environments.

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

Step 2 Download and install Cadaver. For installation details, see the related document.

Step 3 Run the **cadaver logical ip address** command. **logical ip address** indicates the IP address of the container that provides the HTTPS service.

NOTE

- You can access the shared space by entering **https://IP** only after the HTTPS service is configured as described in section **3.8.5.2 Configuring the HTTPS Service (IPv4 Address for Front-End Service)**.
- If you access the server using HTTPS:
  - An IPv6 address consists of an IP address and a port number. The IP address must be enclosed in square brackets ([]), for example, [1::99]:443.
  - The default service port number is 443.
- By default, the storage system provides the HTTPS service certificate. You are advised to replace the certificate with the private certificate before accessing the HTTPS share space. After the certificate is replaced, the CA certificate of the storage system must be imported for the browser to clear security alarms. As the service IP address is used to access the HTTPS service, alarm "**This website's address does not match the address in the security certificate**" cannot be cleared.
- After the certificate provided by the storage system expires or is revoked, the browser displays a security alarm and you need to replace the certificate.
- The storage system supports HTTP 1.0, HTTP 1.1, and HTTPS (TLS1.2). When accessing the shared space using a web browser, ensure that the browser uses a protocol version supported by the storage system.

Step 4 Enter the user name and password of the local authentication user as prompted.

NOTE

The default security policies for accessing the HTTP share are as follows:

- If a user enters incorrect passwords for three consecutive times within 5 minutes, the user is not allowed to log in for 5 minutes.
- If a host IP address is incorrectly entered for 10 times within 5 minutes, the access to the host IP address is not allowed for 5 minutes.

To modify the security policy for accessing the HTTP share, see **5.3 How Can I Modify Security Policies for Accessing HTTP and FTP Shares?**.

----End

3.8.6 Configuring an FTP Share

FTPS enables file transfer between two hosts that run different OSs and employ different file structures and character sets. After a directory is shared in FTPS mode, FTPS clients can access the directory.

3.8.6.1 Preparing for the Configuration

Before configuring the FTPS service, perform the operations in this section to check and configure the environment.

Procedure

Step 1 Check the license. The FTPS service depends on the license file. Ensure that the imported license file contains SmartContainer License Standard and SmartContainer License Premium.

1. Log in to DeviceManager.
2. On the navigation bar, choose **Settings** > **License Management**.
3. In the middle function pane, verify that **SmartContainer License Standard** and **SmartContainer License Premium** are displayed in the feature list.

NOTE

- If no license file has been imported, import a license file by referring to the initialization guide.
- If **SmartContainer License Standard** or **SmartContainer License Premium** is not displayed in the feature list, contact technical support engineers.

Step 2 Activate the container service. For details, see section "Activating the Container Service" in the *SmartContainer Feature Guide*.

NOTE

The FTPS service must be deployed based on the container capability provided by the storage system. Before configuring the FTPS service, you need to activate the container service.

Step 3 Configure the interface module for the FTPS service. For details, see section "Configuring the Interface Module" in the *SmartContainer Feature Guide*.

NOTE

The interface module used for the HTTPS and FTPS services must be configured as the front-end container mode or back-end container mode. The interface module is exclusively occupied by the container service and cannot be used for other services.

Step 4 Check the certificate. To access the FTPS service, you need to import an FTPS certificate. Ensure that the imported certificate contains the FTPS certificate.

1. Log in to DeviceManager.
2. Choose **Settings** > **Certificates** > **Certificate Management**.
3. In the middle function pane, ensure that **FTPS certificate** is displayed in the **Scenario** column and the corresponding value in the **Certificate** column is 1.

NOTE

- If the FTPS certificate fails to be imported, import the certificate by referring to section "Managing the Security Certificate" in the *Security Configuration Guide*.
- To enhance security of links in FTPS certificate scenarios, you are advised to replace the default security certificates and private keys of the browser and storage system FTPS service with your security certificates and private keys. For details about how to replace the FTPS certificate, see section "Managing the Security Certificate" in the *Security Configuration Guide*.

----End

3.8.6.2 Configuring the FTPS Service (IPv4 Address for Front-End Service)

The storage system enables you to allocate different FTPS share access permissions to different users.

Prerequisites

The container service has been enabled. Each controller has at least one idle interface module configured to the front-end container mode and only one idle interface module configured to the back-end container mode. The requirements of the interface modules are as follows:

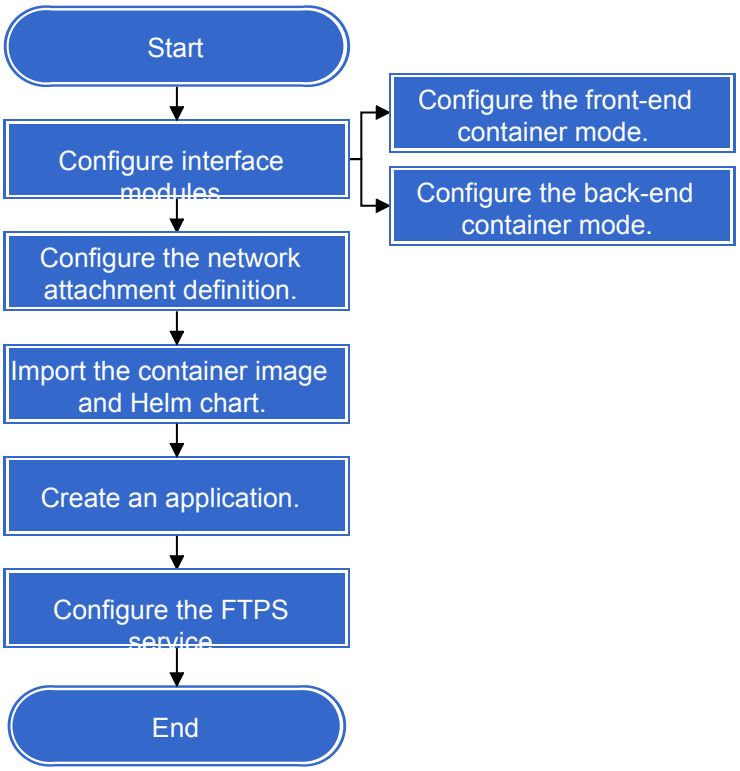
- 10GE electrical interface modules and SmartIO interface modules (with the rate of 10 Gbit/s or 25 Gbit/s) can be configured to the front-end container mode.
- 25 Gbit/s RoCE interface modules can be configured to the back-end container mode.

Configuration Process

The configuration process helps you understand the service configuration logic that needs to be followed during FTPS service configuration.

Figure 3-12 shows the process of configuring the FTPS service.

Figure 3-12 FTPS service configuration process



Configuration Example

The procedure for configuring the FTPS service is as follows:

Step 1 Log in to the CLI as an administrator or super administrator.

Step 2 Configure the interface modules.

1. Run the **change interface_module id=CTE0.A.IOM1,CTE0.B.IOM1 usage_type=container_front_end** command to configure the interface modules CTE0.A.IOM1 and CTE0.B.IOM1 as the front-end container mode.

NOTE

- To obtain the value of **interface_module id**, run the **show interface_module** command without parameters.
- 10GE electrical interface modules and SmartIO interface modules (with the rate of 10 Gbit/s or 25 Gbit/s) can be configured to the front-end container mode.
- After an interface module is configured to work in front-end container mode, the interface module can only be used for network communication of container front-end services and does not serve for basic services of the storage system.
- Before performing this operation, ensure that all services on the interface module have been stopped.

```
developer:/>change interface_module id=CTE0.A.IOM1,CTE0.B.IOM1 usage_type=container_front_end
DANGER: You are about to change the mode of the interface module.
This operation may cause that the services of all ports on the interface module are interrupted.
Suggestion:
1. Before you perform this operation, ensure that the services of all ports on the interface module are stopped.
2. After performing this operation, the interface module can only be used for network communication of corresponding mode.
Have you read danger alert message carefully?(y/n)y

Are you sure you really want to perform the operation?(y/n)y
Command executed successfully.
```

2. Run the **change interface_module id=CTE0.A.IOM3,CTE0.B.IOM3 usage_type=container_back_end** command to set the interface modules CTE0.A.IOM3 and CTE0.B.IOM3 to the back-end container mode.

NOTE

- To obtain the value of **interface_module id**, run the **show interface_module** command without parameters.
- 25 Gbit/s RoCE interface modules can be configured to the back-end container mode.
- After an interface module is configured to work in back-end container mode, the interface module can only be used for network communication of container back-end services and does not serve for basic services of the storage system.
- Before performing this operation, ensure that all services on the interface module have been stopped.

```
developer:/>change interface_module id=CTE0.A.IOM3,CTE0.B.IOM3 usage_type=container_back_end
DANGER: You are about to change the mode of the interface module.
This operation may cause that the services of all ports on the interface module are interrupted.
Suggestion:
1. Before you perform this operation, ensure that the services of all ports on the interface module are stopped.
2. After performing this operation, the interface module can only be used for network communication of corresponding mode.
Have you read danger alert message carefully?(y/n)y

Are you sure you really want to perform the operation?(y/n)y
Command executed successfully.
```

Step 3 Configure the network plane.

1. Create a network plane by running the **create net_plane name=***?* **ipv4_subset_base=***?* **mask=***?* **ipv4_subset_range=***?* **mtu=***?* **failover_enabled=***?* command.

```
admin:/>create net_plane name=net_plane1 ipv4_subset_base=x.x.0.0 mask=255.255.255.0 ipv4_subset_range=x.x.0.15-x.x.0.15 mtu=1500 failover_enabled=yes
Command executed successfully.
```


NOTE

In this configuration example, when configuring the network plane for the FTPS service, pay attention to the following points:

- If the IP address segment specified by the **ipv4_subset_range** parameter contains only one IP address, this IP address is used for communication between the FTPS service and the host when an application is created in step **Step 5**.
- If the IP address segment specified by the **ipv4_subset_range** parameter contains multiple IP addresses, an IP address in the IP address segment is randomly selected for communication between the FTPS service and the host when an application is created in step **Step 5**.

2. Add ports for the created network plane by running the **add net_plane eth_port net_plane_id=1 port_list=CTE0.A.IOM1.P0,CTE0.A.IOM1.P1,CTE0.B.IOM1.P0,CTE0.B.IOM1.P1** command.

NOTE

The value of **net_plane_id** is the ID of the network plane created in step **Step 3.1**. You can run **show net_plane general** without parameters to obtain the ID.

```
admin:/>add net_plane eth_port net_plane_id=1
port_list=CTE0.A.IOM1.P0,CTE0.A.IOM1.P1,CTE0.B.IOM1.P0,CTE0.B.IOM1.P1
Add ETH port CTE0.A.IOM2.P2 to network plane successfully.
Add ETH port CTE0.B.IOM2.P2 to network plane successfully.
```

Step 4 Import the container image and Helm chart.

1. Obtain the container image and Helm chart.

   Download the container image and Helm chart and save them to a directory on the FTP or SFTP server.

Table 3-69 Software package list

Software Package	Description and How to Obtain
Container image **NOTE** An example of the software name is **OceanStor_*Storage device version_Application*_image_signature.tgz**.	The container image version must match the storage device version. – An enterprise user can log in to **http://support.huawei.com/enterprise** to apply for an account and password. Choose **Software Download** > **Centralized Storage**. Click your product model and specify the product version in **Select Version**. Click the desired software in the **Version and Patch** area and then download the corresponding software. – A carrier user can log in to **https://support.huawei.com/carrier**. Search for the product model, click the **Software** tab, and choose the required version to download the corresponding software.

Software Package	Description and How to Obtain
Helm chart **NOTE** An example of the software name is **OceanStor_*Storage device version*_*Application*_chart_signature.tgz**.	The Helm chart version must match the storage device version. – An enterprise user can log in to **http://support.huawei.com/enterprise** to apply for an account and password. Choose **Software Download** > **Centralized Storage**. Click your product model and specify the product version in **Select Version**. Click the desired software in the **Version and Patch** area and then download the corresponding software. – A carrier user can log in to **https://support.huawei.com/carrier**. Search for the product model, click the **Software** tab, and choose the required version to download the corresponding software.

2. Import the container image named **XXXX_XXX_ftp_image_signature.tgz** in the **/home/permitdir/** directory by running the following command:

   import container_image ip=x.x.0.16 user=admin password=********** path=/home/permitdir/XXXX_XXX_ftp_image_signature.tgz**

   NOTE

   Ensure that the container image has been obtained and uploaded to the FTP or SFTP server that can communicate with the management network port of the storage system.

   ```
   admin:/>import container_image ip=x.x.0.16 user=admin password=************ path=/home/permitdir/
   XXXX_XXX_ftp_image_signature.tgz
   Download package. SUCCESS
   Command executed successfully.
   ```

3. Import the Helm chart named **XXXX_XXX_ftp_chart_signature.tgz** in the **/home/permitdir/** directory by running the following command:

   import helm_chart ip=x.x.0.16 user=admin password=********** path=/home/permitdir/XXXX_XXX_ftp_chart_signature.tgz**

   NOTE

   Ensure that the Helm chart has been obtained and uploaded to the FTP or SFTP server that can communicate with the management network port of the storage system.

   ```
   admin:/>import helm_chart ip=x.x.0.16 user=admin password=************ path=/home/permitdir/
   XXXX_XXX_ftp_chart_signature.tgz
   Download package. SUCCESS
   Command executed successfully.
   ```

Step 5 Create a containerized application to start the FTPS service by running the following command:

create container_application general app=*?* **version**=*?* **namespace=**? **dynamic_config**=*?*

- **app** indicates the name of the chart package for creating the application. The value of **app** can be obtained from the **Application** field in the command

output of the **show helm_chart general** command. An example value is **ftp-chart**.

- **version** indicates the version of the chart package for creating the application. The value of **version** can be obtained from the **Version** field in the command output of the **show helm_chart general** command.
- **namespace** indicates the application namespace. The value of **namespace** can be obtained from the **namespace** field in the command output of the **show container_application dynamic_config app=? version=?** command. The storage system allows you to access containers whose namespaces are set to **http** and **ftp** to configure and manage the HTTPS and FTPS services.
- **dynamic_config** is the application parameter. You can run the **show container_application dynamic_config app**=*?* **version**=*?* command to obtain the configurable items of **dynamic_config**.

The following is an example command:

```
admin:/>create container_application general app=ftp-chart version=1.1.0 namespace=ftp
dynamic_config="netPlaneId=1,storageSize=2Gi"
Command executed successfully.
```

NOTE

- The value of **netPlaneId** is the ID of the network plane created in step **Step 3.1**. You can run **show net_plane general** without parameters to obtain the ID.
- The capacity units supported by **storageSize** are Gi and Ti, which are equivalent to GB and TB (converted based on 1 TB = 1024 GB) used in the storage system.

Step 6 Configure the FTPS service.

1. Access the container where the FTPS service is running by running the following command:

   change container_application view pod_name=ftp-pod-0 namespace=ftp

   NOTE

   To obtain the value of **pod_name**:

   In versions earlier than 6.1.5, run the **show container_application general name=ftp-chart** command.

   In 6.1.5 and later versions, run the **show container_application general name=ftp-chart namespace=ftp** command.

2. Run the **ifconfig** command to check the front-end service IP address of the container.

   NOTE

   The front-end service IP address of the container is determined by the network segment bound to the network plane during the application creation:

   - In step **Step 3.1**, if the IP segment specified by the **ipv4_subset_range** parameter contains only one IP address, this IP address is the front-end service IP address of the container.
   - In step **Step 3.1**, if the IP segment specified by the **ipv4_subset_range** parameter contains multiple IP addresses, one of the IP addresses is randomly selected as the front-end service IP address of the container.

3. Run the **vi /mnt/nfs/etc/config/proftpd.conf** command to open the configuration file of the FTPS service.

   a. Press **i** to enter the editing mode.

b. Change the IP address after **DefaultAddress** to the front-end service IP address of the container to listen to the port.

c. Type **:wq** and press **Enter** to save the settings and exit.

The command output is as follows:

```
ServerName                  "FTP Server"
ServerType                  standalone
ServerIdent          off

DefaultAddress      x.x.0.15
SocketBindTight     on

# Port 21 is the standard FTP port.
Port                        21

# Don't use IPv6 support by default.
UseIPv6                     off
```

4. Run the **startup.sh reload** command to enable the modified FTPS service configuration.
5. Configure the FTPS service.

Create an FTP user group and a user.

– Create a user group.

ftpasswd --group --name=Group1 -gid=666 --file=/mnt/nfs/etc/config/ftpd.group

– Create the root directory of the user.

mkdir /mnt/nfs/ftpuser1

chmod 777 /mnt/nfs/ftpuser1

– Create a user.

ftpasswd --sha512 --passwd --file=/mnt/nfs/etc/config/ftpd.passwd --name=user1 --home=/mnt/nfs/ftpuser1 --uid=666 --shell=/usr/sbin/nologin

NOTE

The password must meet the following requirements:

- The password contains at least eight characters.
- The password cannot be the same as the account name.
- The password must contain at least four types of the following characters: uppercase letters, lowercase letters, digits, and special characters. The special characters include `~!@#$%^&*()-_=+|[{}];:'",<.>/? and spaces.

– Add the user to the user group.

ftpasswd --group --name=Group1 --add-member=user1 --file=/mnt/nfs/etc/config/ftpd.group

NOTE

- This section describes only the basic configurations of FTPS users and user groups. For details, see section **4.9.2 Managing Users and Permissions**.
- This section describes only some basic configurations of the FTPS service. For details about the FTPS service configurations, see related commands of the open-source software ftpasswd.

----End

3.8.6.3 Configuring the FTPS Service (IPv6 Address for Front-End Service)

By configuring the FTPS service, you can assign different access permissions to different users.

Prerequisites

The container service has been enabled. Each controller has at least one idle interface module configured to the front-end container mode and only one idle interface module configured to the back-end container mode. The requirements of the interface modules are as follows:

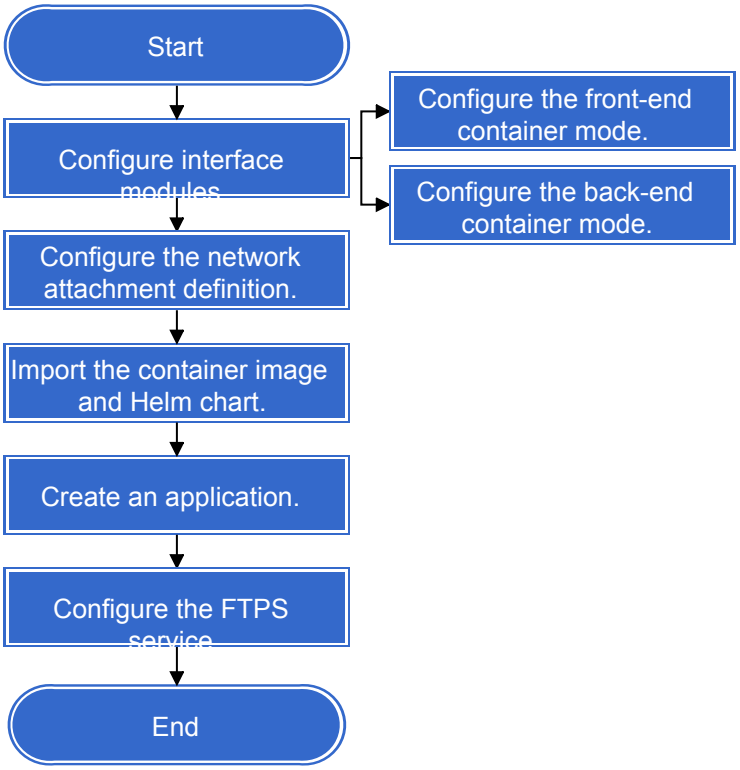
- 10GE electrical interface modules and SmartIO interface modules (with the rate of 10 Gbit/s or 25 Gbit/s) can be configured to the front-end container mode.
- 25 Gbit/s RoCE interface modules can be configured to the back-end container mode.

Configuration Process

The configuration process helps you understand the service configuration logic that needs to be followed during FTPS service configuration.

Figure 3-13 shows the process of configuring the FTPS service.

Figure 3-13 FTPS service configuration process



Configuration Example

The procedure for configuring the FTPS service is as follows:

Step 1 Log in to the CLI as an administrator or super administrator.

Step 2 Configure the interface modules.

1. Run the **change interface_module id=CTE0.A.IOM1,CTE0.B.IOM1 usage_type=container_front_end** command to configure the interface modules CTE0.A.IOM1 and CTE0.B.IOM1 as the front-end container mode.

   NOTE

   - To obtain the value of **interface_module id**, run the **show interface_module** command without parameters.
   - 10GE electrical interface modules and SmartIO interface modules (with the rate of 10 Gbit/s or 25 Gbit/s) can be configured to the front-end container mode.
   - After an interface module is configured to work in front-end container mode, the interface module can only be used for network communication of container front-end services and does not serve for basic services of the storage system.
   - Before performing this operation, ensure that all services on the interface module have been stopped.

   ```
   developer:/>change interface_module id=CTE0.A.IOM1,CTE0.B.IOM1 usage_type=container_front_end
   DANGER: You are about to change the mode of the interface module.
   ```



```
This operation may cause that the services of all ports on the interface module are interrupted.
Suggestion:
1. Before you perform this operation, ensure that the services of all ports on the interface module are stopped.
2. After performing this operation, the interface module can only be used for network communication of corresponding mode.
Have you read danger alert message carefully?(y/n)y

Are you sure you really want to perform the operation?(y/n)y
Command executed successfully.
```

2. Run the **change interface_module id=CTE0.A.IOM3,CTE0.B.IOM3 usage_type=container_back_end** command to set the interface modules CTE0.A.IOM3 and CTE0.B.IOM3 to the back-end container mode.

   NOTE

   - To obtain the value of **interface_module id**, run the **show interface_module** command without parameters.
   - 25 Gbit/s RoCE interface modules can be configured to the back-end container mode.
   - After an interface module is configured to work in back-end container mode, the interface module can only be used for network communication of container back-end services and does not serve for basic services of the storage system.
   - Before performing this operation, ensure that all services on the interface module have been stopped.

```
developer:/>change interface_module id=CTE0.A.IOM3,CTE0.B.IOM3 usage_type=container_back_end
DANGER: You are about to change the mode of the interface module.
This operation may cause that the services of all ports on the interface module are interrupted.
Suggestion:
1. Before you perform this operation, ensure that the services of all ports on the interface module are stopped.
2. After performing this operation, the interface module can only be used for network communication of corresponding mode.
Have you read danger alert message carefully?(y/n)y

Are you sure you really want to perform the operation?(y/n)y
Command executed successfully.
```

Step 3 Configure the network plane.

1. Run the following command to create a network plane whose IP address segment is 1::90–1::90 and name is net_plane1: **create net_plane name=net_plane1 ipv6_subset_base=1::0 prefix_length=64 ipv6_subset_range=1::90-1::90 failover_enabled=yes**

   NOTE

   In this configuration example, when configuring the network plane for the FTPS service, pay attention to the following points:

   - If the IP address segment specified by the **ipv6_subset_range** parameter contains only one IP address, this IP address is used for communication between the FTPS service and the host when an application is created in step **Step 5**.
   - If the IP address segment specified by the **ipv6_subset_range** parameter contains multiple IP addresses, an IP address in the IP address segment is randomly selected for communication between the FTPS service and the host when an application is created in step **Step 5**.

```
admin:/>create net_plane name=net_plane1 ipv6_subset_base=1::0 prefix_length=64 ipv6_subset_range=1::90-1::90 failover_enabled=yes
Command executed successfully.
```

2. Add ports for the created network plane by running the **add net_plane eth_port net_plane_id=1**

port_list=CTE0.A.IOM1.P0,CTE0.A.IOM1.P1,CTE0.B.IOM1.P0,CTE0.B.IOM1.P1 command.

NOTE

The value of **net_plane_id** is the ID of the network plane created in step **Step 3.1**. You can run **show net_plane general** without parameters to obtain the ID.

```
admin:/>add net_plane eth_port net_plane_id=1
port_list=CTE0.A.IOM1.P0,CTE0.A.IOM1.P1,CTE0.B.IOM1.P0,CTE0.B.IOM1.P1
Add ETH port CTE0.A.IOM2.P2 to network plane successfully.
Add ETH port CTE0.B.IOM2.P2 to network plane successfully.
```

Step 4 Import the container image and Helm chart.

1. Obtain the container image and Helm chart.

   Download the container image and Helm chart and save them to a directory on the FTP or SFTP server.

Table 3-70 Software package list

Software Package	Description and How to Obtain
Container image **NOTE** An example of the software name is **OceanStor_*Storage device version_Application*_image_signature.tgz**.	The container image version must match the storage device version. – An enterprise user can log in to **http://support.huawei.com/enterprise** to apply for an account and password. Choose **Software Download** > **Centralized Storage**. Click your product model and specify the product version in **Select Version**. Click the desired software in the **Version and Patch** area and then download the corresponding software. – A carrier user can log in to **https://support.huawei.com/carrier**. Search for the product model, click the **Software** tab, and choose the required version to download the corresponding software.

Software Package	Description and How to Obtain
Helm chart **NOTE** An example of the software name is **OceanStor_*Storage device version_Application*_chart_signature.tgz**.	The Helm chart version must match the storage device version. – An enterprise user can log in to **http://support.huawei.com/enterprise** to apply for an account and password. Choose **Software Download** > **Centralized Storage**. Click your product model and specify the product version in **Select Version**. Click the desired software in the **Version and Patch** area and then download the corresponding software. – A carrier user can log in to **https://support.huawei.com/carrier**. Search for the product model, click the **Software** tab, and choose the required version to download the corresponding software.

2. Import the container image named **XXXX_XXX_ftp_image_signature.tgz** in the **/home/permitdir/** directory by running the following command:

   import container_image ip=x.x.0.16 user=admin password=********** path=/home/permitdir/XXXX_XXX_ftp_image_signature.tgz**

   NOTE

   Ensure that the container image has been obtained and uploaded to the FTP or SFTP server that can communicate with the management network port of the storage system.

   ```
   admin:/>import container_image ip=x.x.0.16 user=admin password=************ path=/home/permitdir/XXXX_XXX_ftp_image_signature.tgz
   Download package. SUCCESS
   Command executed successfully.
   ```

3. Import the Helm chart named **XXXX_XXX_ftp_chart_signature.tgz** in the **/home/permitdir/** directory by running the following command:

   import helm_chart ip=x.x.0.16 user=admin password=********** path=/home/permitdir/XXXX_XXX_ftp_chart_signature.tgz**

   NOTE

   Ensure that the Helm chart has been obtained and uploaded to the FTP or SFTP server that can communicate with the management network port of the storage system.

   ```
   admin:/>import helm_chart ip=x.x.0.16 user=admin password=************ path=/home/permitdir/XXXX_XXX_ftp_chart_signature.tgz
   Download package. SUCCESS
   Command executed successfully.
   ```

Step 5 Create a containerized application to start the FTPS service by running the following command:

create container_application general app=*?* **version**=*?* **namespace=**? **dynamic_config**=*?*

- **app** indicates the name of the chart package for creating the application. The value of **app** can be obtained from the **Application** field in the command output of the **show helm_chart general** command. An example value is **ftp-chart**.
- **version** indicates the version of the chart package for creating the application. The value of **version** can be obtained from the **Version** field in the command output of the **show helm_chart general** command.
- **namespace** indicates the application namespace. The value of **namespace** can be obtained from the **namespace** field in the command output of the **show container_application dynamic_config app=? version=?** command. The storage system allows you to access containers whose namespaces are set to **http** and **ftp** to configure and manage the HTTPS and FTPS services.
- **dynamic_config** is the application parameter. You can run the **show container_application dynamic_config app**=*?* **version**=*?* command to obtain the configurable items of **dynamic_config**.

The following is an example command:

```
admin:/>create container_application general app=ftp-chart version=1.1.0 namespace=ftp
dynamic_config="netPlaneId=1,storageSize=2Gi"
Command executed successfully.
```

NOTE

- The value of **netPlaneId** is the ID of the network plane created in step **Step 3.1**. You can run **show net_plane general** without parameters to obtain the ID.
- The capacity units supported by **storageSize** are Gi and Ti, which are equivalent to GB and TB (converted based on 1 TB = 1024 GB) used in the storage system.

Step 6 Configure the FTPS service.

1. Access the container where the FTPS service is running by running the following command:

   change container_application view pod_name=ftp-pod-0 namespace=ftp

   NOTE

   To obtain the value of **pod_name**:

   In versions earlier than 6.1.5, run the **show container_application general name=ftp-chart** command.

   In 6.1.5 and later versions, run the **show container_application general name=ftp-chart namespace=ftp** command.

2. Run the **vi /mnt/nfs/etc/config/proftpd.conf** command to open the configuration file of the FTPS service, and change the value of **UseIPv6** to **on**. Press **i** to enter the editing mode and set parameters. Then, type **:wq** and press **Enter** to save the settings and exit.
3. Run the **ifconfig** command to check the front-end service IP address of the container.

NOTE

The front-end service IP address of the container is determined by the network segment bound to the network plane during the application creation:

- In step **Step 3.1**, if the IP segment specified by the **ipv6_subset_range** parameter contains only one IP address, this IP address is the front-end service IP address of the container.
- In step **Step 3.1**, if the IP segment specified by the **ipv6_subset_range** parameter contains multiple IP addresses, one of the IP addresses is randomly selected as the front-end service IP address of the container.

4. Run the **vi /mnt/nfs/etc/config/proftpd.conf** command to open the configuration file of the FTPS service.
   a. Press **i** to enter the editing mode.
   b. Change the IP address after **DefaultAddress** to the front-end service IP address of the container to listen to the port.
   c. Change the value of **UseIPv6** to **on** to enable the IPv6 service.
   d. Type **:wq** and press **Enter** to save the settings and exit.

   The command output is as follows:

```
ServerName                      "FTP Server"
ServerType                      standalone
ServerIdent             off

DefaultAddress      1::90
SocketBindTight     on

# Port 21 is the standard FTP port.
Port                            21

# Don't use IPv6 support by default.
UseIPv6                         on
```

5. Run the **startup.sh reload** command to enable the modified FTPS service configuration.
6. Run the **vi /mnt/nfs/etc/config/net_cnet_firewall.ini** command to open the firewall configuration file. Press **i** to enter the editing mode and set parameters. Then, type **:wq** and press **Enter** to save the settings and exit.

   The command output is as follows:

```
#such as:"21,53,200:300,305"
tcp_allow_ports="20,21,989:990,51000:52000"
udp_allow_ports=""
tcp_allow_ports_ipv6="20,21,989:990,51000:52000"
udp_allow_ports_ipv6=""
```

7. Run the **startup.sh firewall** command to make the firewall configuration changes to take effect.
8. Configure the FTPS service.

   Create an FTP user group and a user.

   - Create a user group.

     ftpasswd --group --name=Group1 -gid=666 --file=/mnt/nfs/etc/config/ftpd.group

   - Create the root directory of the user.

     mkdir /mnt/nfs/ftpuser1

     chmod 777 /mnt/nfs/ftpuser1

- Create a user.

  ftpasswd --sha512 --passwd --file=/mnt/nfs/etc/config/ftpd.passwd --name=user1 --home=/mnt/nfs/ftpuser1 --uid=666 --shell=/usr/sbin/nologin

  NOTE

  The password must meet the following requirements:

  - The password contains at least eight characters.
  - The password cannot be the same as the account name.
  - The password must contain at least four types of the following characters: uppercase letters, lowercase letters, digits, and special characters. The special characters include `~!@#$%^&*()-_=+|[{}];:'",<.>/? and spaces.

- Add the user to the user group.

  ftpasswd --group --name=Group1 --add-member=user1 --file=/mnt/nfs/etc/config/ftpd.group

  NOTE

  - This section describes only the basic configurations of FTPS users and user groups. For details, see section **4.9.2 Managing Users and Permissions**.
  - This section describes only some basic configurations of the FTPS service. For details about the FTPS service configurations, see related commands of the open-source software ftpasswd.

----End

3.8.6.4 Accessing the FTP Shared Space

This section describes how to access the FTP shared space.

Context

The corresponding path in the container for storage resources in the FTP shared space is the root directory path created by the user in steps **Step 6.8**.

Accessing FTP Shares over FTPS

Currently, you can only access FTP shares over FTPS using related tool software. The following describes how to access FTP shares over FTPS using FileZilla software as an example.

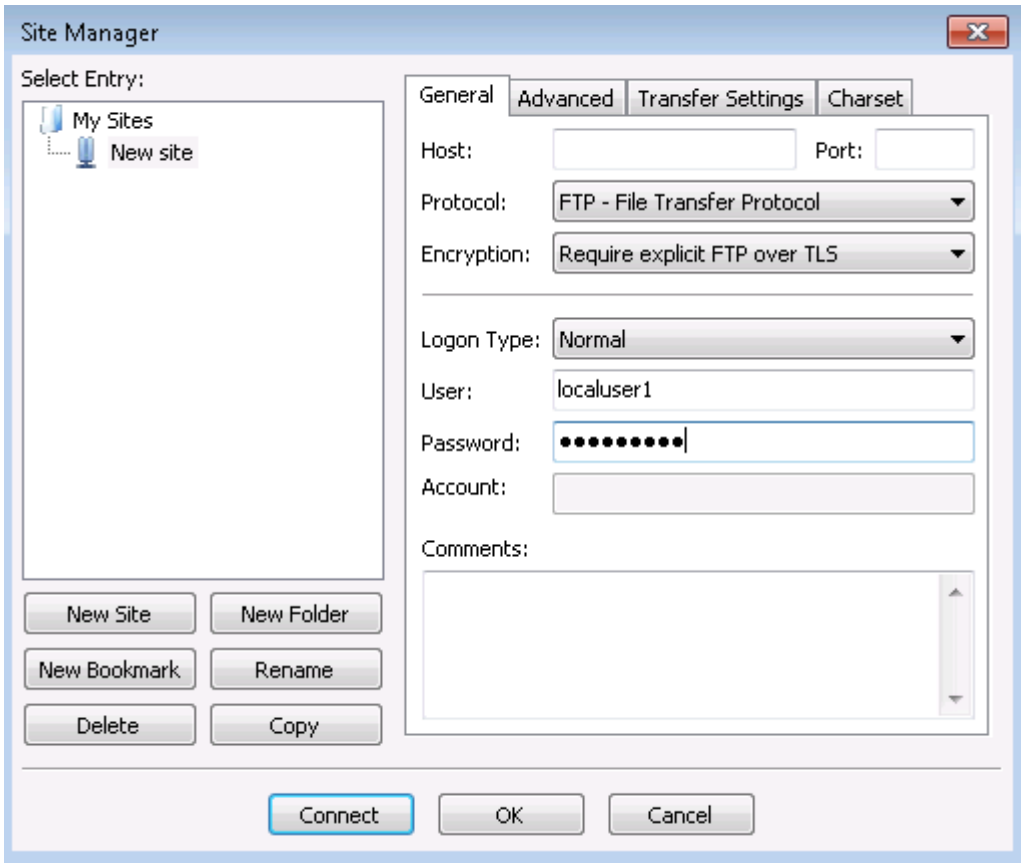
Step 1 Open the FileZilla client software.

Step 2 Choose **File** > **Site Manager**.

The **Site Manager** dialog box is displayed.

Step 3 Click **New site** to create a site.

Step 4 On the **General** tab page, type configuration information of storage system's FTP shares.



Description of parameters in the above figure:

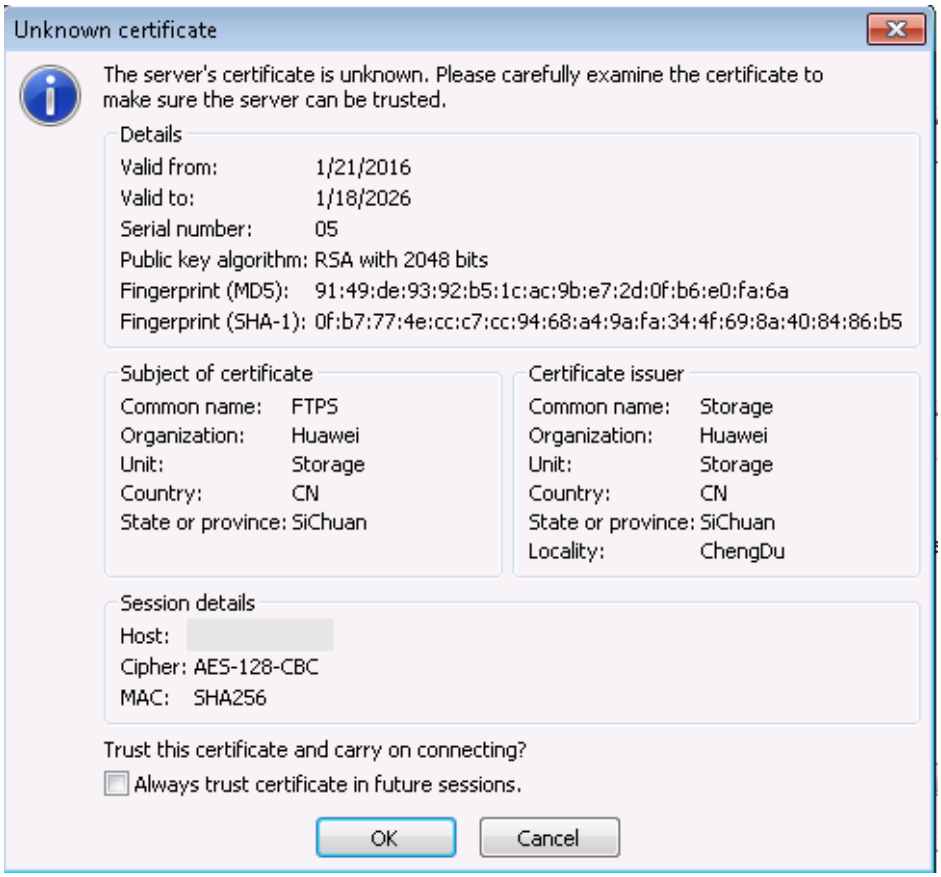
- **Host** indicates the IP address of the container that provides the FTPS service in the storage system.
- **Port** indicates the default port.
- **Protocol** indicates the used protocol type. Select **FTP - File Transfer Protocol** if you use FTPS.
- **Encryption** indicates the encryption mode. The value that you select must be consistent with that set in **FTPS Connection Mode**. If **FTPS Connection Mode** is **Show**, select **Require explicit FTP over TLS**. If **FTPS Connection Mode** is **Hide**, select **Require implicit FTP over TLS**.
- **Logon Type** indicates the login mode. Select **Normal** here.
- **User** indicates the name of a user account used to access FTP shares.
- **Password** indicates the password used to access FTP shares.

  NOTE

  If a host fails to log in to the FTP shared space for three or more times within 5 minutes, the default security policy of the system prohibits the host from accessing the FTP share within the next 5 minutes. To modify the security policy, see **5.3 How Can I Modify Security Policies for Accessing HTTP and FTP Shares?**.

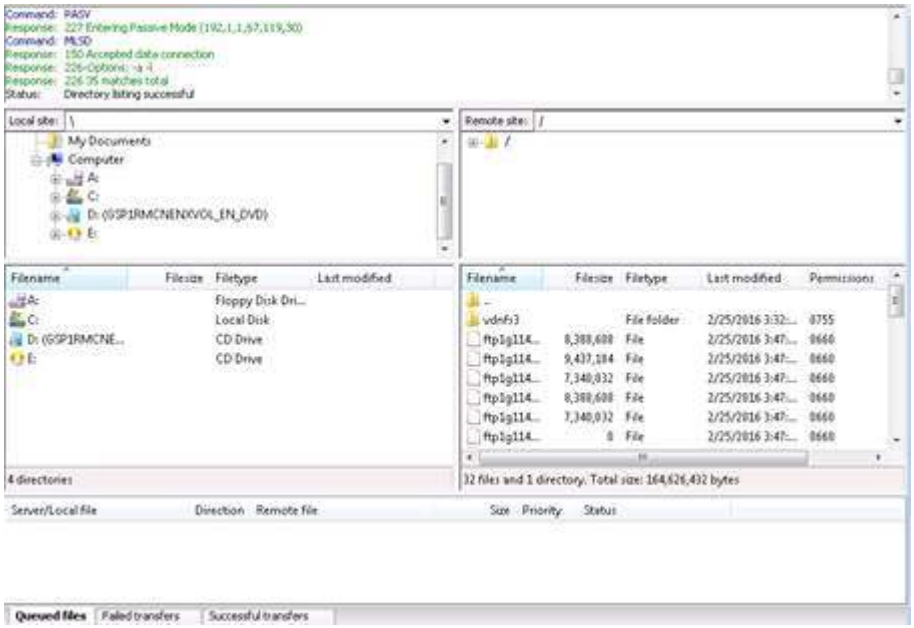
Step 5 Click **Connect** to connect to the FTP server.

If you use the default certificate, a certificate warning message is displayed.



Step 6 (Optional) Click **OK** to confirm the certificate information.

Step 7 Go to the page of FTP shares.



----End

3.8.7 Accessing Cross-Protocol Shares

A storage system allows NFS and CIFS shares to be configured for the same file system concurrently. This section describes how a storage system uses the user mapping function to allow users to access shared files across protocols (CIFS-NFS) used by clients on different platforms and implement precise permission control.

3.8.7.1 Overview

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

CIFS-NFS Share Access

A storage system allows users to share a file system or dtree using NFS and CIFS at the same time. Different clients can access a file system or dtree simultaneously. Windows, Linux, and UNIX adopt different mechanisms to authenticate users and control access. The storage system manages user mapping and permission control of different operating systems in a unified manner, protecting the security of CIFS-NFS share access.

- If a CIFS user attempts to access a file or directory, the storage system authenticates local or AD domain users first. If the UNIX permission (UNIX Mode bits) has been configured for the file or directory, the CIFS user is mapped as an NFS user based on preset user mapping rules during authentication. Then the storage system performs UNIX permission authentication for the user.
- If an NFS user attempts to access a file or directory with NT ACLs, the NFS user is mapped as a CIFS user based on the preset mapping rules. Then the storage system performs NT ACL permission authentication for the user.

CIFS-NFS Share Access Permissions

If permission types of a file or directory and a client that attempts to access the file or directory do not match, CIFS-NFS cross-protocol access is required and you must map the permission of the file or directory so that it can be displayed by the client.

- NFS client accessing a file or directory with the NTFS permission

  When an NFS client checks the NTFS permission that a file or directory has, the client can obtain the UNIX permission mapped from an NT ACL. The NFS client displays as many permissions as possible but the actual permissions are determined by the NT ACL. For example, the NFS client shows that all users have read, write, and execute permissions, but one of the users may only have the write permission.

- CIFS client accessing a file or directory with the UNIX permission

  When a CIFS client checks the UNIX permission that a file or directory has, the UNIX permission is mapped into four ACEs for the CIFS client. The ACEs are for the owner, owner primary group, **everyone**, and the current Windows user for the file or directory respectively. The NT ACL is displayed only but not used to control actual operation permissions.

Table 3-71 shows how permissions are converted among UNIX Mode bits and NT ACLs.

Table 3-71 Permission conversion among UNIX Mode bits and NT ACLs

File Permission	Permission Conversion
A file or directory only has valid UNIX Mode bits.	• If an NFS or CIFS client sends a request to read an ACL, one ACL is mapped based on UNIX Mode bits. • If a CIFS client sends a request to set an ACL, an NT ACL takes effect and UNIX Mode bits with the maximum permissions are mapped based on the NT ACL.
A file or directory has a valid NT ACL.	If an NFS client sends a request to read UNIX Mode bits, UNIX Mode bits (mapped based on the NT ACL) of the storage system are returned directly.

CIFS-NFS User Mapping

Windows systems (CIFS) and Linux systems (NFS) use different mechanisms to identify and authenticate users:

- Windows systems use security identifiers (SIDs) to identify users. SIDs apply to all users, user groups, services, and computers in the systems. CIFS supports NT ACLs for authentication.
- 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. NFS supports diversified security control mechanisms such as UNIX Mode bits for authentication.

During CIFS-NFS 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:

- For a CIFS client, a user mapping occurs when the security mode of the file system to be accessed is UNIX, that is, files or directories in the file system have only the UNIX Mode bits permission. A user will have both the permissions before and after user mapping.
- For an NFS client, a user mapping occurs when the security mode of the file system to be accessed is NTFS, that is, files or directories in the file system have the NT ACL permission. A user will have both the permissions before and after user mapping.
- When a parent directory has inheritable NT ACL permission, 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, a user will have both the permissions before and after user mapping. When the parent directory does not have any inheritable NT ACL permission, files or directories created no matter on an NFS client or a CIFS client will have the UNIX Mode bits

permission. In this case, if the NFS client accesses files or directories, no user mapping occurs. That is, the user's permission remains unchanged.

- If mappings are changed on CIFS clients, the change takes effect after CIFS connections are disconnected and next re-authentication is performed.
- User mappings on NFS clients are cached and expire after four hours by default. New user mappings and user information changes take effect after the cached data expires.

User mapping rules specify the mappings among different user accounts. They can be saved in a local database or managed in an AD domain in a centralized manner. A user mapping rule includes the mapping type, source 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.

The following describes how local user mapping is performed:

- 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 storage system, LDAP domain, and NIS domain. Based on the queried user name and the local mapping, the user name, SID, and owning group of the mapped user will be queried.
- CIFS-NFS user mapping: A CIFS user is authenticated by SID on the service end. When a user mapping occurs, the mapped user will be queried based on the user name to which the SID corresponds and the local mapping. Then the UID to which the mapped user name corresponds and its owning group will be queried in the sequence of the local storage system, LDAP domain, and NIS domain.

NOTE

It is not advised to configure the same UID or user name in the local storage system, LDAP domain, or NIS domain. If the same UID or user name exists, the user mapping results will not be the expected results.

After user mapping, on an NFS client, the owner information of files or directories owned by CIFS users (the files or directories that are created by CIFS users or the owner information of the files or directories are changed to CIFS users) is the information of the NFS users mapped from CIFS users. If no mapping rules have been configured for CIFS users, the owner information of the files or directories is about the IDs (calculated using IDMAP, a hash algorithm) of the CIFS users.

After user mapping, on a CIFS client, the owner information of the files or directories owned by NFS users (the files or directories that are created by NFS users or the owner information of the files or directories are changed to NFS users) is about NFS user names. If NFS users are NIS or LDAP domain users, the owner information is displayed as **UNIXUser***user name*.

NOTE

When CIFS users are mapped to NFS users, quota statistics will be collected for the NFS users or owning user group.

3.8.7.2 Managing CIFS-NFS User Mappings

Managing CIFS-NFS user mappings includes configuring the mapping parameters and creating a user mapping.

3.8.7.2.1 Configuring Mapping Parameters

You can create user mappings in both the local storage system and the external IDMU domain to access shares across different systems. The following introduces how to set the mapping mode as well as timeout duration of the IDMU query, and search for the domain name.

Context

If you only use IDMU user mappings, you do not need to configure user mappings in the local storage system.

Procedure

Step 1 Choose **Services** > **File Service** > **Authentication Users** > **User Mappings**.

Step 2 Select the vStore for which you want to configure mapping parameters from the **vStore** drop-down list in the upper left corner.

Step 3 Click **Set Mapping Parameter**.

The **Set Mapping Parameter** page is displayed on the right.

Step 4 Enable **Mapping Parameters** and configure user mapping parameters.

Table 3-72 describes the parameters.

Table 3-72 Mapping parameters

Parameter	Description
Mapping Mode	Global parameter of user mappings, including: • **Support only user mapping of this system**: The system only supports user mappings created in this system. • **Support only user mapping in IDMU**: The system only supports user mappings in the IDMU domain. • **Preferentially support user mapping in IDMU**: When user mappings of a specified source user exist both in the system and the IDMU domain, the system preferentially uses the mapping in the IDMU domain. • **Preferentially support user mapping of this system**: When user mappings of a specified source user exist both in the system and the IDMU domain, the system preferentially uses the mapping in this system.

Parameter	Description
IDMU Search Timeout Duration (s)	Timeout duration for the system to search for a specified user mapping in the IDMU domain. [Value range] 5 to 120
IDMU Search DN	Benchmark directory where the system searches for a specified user mapping in the IDMU domain. The benchmark directory stores the information of user mappings. [Value range] The directory contains 0 to 255 characters.
Map to User with Same Name	Indicates whether to map to users with the same name. After this function is enabled, the system automatically maps UNIX users and Windows users with the same name.
Default UNIX User	When user mapping is enabled and a Windows user fails to be mapped, the Windows user will be mapped to this default UNIX user.
Default Windows User	When user mapping is enabled and a UNIX user fails to be mapped, the UNIX user will be mapped to this default Windows user. If the default Windows user is an AD domain user, the naming format is *Domain name**Domain user name*. The AD domain name can only be a NetBIOS name. You can query the NetBIOS name of a domain by running the **nbtstat -n** command. Alternatively, you can right-click the domain on the **Active Directory Users and Computers** page, choose **Properties** from the shortcut menu, and find the value of **Domain name (pre-Windows 2000)** in the dialog box that is displayed. The value is the NetBIOS name of the domain.

NOTE

Map to User with Same Name, **Default UNIX User**, and **Default Windows User** are available only when **Mapping Mode** is set to **Support only user mapping of this system**, **Preferentially support user mapping in IDMU**, or **Preferentially support user mapping of this system**. **IDMU Search Timeout Duration (s)** and **IDMU Search DN** are available only when **Mapping Mode** is set to **Support only user mapping in IDMU**, **Preferentially support user mapping in IDMU**, or **Preferentially support user mapping of this system**.

Step 5 Confirm your operation as prompted.

----End

3.8.7.2.2 Creating a User Mapping

This operation enables the system to map a source user to a target user based on a mapping relationship for accessing shares across protocols.

NOTE

If **Map to User with Same Name** is enabled, default user mapping (**Default UNIX User** or **Default Windows User**) is configured, and user mapping is created, you can follow the following sequence to search for user mapping: the created user mappings > user mappings with the same name > the default user mapping.

Procedure

Step 1 Choose **Services** > **File Service** > **Authentication Users** > **User Mappings**.

Step 2 Select the vStore for which you want to create a user mapping from the **vStore** drop-down list in the upper left corner.

Step 3 Click **Create**.

The **Create User Mapping** page is displayed on the right.

Step 4 Set basic user mapping parameters.

Table 3-73 describes the parameters.

Table 3-73 Basic user mapping parameters

Parameter	Description
Mapping Mode	User mapping mode related to the operating system. Possible options are: • **Windows to UNIX**: When accessing UNIX shares using Windows, a Windows user has all the permissions granted to the target user. • **UNIX to Windows**: When accessing Windows shares using UNIX, a UNIX user has all the permissions granted to the target user. • **Kerberos to UNIX**: When a client accesses UNIX shares through Kerberos authentication, the Kerberos user has all the permissions granted to the target user.

Parameter	Description
Source User	Source user in the mapping. **NOTE** • The name of the source user supports the wildcard (*). For example, **user*** indicates all user names starting with **user**. • The user name can be a common or domain user name. An AD domain user name uses a backslash (\) to connect the domain name and user name. Only one backslash (\) is allowed, for example, **china\user001**. The AD domain name can only be a NetBIOS name. You can query the NetBIOS name of a domain by running the **nbtstat -n** command. Alternatively, you can right-click the domain on the **Active Directory Users and Computers** page, choose **Properties** from the shortcut menu, and find the value of **Domain name (pre-Windows 2000)** in the dialog box that is displayed. The value is the NetBIOS name of the domain.
Target User	Target user in the mapping. **NOTE** The user name can be a common or domain user name. An AD domain user name uses a backslash (\) to connect the domain name and user name. Only one backslash (\) is allowed, for example, **china\user001**. The AD domain name can only be a NetBIOS name. You can query the NetBIOS name of a domain by running the **nbtstat -n** command. Alternatively, you can right-click the domain on the **Active Directory Users and Computers** page, choose **Properties** from the shortcut menu, and find the value of **Domain name (pre-Windows 2000)** in the dialog box that is displayed. The value is the NetBIOS name of the domain.
Priority	Priority of the mapping. A smaller value indicates a higher priority. When multiple mappings share the same source user, the system uses the mapping with the highest priority. [Value range] 1 to 32

Step 5 Click **Add to Mapping List** to add the mapping to the list below.

NOTE

You can set user mapping parameters and click **Add to Mapping List** to configure multiple user mappings.

Step 6 Test, modify, or delete a user mapping.

- Testing a user mapping

  Select a user mapping and click **Test** to check whether the target user in the user mapping exists.

  NOTE

  You can also click **More** on the right of a desired user mapping and select **Test**.

- Modifying a user mapping

  a. Click **More** on the right of the desired user mapping and select **Modify**.

  The **Modify User Mapping** page is displayed on the right.

b. Set basic user mapping parameters.
   Table 3-73 describes the parameters.
c. Click **OK**.

- Deleting a user mapping
  Select one or more desired user mappings and click **Delete**.

  NOTE

  You can also click **More** on the right of a desired user mapping and select **Delete**.

Step 7 Click **OK**.

----End

Example

- User mapping rule example 1: Map Windows user **win_user01** to UNIX user **ux_user01**.
  - Source user: win_user01
  - Target user: ux_user01
  - Mapping type: Windows to Unix
  - Priority: 10 (default)
- User mapping rule example 2: Map any UNIX user to **user1** in the AD domain (domain name **authtest**).
  - Source user: *
  - Target user: authtest\user1
  - Mapping type: Unix to Windows
  - Priority: 10 (default)

3.8.7.3 Accessing a CIFS File Across Protocols

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

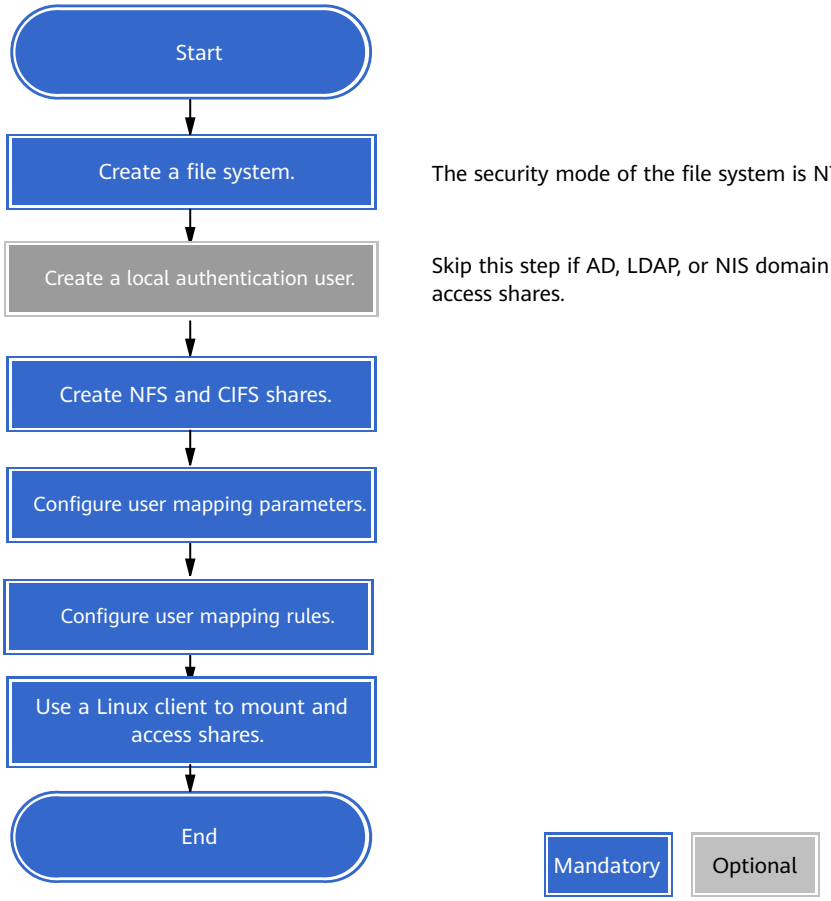
Prerequisites

- The user of the Linux client has the same UID and GID as the local authentication user.
  You can query the local authentication user ID and ID of its owning primary group on the DeviceManager. On the Linux client, you can run the **groupadd -g** *GID user group name* command to create a user group, and then run the **useradd -u** *UID* **-g** *GID user name* command to create a user.
- Before you use an AD domain user to configure user mapping rules, the storage system has been added to the AD domain.

Context

Before users can use an NFS client to access shared files and folders for which NT ACLs have been configured, the administrator must follow the process as shown in Figure 3-14 to configure related parameters.

Figure 3-14 Flowchart of configuring cross-protocol access of a CIFS file



Example

Table 3-74 provides an example of data planning during the configuration.

Table 3-74 Example of data planning

Item	Planned Value
File system	Name: share_dir Security mode: NTFS

Item	Planned Value
Local authentication user	Name: unix_user1 ID: 100001 Primary group name: unix_group Primary group ID: 100000
	Name: cifs_user1
NFS client user	Name: unix_user1 The user must have the same UID and GID as the local authentication user.
NFS share	• File system: share_dir • Type of the client: host • Name or IP address: x.x.0.10 • Permission: Read-write • Advanced: The default settings are used.
CIFS share	• File system: share_dir • Share name: share_dir_cifs • Local authentication user: cifs_user1 • Permission level: Full control
Mapping Mode	Local system user mappings are supported preferentially.
User mapping rule	• Mapping type: Unix to Windows • Source user: **unix_user1** • Target user: **cifs_user1** • Priority: 10

Step 1 Create a file system.

1. Choose **Services** > **File Service** > **File Systems**.
2. Create a file system named **share_dir** as planned.

Step 2 Create a local UNIX authentication user group and user.

1. Choose **Services** > **File Service** > **Authentication Users** > **UNIX Users** > **Local Authentication User Groups**.
2. Click **Create** to create a local authentication user group named **unix_group** as planned.

3. Choose **Services** > **File Service** > **Authentication Users** > **UNIX Users** > **Local Authentication Users**.
4. Click **Create** to create a local authentication user named **unix_user1** as planned.

Step 3 Create a local Windows authentication user.

1. Choose **Services** > **File Service** > **Authentication Users** > **Windows Users** > **Local Authentication Users**.
2. Click **Create** to create a local authentication user named **cifs_user1** as planned.

Step 4 Create an NFS share and a CIFS share for the same file system.

1. Choose **Services** > **File Service** > **Shares.**
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. Choose **Services** > **File Service** > **Authentication Users** > **User Mappings**.
2. Click **Set Mapping Parameter** and set **Mapping Mode** to **Preferentially support user mapping of this system.**

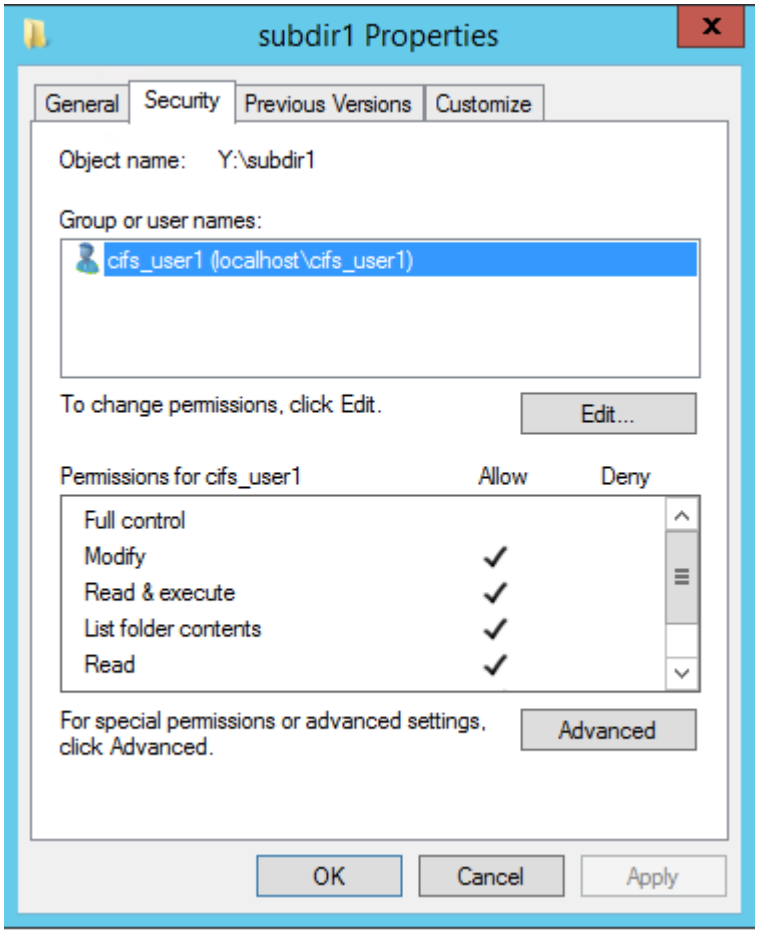
Step 6 Configure user mapping rules.

1. Choose **Services** > **File Service** > **Authentication Users** > **User Mappings**.
2. Click **Create** and configure user mapping rules as planned.

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 modify permission ACE to user **cifs_user1**.
4. Delete the **Everyone** permissions for **subdir1,** so as to verify that the NFS client has permissions of the mapped Windows user.



Step 8 Run the **change service nfs_config g_ntfs_unix_security_ops=ignore** command on the storage system to ignore any modification on NFS client permissions.

NOTE

This operation is required because **Security Style** of the file system **share_dir** in this example is **NTFS** and Windows ACLs exist.

Step 9 Use an NFS client to mount the share and access the share as local user **unix_user1**.

1. Use an NFS client to mount the NFS share.
2. Run the **groupadd -g 100000 unix_group** command to create a user group that has the same GID as the local authentication user group.
3. Run the **useradd -u 100001 -g 100000 unix_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 - unix_user1** command to switch users.
5. Write data to folder **subdir1**.

   If the data is written to the folder successfully, the Linux client has a write permission for the folder.

----End

3.8.7.4 Accessing an NFS File Across Protocols

This section describes how a CIFS client accesses a file or directory for which the UNIX permission has been configured.

Prerequisites

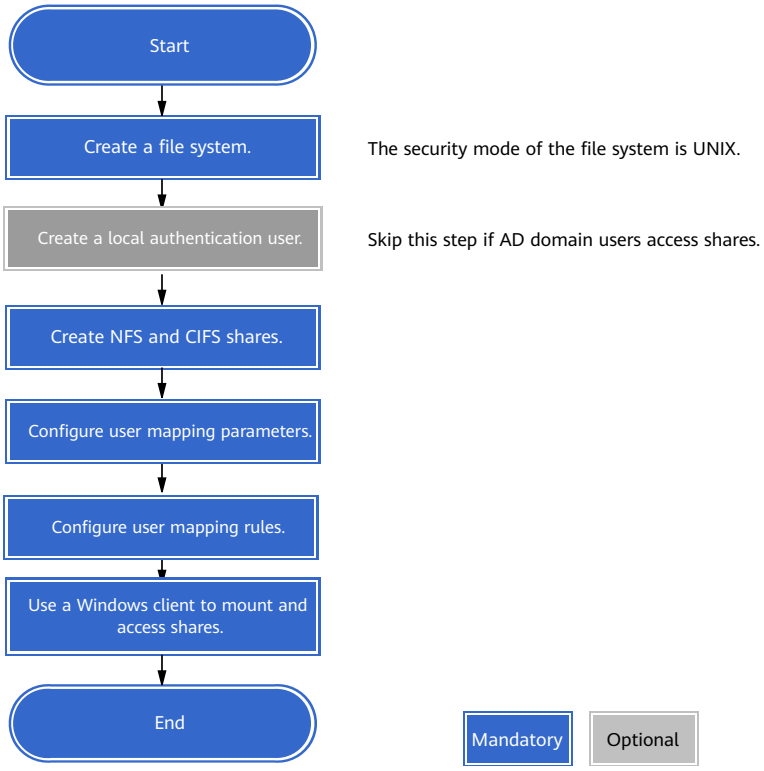
The user of the Linux client has the same UID and GID as the local authentication user.

You can query the local authentication user ID and ID of its owning primary group on the DeviceManager. On the Linux client, you can run the **groupadd -g** *GID user group name* command to create a user group, and then run the **useradd -u** *UID* **-g** *GID user name* command to create a user.

Context

Before users can use a Windows client to access shared files and folders for which the UNIX permission has been configured, the administrator needs to follow the process as shown in **Figure 3-15** to configure related parameters.

Figure 3-15 Flowchart of configuring cross-protocol access of an NFS file



Example

Table 3-75 provides an example of data planning during the configuration.

Table 3-75 Example of data planning

Item	Planned Value
File system	Name: share_dir2 Security mode: UNIX
Local authentication user	Name: cifs_user2
	Name: unix_user2 ID: 100002 Primary group name: unix_group Primary group ID: 100000
NFS client user	Name: unix_user2 The user must have the same UID and GID as the local authentication user.

Item	Planned Value
NFS share	• File system: share_dir2 • Type of the client: host • Name or IP address: x.x.0.10 • Permission: Read-write • Advanced: The default settings are used.
CIFS share	• File system: share_dir2 • Share name: share_dir_cifs2 • Local authentication user: cifs_user2 • Permission level: Full control
Mapping Mode	Local system user mappings are supported preferentially.
User mapping rule	• Mapping type: Windows to Unix • Source user: cifs_user2 • Target user: unix_user2 • Priority: 10

Windows operating systems do not allow a file name to contain special characters. Therefore, it is recommended that the file name and directory name of an NFS share do not contain special characters including \:*/?"<>|, and the file name and directory name do not end with a period (.) or a space. Otherwise, the storage system converts the file name and directory name to short names (for example, **~PY203**).

Step 1 Create a file system.

1. Choose **Services** > **File Service** > **File Systems**.
2. Create a file system named **share_dir2** as planned.

Step 2 Create a local Windows authentication user.

1. Choose **Services** > **File Service** > **Authentication Users** > **Windows Users** > **Local Authentication Users**.
2. Click **Create** to create a local authentication user named **cifs_user2** as planned.

Step 3 Create a UNIX local authentication user group and user.

1. Choose **Services** > **File Service** > **Authentication Users** > **UNIX Users** > **Local Authentication User Groups**.

2. Click **Create** to create a local authentication user group named **unix_group** as planned.

3. Choose **Services** > **File Service** > **Authentication Users** > **UNIX Users** > **Local Authentication Users**.
4. Click **Create** to create a local authentication user named **unix_user2** as planned.

Step 4 Create an NFS share and a CIFS share for the same file system.

1. Choose **Services** > **File Service** > **Shares**.
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. Choose **Services** > **File Service** > **Authentication Users** > **User Mappings**.
2. Click **Set Mapping Parameter** and set **Mapping Mode** to **Preferentially support user mapping of this system.**

Step 6 Configure user mapping rules.

1. Choose **Services** > **File Service** > **Authentication Users** > **User Mappings**.
2. Click **Create** and configure user mapping rules as planned.

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 unix_group** command to create a user group that has the same GID as the local authentication user group.
3. Run the **useradd -u 100002 -g 100000 unix_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 - unix_user2** command to switch users.
5. Create the **file1** file and grant the read-only permission.

   NOTE

   The security style of the file system (**share_dir2**) on the storage system is **UNIX**. The default UNIX permission of the root directory of the file system is **755**. Therefore, first run the **change file_system general file_system_id=*?* unix_permissions=777** command on the storage system to change the UNIX permission to **777**.

   ```
   # touch file1
   # chmod 400 file1
   ```

Step 8 Use **cifs_user2** to access **file1** on a Windows client and verify that it has only the read-only permission.

----End

4 Managing Basic Storage Services

This chapter describes how to manage basic storage services through DeviceManager.

4.1 Managing File Systems

This section describes how to manage and maintain created file systems.

4.1.1 Viewing File Systems

This operation enables you to view basic information about a file system.

Context

- On the file system management page, you can click to refresh file system information.
- On the file system management page, you can click or next to a parameter and enter a keyword or select a parameter value to search for the required file systems.

- On the file system management page, you can click and select the file system parameters you want to view.
- On the file system management page, you can click or next to a parameter to change the display order of file systems.

Procedure

Step 1 Choose **Services** > **File Service** > **File Systems**.

Step 2 Select a vStore from the **vStore** drop-down list in the upper left corner.

Step 3 In the function pane, view file system information about the vStore.

Table 4-1 describes the parameters.

Table 4-1 File system parameters

Parameter	Description
Name	Name of a file system. **NOTE** You can click the name of a file system to view its details and manage it.
ID	ID of a file system.
Owning vStore	Name of the vStore to which a file system belongs. **NOTE** This parameter is available only when **vStore** is set to **All vStores** in **Step 2**.
vStore ID	ID of the vStore to which a file system belongs. **NOTE** This parameter is available only when **vStore** is set to **All vStores** in **Step 2**.
Capacity	Capacity information of a file system, including the total file system capacity and the ratio of the used capacity (allocated capacity) to the total capacity. **NOTE** You can hover your mouse over **Capacity** of a file system to view its total capacity, allocated capacity, data protection capacity, and capacity alarm threshold.
Total	Capacity configured for the file system.
Allocated Capacity	Amount of user data written to the file system. **NOTE** If the file system is a clone file system, the allocated capacity does not include the data volume inherited from the parent file system.
Data Protection	Capacity used for data protection on the file system.
Available	Amount of user data that can be written to the file system.

Parameter	Description
Used	Ratio of the used capacity (allocated capacity) to the total capacity of a file system.
Health Status	Health status of a file system.
Running Status	Running status of a file system.
Created	Time when a file system was created.
WORM	WORM mode of a file system.
Data Protection	Data protection information of a file system.
Shares	Share information of a file system.
Quotas	Check whether a quota has been configured for a file system.
Quota Status	Quota status of a file system. The value can be: • Disabled: The quota statistics function is disabled for the file system. The system does not collect statistics on the quota usage of the file system. In this case, hard and soft quotas do not take effect. • Initializing: The system is scanning the space usage or file quantity in the file system. • Enabled: The quota statistics function has been enabled for the file system. The system collects statistics on the space usage or file quantity used by the file system.
Dtrees	Number of dtrees in a file system.
Owning Storage Pool	Owning storage pool of a file system.
Clone File System	Indicates whether this is a clone file system.

Parameter	Description
Security Style	It is used to set the access control style of a file system in multi-protocol mode. **NOTE** Only 6.1.5 and later versions support **Mixed** and **Native**. • Mixed Allows users of both CIFS and NFS clients to access and control file systems. The last configured permissions prevail. • Native Controls CIFS users' permissions with Windows NT ACLs and NFS users' permissions with UNIX permissions (UNIX mode bits, POSIX ACLs, and NFSv4 ACLs). Windows NT ACLs and UNIX permissions will neither affect nor synchronize with each other. – For CIFS share access, Windows NT ACLs determine whether Windows users have access permission. **NOTE** If Windows NT ACLs do not exist, UNIX mode bits determine whether Windows users have access permission. – For NFS share access, access permission of UNIX users is determined by UNIX permissions. • NTFS Controls CIFS users' permissions with Windows NT ACLs. • UNIX Controls NFS users' permissions with UNIX mode bits or NFSv4 ACLs.
NAS Lock Policy	**NAS Lock Policy** includes **Mandatory Lock** and **Advisory Lock**. • **Mandatory Lock** is recommended if clients using different protocols simultaneously access the same file or directory. • **Advisory Lock** is recommended if high read and write performance is required and clients using different protocols do not access the same file or directory simultaneously. **NOTE** – This parameter is available only when **Security Style** is set to **Native**. – Only 6.1.5 and later versions support this parameter.
Audit Log	Indicates whether this is an audit log file system.

Step 4 (Optional) Click the name of a file system to view its summary, share, quota, and protection information. If the WORM function is enabled for a file system, you can click **Advanced** to view the WORM information of the file system.

NOTE

You can select **Only show shares of the file system** or **Only show quotas of the file system** to filter the data. If you do not select these options, the system displays the data of the file system and dtrees in the file system.

----End

4.1.2 Adding a File System to a HyperCDP Schedule

This section describes how to add a file system to an existing HyperCDP schedule to create HyperCDP objects for that file system periodically.

Prerequisites

- The file system has not been added to any HyperCDP schedule.
- The storage system is running properly, and the storage pool where the file system resides has sufficient space.

Procedure

Step 1 Choose **Services** > **File Service** > **File Systems**.

Step 2 Select the vStore to which the desired file system belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Select the desired file system and choose **Protect** > **Add to HyperCDP Schedule**.

The **Add to HyperCDP Schedule** page is displayed.

NOTE

You can also click **More** on the right of the desired file system and select **Add to HyperCDP Schedule**.

Step 4 Click ▶ on the right of **Selected File Systems**. In the **Available File Systems** area, select the desired file system to add it to the **Selected File Systems** area.

Step 5 Select a HyperCDP schedule.

NOTE

If no HyperCDP schedule exists, click **Create**.

Step 6 Click **OK**.

----End

4.1.3 Modifying a File System

This operation enables you to modify the name and description of a file system.

Procedure

Step 1 Choose **Services** > **File Service** > **File Systems**.

Step 2 Select the vStore to which the desired file system belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Click **More** on the right of the desired file system and select **Modify**.

The **Modify File System** page is displayed on the right.

NOTE

You can also click the name of the desired file system. In the upper right corner of the page that is displayed, click **Modify** from the **Operation** drop-down list.

Step 4 Modify the attributes of the file system.

Table 4-2 describes the parameters.

Table 4-2 File system parameters

Parameter	Description
Name	Name of the file system. [Value range] • The name must be unique. • The name can contain only letters, digits, periods (.), underscores (_), hyphens (-), and characters of different languages. • The name contains 1 to 255 characters.
Description	Description of the file system. [Value range] The description can be left blank or contain up to 255 characters.
Capacity Alarm Threshold (%)	Alarm threshold of the file system capacity. An alarm will be generated when the threshold is reached. **NOTE** • **Capacity Alarm Threshold (%)** is a hidden parameter. To display hidden parameters, select **Advanced**. • Capacity threshold = File system capacity x (1 - Reserved snapshot space ratio (%)) x Capacity alarm threshold (%) • The alarm is cleared only when the used capacity of the file system is smaller than Max {90% of the threshold capacity, threshold capacity - 1 GB}.

Parameter	Description
Reserved Snapshot Space Ratio (%)	Percentage of the file system snapshot space to the file system capacity. **NOTE** • When you modify the reserved snapshot space ratio, make sure the reserved space after modification do not exceed the remaining space of the file system. • The file system space must not occupy the space reserved for snapshots. For example, if the capacity of a file system is 100 GB and the reserved snapshot space ratio is 20%, the used capacity of the file system cannot exceed 80 GB. • Snapshots can be created when the file system space is full but the space reserved for snapshots is not full. • Only 6.1.5 and later versions support this parameter.
Delete Obsolete Read-Only Snapshot	Indicates whether to delete obsolete read-only snapshots. If used space of the file system reaches the capacity alarm threshold and used space of snapshots is larger than space reserved for snapshots (source file system capacity x reserved snapshot space ratio), the system automatically deletes the oldest non-secure read-only snapshots. **NOTE** • **Delete Obsolete Read-Only Snapshot** is a hidden parameter. To display hidden parameters, select **Advanced**. • If both **Delete Obsolete Read-Only Snapshot** and **Capacity Auto-negotiation Policy** are enabled, the capacity auto-negotiation policy is executed first. • Only 6.1.5 and later versions support this parameter.

Parameter	Description
Capacity Auto-negotiation Policy	The available capacity autonegotiation policies are as follows: ● **Not used**: The storage capacity used by a file system is fixed and is not flexibly adjusted by the storage system. ● **Auto expansion**: The file system capacity is automatically increased to meet user needs for more data writes, when the available space of a file system is about to run out and the storage pool has available space. ● **Auto expansion/reduction**: The storage system automatically adjusts the file system capacity based on file system space usage. When the available space of a file system is about to run out and the storage pool has available space, automatic capacity expansion will be used to increase file system capacity. When the file system's storage space is released, it can be reclaimed into a storage pool and used by other file systems in data write requests. **NOTE** ● **Capacity Auto-negotiation Policy** is a hidden parameter. To display hidden parameters, select **Advanced**. ● If both **Delete Obsolete Read-Only Snapshot** and **Capacity Auto-negotiation Policy** are enabled, the capacity auto-negotiation policy is executed first. ● Only 6.1.5 and later versions support this parameter.
Auto Expansion Trigger Threshold (%)	When the ratio of the used capacity to the total capacity of a file system is greater than this threshold, the storage system automatically triggers file system capacity expansion. **NOTE** ● This parameter is displayed only when **Capacity Auto-negotiation Policy** is set to **Auto expansion** or **Auto expansion/reduction**. ● The value of **Auto Expansion Trigger Threshold (%)** must be greater than that of **Auto Reduction Trigger Threshold (%)**. ● Only 6.1.5 and later versions support this parameter.
Auto Reduction Trigger Threshold (%)	When the ratio of the used capacity to the total capacity of a file system is smaller than this threshold, the storage system automatically triggers space reclamation to reduce the file system capacity. **NOTE** ● This parameter is displayed only when **Capacity Auto-negotiation Policy** is set to **Auto expansion/reduction**. ● Only 6.1.5 and later versions support this parameter.

Parameter	Description
Auto Expansion Upper Limit	Upper limit of automatic capacity expansion. **NOTE** • This parameter is displayed only when **Capacity Auto-negotiation Policy** is set to **Auto expansion** or **Auto expansion/reduction**. • Only 6.1.5 and later versions support this parameter.
Auto Reduction Lower Limit	Lower limit of automatic capacity reduction. **NOTE** • This parameter is displayed only when **Capacity Auto-negotiation Policy** is set to **Auto expansion/reduction**. • Only 6.1.5 and later versions support this parameter.
Snapshot Directory Visibility	Indicates whether to visualize the directory of the file system snapshots.
Auto Atime Update	Indicates whether to enable **Auto Atime Update**. Atime indicates the last file system access time. After this function is enabled, Atime is updated every time data in the file system is accessed. **NOTE** Enabling **Auto Atime Update** compromises the system performance.
Quota	Determine whether to enable the quota function of a file system based on service requirements. When the **Quota** function is disabled, the system does not collect statistics on quota usage. In this case, hard and soft quotas do not take effect.
VAAI	Indicates whether to enable VAAI. VMware Storage APIs for Array Integration (VAAI) are a set of APIs that allow ESXi hosts to offload specific file operations to the storage array. This enables vSphere to quickly implement key operations and reduces the usage of the host CPU, memory, and storage bandwidth for higher efficiency and lower O&M costs. • Enabled: The host offloads file operations to the storage array. Once it is enabled, it cannot be disabled. • Disabled: VAAI is not used. **NOTE** – Only 6.1.5 and later versions support this parameter.

Parameter	Description
Security Style	Select a security style based on service requirements. It is used to set the access control style of a file system in multi-protocol mode. • **Mixed** Allows users of both CIFS and NFS clients to access and control file systems. The last configured permissions prevail. **NOTE** – If **Mixed** is selected, you are advised to enable user mapping and set **Mapping Mode** to **Support only user mapping of this system** in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameter**. – You are advised to configure a default UNIX user for the CIFS service in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameters**. The UNIX user must be an existing local authentication user, NIS domain user, or LDAP domain user. – You are advised to configure a default Windows user for the NFS service in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameters**. The Windows user must be an existing local authentication user or AD domain user. – Only 6.1.5 and later versions support the **Mixed** security style. • Native Controls CIFS users' permissions with Windows NT ACLs and NFS users' permissions with UNIX permissions (UNIX mode bits, POSIX ACLs, and NFSv4 ACLs). Windows NT ACLs and UNIX permissions will neither affect nor synchronize with each other. – For CIFS share access, Windows NT ACLs determine whether Windows users have access permission. **NOTE** If Windows NT ACLs do not exist, UNIX mode bits determine whether Windows users have access permission. – For NFS share access, access permission of UNIX users is determined by UNIX permissions.

Parameter	Description
	NOTE – If **Native** is selected, you are advised to enable user mapping and set **Mapping Mode** to **Support only user mapping of this system** in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameter**. – You are advised to configure a default UNIX user for the CIFS service in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameters**. The UNIX user must be an existing local authentication user, NIS domain user, or LDAP domain user. – You are advised to configure a default Windows user for the NFS service in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameters**. The Windows user must be an existing local authentication user or AD domain user. – Only 6.1.5 and later versions support the **Native** security style. • **NTFS** Controls CIFS users' permissions with Windows NT ACLs. **NOTE** – If **NTFS** is selected, you are advised to enable user mapping and set **Mapping Mode** to **Support only user mapping of this system** in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameter**. – In addition, you are advised to configure a default Windows user for the NFS service in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameter**. The default Windows user must be an existing local authentication user or AD domain user. • **UNIX** Controls NFS users' permissions with UNIX mode bits or NFSv4 ACLs. **NOTE** – If **UNIX** is selected, you are advised to enable user mapping and set **Mapping Mode** to **Support only user mapping of this system** in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameter**. – In addition, you are advised to configure a default UNIX user for the CIFS service in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameter**. The UNIX user must be an existing local authentication user, NIS domain user, or LDAP domain user.

Parameter	Description
NAS Lock Policy	**NAS Lock Policy** includes **Mandatory Lock** and **Advisory Lock**. • **Mandatory Lock** is recommended if clients using different protocols simultaneously access the same file or directory. • **Advisory Lock** is recommended if high read and write performance is required and clients using different protocols do not access the same file or directory simultaneously. **NOTE** – This parameter is available only when **Security Style** is set to **Native**. – Only 6.1.5 and later versions support this parameter.
Data Reduction	Indicates whether to enable data reduction. After this function is enabled, the system performs deduplication and compression on the file system to save storage space. **NOTE** The data reduction switch can be modified only after a SmartDedupe & SmartCompression license is imported to the system.

Step 5 Set the audit log items of the file system. The system records audit logs of operations on the file system. The audit log items include **Create**, **Delete**, **Read**, **Write**, **Open**, **Close**, **Rename**, **List folders**, **Obtain properties**, **Set properties**, **Obtain security properties**, **Set security properties**, **Obtain extension properties**, and **Set extension properties**.

NOTE

- To ensure that the selected audit log items take effect, choose **Settings** > **File Service** > **Audit Log** to enable the audit log function.
- If too many audit logs are generated and the audit log collection speed is lower than the audit log writing speed, the temporary buffer space may be insufficient, causing service interruption risks. You are advised to properly configure the items to be audited. For example, configure only **Create**, **Delete**, and **Write** for a file system.

Step 6 Set the WORM properties of the file system. The WORM file system ensures that a file enters the protected state after being written. In this case, the file cannot be modified, moved, or deleted, but can be read for multiple times.

NOTE

Due to the sensitivity of a WORM file system to data security, the following configuration operations on file systems are restricted:

- Only read-only snapshots can be created for the WORM file system. The snapshot file systems created for the WORM file system also have the WORM feature. The WORM file system cannot be rolled back using a snapshot.
- When configuring the remote replication function, if **Pair Creation** is set to **Manual**, ensure that the WORM file system modes at both ends are the same. Otherwise, the primary/secondary relationship cannot be established.
- When configuring remote replication, if **Pair Creation** is set to **Automatic**, ensure that the global WORM regulatory clock has been initialized on the remote end.

Table 4-3 describes the parameters.

NOTE

This parameter is available only when WORM is enabled for the file system.

Table 4-3 WORM properties of a file system

Parameter	Description
Mode	Indicates the compliance mode of WORM protection. The **Mode** is **Regulatory compliance**: • Files within the protection period cannot be modified, renamed, or deleted by common users or system administrators. • Files whose protection period expires can be deleted but cannot be modified or renamed by common users or system administrators. • A file system that contains files within the protection period cannot be deleted by system administrators. • A file system that contains files whose protection period expires can be deleted by system administrators.
Min. Protection Period	Minimum protection period supported by the WORM file system. The protection period of a file in the WORM file system cannot be smaller than the value of this parameter. [Value range] 0 to 70 years or **Indefinite**. **NOTE** The value of **Min. Protection Period** must be less than or equal to that of **Max. Protection Period**.
Max. Protection Period	Maximum protection period supported by the WORM file system. The protection period of a file in the WORM file system cannot be longer than the value of this parameter. [Value range] 1 day to 70 years or **Indefinite**. **NOTE** The value of **Max. Protection Period** cannot be 0.

Parameter	Description
Default Protection Period	Default protection period supported by the WORM file system. The protection period of a file in the WORM file system is the default value of the parameter if you do not set a protection period for the file. [Value range] • If the value of **Max. Protection Period** ranges from 1 day to 70 years, **Default Protection Period** is a value from **Min. Protection Period** to **Max. Protection Period**. • If **Max. Protection Period** is set to **Indefinite**, **Default Protection Period** is a value from **Min. Protection Period** to 70 years or is **Indefinite**. **NOTE** To set **Default Protection Period** to **Indefinite**, you must set **Max. Protection Period** to **Indefinite**. Otherwise, the setting fails.
Automatic Lockout	After this function is enabled, a file automatically enters the locked state if not being modified within **Lockout Wait Time** (hours). The file in the locked state is protected. You can only read the file, but cannot modify, rename, or delete it. **NOTE** Modification operations include file data change and metadata change.
Lockout Wait Time	Indicates the wait time before a file automatically enters the locked state. [Value range] 1 minute to 10 years.
Automatic Deletion	After this function is enabled, the system automatically deletes files whose protection periods have expired. **NOTE** Before enabling this function, ensure that files do not need protection and can be automatically deleted by the system after they expire.
WORM Audit Log File System	After the WORM audit log file system is enabled, the system records operation logs of the WORM file system, including **Add a litigation** and **Remove a litigation**.

Step 7 Click **OK**.

Confirm your operation as prompted.

----End

4.1.4 Creating a File System Using a Template

This operation enables you to create a file system based on the parameters of a selected file system. The storage system presets the parameters of the newly

created file system based on the parameters of the selected file system. You can also modify the parameters.

Context

When a template is used to create a file system, the file system copies the attributes except the name of the template. The file system does not copy the share, quota, and data protection configurations of the template.

Procedure

Step 1 Choose **Services** > **File Service** > **File Systems**.

Step 2 Select the vStore to which the file system to be used as the template belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Select the desired file system and click **Create From**.

The **Create File System from Template** page is displayed on the right.

NOTE

Alternatively, perform either of the following operations to go to the **Create File System from Template** page:

- Click **More** on the right of the desired file system and select **Create From**.
- Click the name of the desired file system. In the upper right corner of the page that is displayed, click **Create From** from the **Operation** drop-down list.

Step 4 Modify the preset file system parameters as required.

Table 4-4 describes the parameters.

Table 4-4 File system parameters

Parameter	Description
Name	Name of the file system. [Value range] • The name must be unique. • The name can contain only letters, digits, underscores (_), hyphens (-), and periods (.). • The name contains 1 to 255 characters.
Description	Description of the file system. [Value range] The description can be left blank or contain up to 255 characters.
Owning Storage Pool	Owning storage pool of the file system.

Parameter	Description
Security Style	Select a security style based on service requirements. It is used to set the access control style of a file system in multi-protocol mode. • Mixed Allows users of both CIFS and NFS clients to access and control file systems. The last configured permissions prevail. **NOTE** – If **Mixed** is selected, you are advised to enable user mapping and set **Mapping Mode** to **Support only user mapping of this system** in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameter**. – You are advised to configure a default UNIX user for the CIFS service in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameters**. The UNIX user must be an existing local authentication user, NIS domain user, or LDAP domain user. – You are advised to configure a default Windows user for the NFS service in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameters**. The Windows user must be an existing local authentication user or AD domain user. – Only 6.1.5 and later versions support the **Mixed** security style. • Native Controls CIFS users' permissions with Windows NT ACLs and NFS users' permissions with UNIX permissions (UNIX mode bits, POSIX ACLs, and NFSv4 ACLs). Windows NT ACLs and UNIX permissions will neither affect nor synchronize with each other. – For CIFS share access, Windows NT ACLs determine whether Windows users have access permission. **NOTE** If Windows NT ACLs do not exist, UNIX mode bits determine whether Windows users have access permission. – For NFS share access, access permission of UNIX users is determined by UNIX permissions.

Parameter	Description
	NOTE – If **Native** is selected, you are advised to enable user mapping and set **Mapping Mode** to **Support only user mapping of this system** in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameter**. – You are advised to configure a default UNIX user for the CIFS service in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameters**. The UNIX user must be an existing local authentication user, NIS domain user, or LDAP domain user. – You are advised to configure a default Windows user for the NFS service in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameters**. The Windows user must be an existing local authentication user or AD domain user. – Only 6.1.5 and later versions support the **Native** security style. ● NTFS Controls CIFS users' permissions with Windows NT ACLs. **NOTE** – If **NTFS** is selected, you are advised to enable user mapping and set **Mapping Mode** to **Support only user mapping of this system** in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameter**. – In addition, you are advised to configure a default Windows user for the NFS service in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameter**. The default Windows user must be an existing local authentication user or AD domain user. ● UNIX Controls NFS users' permissions with UNIX mode bits or NFSv4 ACLs. **NOTE** – If **UNIX** is selected, you are advised to enable user mapping and set **Mapping Mode** to **Support only user mapping of this system** in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameter**. – In addition, you are advised to configure a default UNIX user for the CIFS service in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameter**. The UNIX user must be an existing local authentication user, NIS domain user, or LDAP domain user.

Parameter	Description
NAS Lock Policy	**NAS Lock Policy** includes **Mandatory Lock** and **Advisory Lock**. • **Mandatory Lock** is recommended if clients using different protocols simultaneously access the same file or directory. • **Advisory Lock** is recommended if high read and write performance is required and clients using different protocols do not access the same file or directory simultaneously. **NOTE** • This parameter is available only when **Security Style** is set to **Native**. • Only 6.1.5 and later versions support this parameter.
VAAI	Indicates whether to enable VAAI. VMware Storage APIs for Array Integration (VAAI) are a set of APIs that allow ESXi hosts to offload specific file operations to the storage array. This enables vSphere to quickly implement key operations and reduces the usage of the host CPU, memory, and storage bandwidth for higher efficiency and lower O&M costs. • Enabled: The host offloads file operations to the storage array. Once it is enabled, it cannot be disabled. • Disabled: VAAI is not used. **NOTE** – Only 6.1.5 and later versions support this parameter.
Capacity	Capacity of the file system, which indicates the maximum capacity allocated to the thin file system. That is, the total capacity dynamically allocated to the thin file system cannot exceed this value. **NOTE** • The maximum capacity of the file system cannot exceed the system specifications. For details about the specifications, visit **Specifications Query**. • The storage system uses the following capacity algorithms defined by Windows: 1 PB = 1,024 TB, 1 TB = 1,024 GB, 1 GB = 1,024 MB, 1 MB = 1,024 KB, and 1 KB = 1,024 bytes.
Capacity Alarm Threshold (%)	Alarm threshold of the file system capacity. An alarm will be generated when the threshold is reached. **NOTE** • **Capacity Alarm Threshold (%)** is hidden. To display hidden parameters, select **Advanced**. • Capacity threshold = File system capacity x (1 - Reserved snapshot space ratio (%)) x Capacity alarm threshold (%) • The alarm is cleared only when the used capacity of the file system is smaller than Max {90% of the threshold capacity, threshold capacity - 1 GB}.

Parameter	Description
Reserved Snapshot Space Ratio (%)	Percentage of the file system snapshot space to the file system capacity. **NOTE** • The file system space must not occupy the space reserved for snapshots. For example, if the capacity of a file system is 100 GB and the reserved snapshot space ratio is 20%, the used capacity of the file system cannot exceed 80 GB. • Snapshots can be created when the file system space is full but the space reserved for snapshots is not full. • Only 6.1.5 and later versions support this parameter.
Delete Obsolete Read-Only Snapshot	Indicates whether to delete obsolete read-only snapshots. If used space of the file system reaches the capacity alarm threshold and used space of snapshots is larger than space reserved for snapshots (source file system capacity x reserved snapshot space ratio), the system automatically deletes the oldest non-secure read-only snapshots. **NOTE** • **Delete Obsolete Read-Only Snapshot** is a hidden parameter. To display hidden parameters, select **Advanced**. • If both **Delete Obsolete Read-Only Snapshot** and **Capacity Auto-negotiation Policy** are enabled, the capacity auto-negotiation policy is executed first. • Only 6.1.5 and later versions support this parameter.

Parameter	Description
Capacity Auto-negotiation Policy	The available capacity autonegotiation policies are as follows: • **Not used**: The storage capacity used by a file system is fixed and is not flexibly adjusted by the storage system. • **Auto expansion**: The file system capacity is automatically increased to meet user needs for more data writes, when the available space of a file system is about to run out and the storage pool has available space. • **Auto expansion/reduction**: The storage system automatically adjusts the file system capacity based on file system space usage. When the available space of a file system is about to run out and the storage pool has available space, automatic capacity expansion will be used to increase file system capacity. When the file system's storage space is released, it can be reclaimed into a storage pool and used by other file systems in data write requests. **NOTE** • **Capacity Auto-negotiation Policy** is a hidden parameter. To display hidden parameters, select **Advanced**. • If both **Delete Obsolete Read-Only Snapshot** and **Capacity Auto-negotiation Policy** are enabled, the capacity auto-negotiation policy is executed first. • Only 6.1.5 and later versions support this parameter.
Auto Expansion Trigger Threshold (%)	When the ratio of the used capacity to the total capacity of a file system is greater than this threshold, the storage system automatically triggers file system capacity expansion. **NOTE** • This parameter is displayed only when **Capacity Auto-negotiation Policy** is set to **Auto expansion** or **Auto expansion/reduction**. • The value of **Auto Expansion Trigger Threshold (%)** must be greater than that of **Auto Reduction Trigger Threshold (%)**. • Only 6.1.5 and later versions support this parameter.
Auto Reduction Trigger Threshold (%)	When the ratio of the used capacity to the total capacity of a file system is smaller than this threshold, the storage system automatically triggers space reclamation to reduce the file system capacity. **NOTE** • This parameter is displayed only when **Capacity Auto-negotiation Policy** is set to **Auto expansion/reduction**. • Only 6.1.5 and later versions support this parameter.

Parameter	Description
Auto Expansion Upper Limit	Upper limit of automatic capacity expansion. **NOTE** • This parameter is displayed only when **Capacity Auto-negotiation Policy** is set to **Auto expansion** or **Auto expansion/reduction**. • Only 6.1.5 and later versions support this parameter.
Auto Reduction Lower Limit	Lower limit of automatic capacity reduction. **NOTE** • This parameter is displayed only when **Capacity Auto-negotiation Policy** is set to **Auto expansion/reduction**. • Only 6.1.5 and later versions support this parameter.
Application Type	Application type of the file system. Preset application types are provided for typical applications. In file service scenarios, possible options are **NAS_Default**, **NAS_Virtual_Machine**, **NAS_Database**, **NAS_Large_File**, **Office_Automation**, and **NAS_EDA**. **NOTE** • The **Application Request Size** and **File System Distribution Algorithm** parameters are set for preset application types. The value of **Application Request Size** is **16 KB** for **NAS_Default**, **NAS_Virtual_Machine**, **Office_Automation**, and **NAS_EDA**, **8 KB** for **NAS_Database**, and **32 KB** for **NAS_Large_File**. If **Application Type** is set to **NAS_Default**, **NAS_Large_File**, **Office_Automation**, or **NAS_EDA**, **File System Distribution Algorithm** is **Directory balance mode**. In this mode, directories are evenly allocated to each controller by quantity. If **Application Type** is set to **NAS_Virtual_Machine** or **NAS_Database**, **File System Distribution Algorithm** is **Performance mode**. In this mode, directories are preferentially allocated to the controller to which the shared IP address belongs, improving access performance of directories and files. • **Application Type** cannot be changed once being configured. You are advised to set the value based on the service I/O model. • To create an application type, run the **create workload_type general name=? io_size=?** command. For details, see the *Command Reference* of the desired model and version. • You can also run the **create file_system general** or **change file_system general** command to create or modify a file system respectively. For details, see the *Command Reference* of the desired model and version.

NOTE

Description and **Capacity Alarm Threshold(%)** are hidden by default. To display hidden parameters, click **Advanced**.

Step 5 Configure data protection for the file system.

1. Enable **Add to HyperCDP Schedule**.

2. Select a HyperCDP schedule to create a HyperCDP object for the file system.

NOTE

- HyperCDP is a high-density snapshot technology that provides continuous data protection for file systems. For details about the HyperCDP feature, see *HyperCDP Feature Guide for File* of the desired version.
- The system has a built-in HyperCDP schedule **NAS_DEFAULT_BUILDIN**. The schedule is executed once an hour (retains the latest three copies), once at 00:05 every day (retains the latest two copies), and once at 00:10 every Sunday (retains the latest two copies).
- When you create a file system, the system selects the built-in HyperCDP schedule **NAS_DEFAULT_BUILDIN** by default.
- A file system can be added to only one HyperCDP schedule. For a file system that has been added to a HyperCDP schedule, if you want to change its owning HyperCDP schedule, you need to remove the file system from the original HyperCDP schedule first.
- If a file system has not been added to a HyperCDP schedule during the file system creation, you can add it to a HyperCDP schedule after the file system is created.

Step 6 Click **Advanced** in the upper right corner and set the audit log items of the file system. The system records audit logs of operations on the file system. The audit log items include **Create**, **Delete**, **Read**, **Write**, **Open**, **Close**, **Rename**, **List folders**, **Obtain properties**, **Set properties**, **Obtain security properties**, **Set security properties**, **Obtain extension properties**, and **Set extension properties**.

NOTE

- To ensure that the selected audit log items take effect, choose **Settings** > **File Service** > **Audit Log** to enable the audit log function.
- If too many audit logs are generated and the audit log collection speed is lower than the audit log writing speed, the temporary buffer space may be insufficient, causing service interruption risks. You are advised to properly configure the items to be audited. For example, configure only **Create**, **Delete**, and **Write** for a file system.

Step 7 Set advanced attributes of the file system.

Table 4-5 describes the parameters.

Table 4-5 Advanced file system parameters

Parameter	Description
Snapshot Directory Visibility	Indicates whether to visualize the directory of the file system snapshots.
Auto Atime Update	Indicates whether to enable **Auto Atime Update**. Atime indicates the last file system access time. After this function is enabled, Atime is updated every time data in the file system is accessed. **NOTE** Enabling **Auto Atime Update** compromises the system performance.

Step 8 Set the WORM properties of the file system. The WORM file system ensures that a file enters the protected state after being written. In this case, the file cannot be modified, moved, or deleted, but can be read for multiple times.

NOTE

Due to the sensitivity of a WORM file system to data security, the following configuration operations on file systems are restricted:

- Only read-only snapshots can be created for the WORM file system. The snapshot file systems created for the WORM file system also have the WORM feature. The WORM file system cannot be rolled back using a snapshot.
- When configuring the remote replication function, if **Pair Creation** is set to **Manual**, ensure that the WORM file system modes at both ends are the same. Otherwise, the primary/secondary relationship cannot be established.
- When configuring remote replication, if **Pair Creation** is set to **Automatic**, ensure that the global WORM regulatory clock has been initialized on the remote end.

Table 4-6 describes the parameters.

NOTE

The WORM properties are hidden. To display hidden parameters, click **Advanced**.

Table 4-6 WORM properties of a file system

Parameter	Description
Mode	Indicates the compliance mode of WORM protection. The **Mode** is **Regulatory compliance**: • Files within the protection period cannot be modified, renamed, or deleted by common users or system administrators. • Files whose protection period expires can be deleted but cannot be modified or renamed by common users or system administrators. • A file system that contains files within the protection period cannot be deleted by system administrators. • A file system that contains files whose protection period expires can be deleted by system administrators. [Value range] Regulatory compliance
Min. Protection Period	Minimum protection period supported by the WORM file system. The protection period of a file in the WORM file system cannot be smaller than the value of this parameter. [Value range] 0 to 70 years or **Indefinite**. **NOTE** The value of **Min. Protection Period** must be less than or equal to that of **Max. Protection Period**.

Parameter	Description
Max. Protection Period	Maximum protection period supported by the WORM file system. The protection period of a file in the WORM file system cannot be longer than the value of this parameter. [Value range] 1 day to 70 years or **Indefinite**. **NOTE** The value of **Max. Protection Period** cannot be 0.
Default Protection Period	Default protection period supported by the WORM file system. The protection period of a file in the WORM file system is the default value of the parameter if you do not set a protection period for the file. [Value range] ● If the value of **Max. Protection Period** ranges from 1 day to 70 years, **Default Protection Period** is a value from **Min. Protection Period** to **Max. Protection Period**. ● If **Max. Protection Period** is set to **Indefinite**, **Default Protection Period** is a value from **Min. Protection Period** to 70 years or is **Indefinite**. **NOTE** To set **Default Protection Period** to **Indefinite**, you must set **Max. Protection Period** to **Indefinite**. Otherwise, the setting fails.
Automatic Lockout	After this function is enabled, a file automatically enters the locked state if not being modified within **Lockout Wait Time** (hours). The file in the locked state is protected. You can only read the file, but cannot modify, rename, or delete it. **NOTE** Modification operations include file data change and metadata change.
Lockout Wait Time	Indicates the wait time before a file automatically enters the locked state. [Value range] 1 minute to 10 years.
Automatic Deletion	After this function is enabled, the system automatically deletes files whose protection periods have expired. **NOTE** Before enabling this function, ensure that files do not need protection and can be automatically deleted by the system after they expire.
WORM Audit Log File System	After the WORM audit log file system is enabled, the system records operation logs of the WORM file system, including **Add a litigation** and **Remove a litigation**.

Parameter	Description
Global WORM Regulatory Clock	Before creating a WORM file system for the first time, you need to initialize the WORM regulatory clock. After this parameter is enabled, the global security regulatory clock is initialized to the current system time and time zone. The WORM regulatory clock prevents modification to file protection periods caused by system time tampering attacks. The WORM regulatory clock includes a global WORM regulatory clock and a file system WORM regulatory clock. To initialize the WORM regulatory clock, you only need to initialize the global WORM regulatory clock. The file system WORM regulatory clock will be automatically initialized using the global WORM regulatory clock when a WORM file system is created. **NOTICE** • The global WORM regulatory clock cannot be modified after being initialized. Before the setting, ensure that the system time and time zone are correct. • Only super administrators can initialize the global WORM regulatory clock.

Step 9 Click **OK**.

Confirm your operation as prompted.

----End

4.1.5 Modifying the Capacity of a File System

This operation enables you to modify the capacity of a file system to meet service requirements.

Procedure

Step 1 Choose **Services** > **File Service** > **File Systems**.

Step 2 Select the vStore to which the desired file system belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Click **More** on the right of the desired file system and select **Modify Capacity**.

The **Modify File System Capacity** page is displayed on the right.

NOTE

You can also click the name of the desired file system. In the upper right corner of the page that is displayed, click **Modify Capacity** from the **Operation** drop-down list.

Step 4 Set the file system capacity.

1. In **Capacity**, set the file system capacity.

NOTE

The file system capacity cannot exceed the system specifications.

2. Select a capacity unit from the right drop-down list.
   Possible options are **Blocks**, **MB**, **GB**, **TB**, and **PB**.

Step 5 Determine whether to change the capacity of a remote file system.

NOTE

- Changing the capacity of a remote file system is supported only when the local file system is configured with remote replication.
- If you do not select a remote file system, only the capacity of the local file system will be changed. To ensure availability of the remote replication pair, change the capacity of the local file system manually.
- Remote file systems with abnormal remote devices or invalid remote replication pairs cannot be selected.

Step 6 Click **OK**.

----End

4.1.6 Deleting a File System

This operation enables you to delete an unneeded file system to release storage space.

Prerequisites

Services on the desired file system have been stopped, and the file system has not been shared or configured with any value-added services.

Procedure

Step 1 Choose **Services** > **File Service** > **File Systems**.

Step 2 Select the vStore to which the desired file systems belong from the **vStore** drop-down list in the upper left corner.

Step 3 Select one or more desired file systems and click **Delete**.

NOTE

Alternatively, perform either of the following operations to delete a file system:

- Click **More** on the right of a desired file system and select **Delete**.
- Click the name of the desired file system. In the upper right corner of the page that is displayed, click **Delete** from the **Operation** drop-down list.

Step 4 Confirm your operation as prompted.

----End

4.2 Managing Dtrees

This section describes how to manage and maintain created dtrees.

4.2.1 Viewing Dtrees

This operation enables you to view details of dtrees.

Context

- On the dtree management page, you can click to refresh dtree information.
- On the dtree management page, you can click next to a parameter and enter a keyword to search for the required dtrees.
- On the dtree management page, you can click to select the dtree parameters you want to view.
- On the dtree management page, you can click or next to a parameter to change the display order of dtrees.

Prerequisites

You have created a file system and a dtree.

Procedure

Step 1 Choose **Services** > **File Service** > **Dtrees**.

Step 2 Select a vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Select a file system and view information about its dtrees in the function pane. Table 4-7 describes the parameters.

Table 4-7 Dtree parameters

Parameter	Description
Name	Dtree name.
ID	Dtree ID.

Parameter	Description
Security Style	It is used to set the access control style of a dtree in multi-protocol mode. **NOTE** Only 6.1.5 and later versions support **Mixed** and **Native**. ● Mixed Allows users of both CIFS and NFS clients to access and control dtrees. The last configured permissions prevail. ● Native Controls CIFS users' permissions with Windows NT ACLs and NFS users' permissions with UNIX permissions (UNIX mode bits, POSIX ACLs, and NFSv4 ACLs). Windows NT ACLs and UNIX permissions will neither affect nor synchronize with each other. – For CIFS share access, Windows NT ACLs determine whether Windows users have access permission. **NOTE** If Windows NT ACLs do not exist, UNIX mode bits determine whether Windows users have access permission. – For NFS share access, access permission of UNIX users is determined by UNIX permissions. ● NTFS Controls CIFS users' permissions with Windows NT ACLs. ● UNIX Controls NFS users' permissions with UNIX mode bits or NFSv4 ACLs.
NAS Lock Policy	**NAS Lock Policy** includes **Mandatory Lock** and **Advisory Lock**. ● **Mandatory Lock** is recommended if clients using different protocols simultaneously access the same file or directory. ● **Advisory Lock** is recommended if high read and write performance is required and clients using different protocols do not access the same file or directory simultaneously. **NOTE** ● This parameter is available only when **Security Style** is set to **Native**. ● Only 6.1.5 and later versions support this parameter.
Shares	Share information of a dtree.
Quotas	Check whether a quota has been configured for a dtree.

Parameter	Description
Quota Status	Quota status of a dtree. The value can be: • Disabled: The quota statistics function is not enabled for the dtree. The system does not collect statistics on the dtree quota usage. In this case, hard and soft quotas do not take effect. • Initializing: The system is scanning the space usage or file quantity of the dtree. • Enabled: The quota statistics function has been enabled for the dtree. The system collects statistics on the space usage or file quantity used by the dtree.

Step 4 (Optional) Click the name of a dtree to view its summary, share, and quota information.

----End

4.2.2 Modifying a Dtree

This operation enables you to modify attributes of a dtree.

Prerequisites

You have created a file system and a dtree.

Procedure

Step 1 Choose **Services** > **File Service** > **Dtrees**.

Step 2 Select the vStore to which the desired file system belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Select the desired file system, click **More** on the right of the desired dtree, and select **Modify**.

The **Modify Dtree** page is displayed on the right.

NOTE

You can also click the name of the desired dtree. In the upper right corner of the page that is displayed, click **Operation** and select **Modify**.

Step 4 Modify dtree attributes.

Table 4-8 describes the parameters.

Table 4-8 Dtree parameters

Parameter	Description
Name	Name of the dtree. [Value range] ● The name must be unique. ● The name can contain only letters, digits, characters of different languages, and special characters (!\"#&%$'()*+-.;<=>?@[]^_`{|}~ and spaces). ● The name contains 1 to 255 characters. ● The name cannot only contain one or two consecutive periods (**.** or **..**).
Quota	Determine whether to enable the quota function of a dtree based on service requirements. When the **Quota** function is disabled, the system does not collect statistics on quota usage. In this case, hard and soft quotas do not take effect.

Parameter	Description
Security Style	Select a security style based on service requirements. It is used to set the access control style of a dtree in multi-protocol mode. ● Mixed Allows users of both CIFS and NFS clients to access and control dtrees. The last configured permissions prevail. **NOTE** – If **Mixed** is selected, you are advised to enable user mapping and set **Mapping Mode** to **Support only user mapping of this system** in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameter**. – You are advised to configure a default UNIX user for the CIFS service in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameters**. The UNIX user must be an existing local authentication user, NIS domain user, or LDAP domain user. – You are advised to configure a default Windows user for the NFS service in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameters**. The Windows user must be an existing local authentication user or AD domain user. – Only 6.1.5 and later versions support the **Mixed** security style. ● Native Controls CIFS users' permissions with Windows NT ACLs and NFS users' permissions with UNIX permissions (UNIX mode bits, POSIX ACLs, and NFSv4 ACLs). Windows NT ACLs and UNIX permissions will neither affect nor synchronize with each other. – For CIFS share access, Windows NT ACLs determine whether Windows users have access permission. **NOTE** If Windows NT ACLs do not exist, UNIX mode bits determine whether Windows users have access permission. – For NFS share access, access permission of UNIX users is determined by UNIX permissions.

Parameter	Description
	NOTE – If **Native** is selected, you are advised to enable user mapping and set **Mapping Mode** to **Support only user mapping of this system** in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameter**. – You are advised to configure a default UNIX user for the CIFS service in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameters**. The UNIX user must be an existing local authentication user, NIS domain user, or LDAP domain user. – You are advised to configure a default Windows user for the NFS service in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameters**. The Windows user must be an existing local authentication user or AD domain user. – Only 6.1.5 and later versions support the **Native** security style. ● NTFS Controls CIFS users' permissions with Windows NT ACLs. **NOTE** – If **NTFS** is selected, you are advised to enable user mapping and set **Mapping Mode** to **Support only user mapping of this system** in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameter**. – In addition, you are advised to configure a default Windows user for the NFS service in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameter**. The default Windows user must be an existing local authentication user or AD domain user. ● UNIX Controls NFS users' permissions with UNIX mode bits or NFSv4 ACLs. **NOTE** – If **UNIX** is selected, you are advised to enable user mapping and set **Mapping Mode** to **Support only user mapping of this system** in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameter**. – In addition, you are advised to configure a default UNIX user for the CIFS service in **Services** > **File Service** > **Authentication Users** > **User Mappings** > **Set Mapping Parameter**. The UNIX user must be an existing local authentication user, NIS domain user, or LDAP domain user.

Parameter	Description
NAS Lock Policy	**NAS Lock Policy** includes **Mandatory Lock** and **Advisory Lock**. • **Mandatory Lock** is recommended if clients using different protocols simultaneously access the same file or directory. • **Advisory Lock** is recommended if high read and write performance is required and clients using different protocols do not access the same file or directory simultaneously. **NOTE** • This parameter is available only when **Security Style** is set to **Native**. • Only 6.1.5 and later versions support this parameter.

Step 5 Click **OK**.

----End

4.2.3 Deleting a Dtree

This operation enables you to delete an unnecessary dtree.

Prerequisites

You have created a file system and a dtree.

Procedure

Step 1 Choose **Services** > **File Service** > **Dtrees**.

Step 2 Select the vStore to which the desired file system belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Select the desired file system, select one or more desired dtrees of the file system, and click **Delete**.

NOTE

Alternatively, perform either of the following operations to delete a dtree:

- Click **More** on the right of a desired dtree and select **Delete**.
- Click the name of a desired dtree. In the upper right corner of the page that is displayed, click **Operation** and select **Delete**.

Step 4 Confirm your operation as prompted.

----End

4.3 Managing Quotas

This section describes how to manage and maintain created quotas.

4.3.1 Viewing Quotas

This operation enables you to view details of a quota.

Context

- On the quota management page, you can click to refresh quota information.
- On the quota management page, you can click to select the quota parameters you want to view.

Prerequisites

You have created a quota for a file system.

Procedure

Step 1 Choose **Services** > **File Service** > **Quotas** > **Custom Quotas**.

Step 2 Select a vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Select a file system and view its quota information in the function pane. **Table 4-9** describes the parameters.

Table 4-9 Quota parameters

Parameter	Description
Dtree	Dtree controled by a quota. **NOTE** This parameter is valid only when **Quota Type** is **Directory quota** for a file system or a quota is created for a dtree.
ID	Quota ID.
Quota Type	Quota type.
User	Name of the user for which a quota takes effect. **NOTE** This parameter is valid only when **Quota Type** is **User quota** for a specified user.
User Group	Name of the user group for which a quota takes effect. **NOTE** This parameter is valid only when **Quota Type** is **User quota** or **User group quota** for a specified user group.
User/User Group Type	Type of the user or user group for which a quota takes effect. The value can be **Local** or **Domain**. **NOTE** This parameter is valid only when **Quota Type** is **User quota** for a specified user or user group, or **User group quota** for a specified user group.

Parameter	Description
Space Soft/Hard Quota	Space soft quota and space hard quota: • If the used file space reaches the space soft quota, the system generates an alarm but still allows writes. After the hard quota is reached, the system immediately forbids writes. • If the used file space reaches the space hard quota, the system immediately forbids writes.
File Quantity Soft/ Hard Quota	File quantity soft quota and file quantity hard quota: • If the number of files reaches the file quantity soft quota, the system generates an alarm but new files can still be added. After the hard quota is reached, new files cannot be added. • If the number of files reaches the file quantity hard quota, new files cannot be added. However, operations on existing files are not affected.

----End

4.3.2 Modifying a Quota

This operation enables you to modify the attributes of a quota.

Prerequisites

You have created a quota for a file system.

Procedure

Step 1 Choose **Services** > **File Service** > **Quotas** > **Custom Quotas**.

Step 2 Select the vStore to which the desired file system belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Select the desired file system, click **More** on the right of the desired quota, and select **Modify**.

The **Modify Quota** page is displayed on the right.

Step 4 Modify space quotas.

Table 4-10 describes the parameters.

Table 4-10 Space quota parameters

Parameter	Description
Hard Quota	Space hard quota. If the quota is reached, the system immediately forbids writes. [Value range] 1 KB to 256 PB The value must be larger than that of **Soft Quota**.
Soft Quota	Space soft quota. If the quota is reached, the system generates an alarm but still allows writes. After the hard quota is reached, the system immediately forbids writes. [Value range] 1 KB to 256 PB The value must be smaller than that of **Hard Quota**.

Step 5 Modify file quantity quotas.

Table 4-11 describes the parameters.

Table 4-11 File quantity quota parameters

Parameter	Description
Hard Quota	File quantity hard quota. If the quota is reached, new files cannot be added. However, operations on existing files are not affected. [Value range] 1 to 2 billion The value must be larger than that of **Soft Quota**.
Soft Quota	File quantity soft quota. If the quota is reached, the system generates an alarm but new files can still be added. After the hard quota is reached, new files cannot be added. [Value range] 1 to 2 billion The value must be smaller than that of **Hard Quota**.

Step 6 Click **OK**.

----End

4.3.3 Deleting a Quota

This operation enables you to delete unnecessary quotas.

Prerequisites

You have created a quota for a file system.

Procedure

Step 1 Choose **Services** > **File Service** > **Quotas** > **Custom Quotas**.

Step 2 Select the vStore to which the desired file system belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Select the desired file system, select one or more desired quotas, and click **Delete**.

NOTE

You can also click **More** on the right of a desired quota and select **Delete**.

Step 4 Confirm your operation as prompted.

----End

4.4 Managing the Service Network

This section describes how to manage the service network of the storage system.

4.4.1 Managing Ethernet Ports

This section describes how to manage Ethernet ports.

4.4.1.1 Viewing Ethernet Ports

This operation enables you to view information about Ethernet ports.

Procedure

Step 1 Choose **Services** > **Network** > **Ethernet Network** > **Ethernet Ports**.

Step 2 View information about Ethernet ports in the function pane. **Table 4-12** describes the parameters.

Table 4-12 Ethernet port parameters

Parameter	Description
Name	Name of an Ethernet port.
Location	Location of an Ethernet port.
ID	ID of an Ethernet port.
Health Status	Health status of an Ethernet port. • **Unknown**: The system fails to query the port status. • **Normal**: Functions and running performance of the Ethernet port are normal and without error. • **Bit errors found**: Bit errors occur when the port transmits data. • **Faulty**: The Ethernet port is functioning improperly and cannot work normally.

Parameter	Description
Running Status	Running status of an Ethernet port. • **Unknown**: The system fails to query the port status. • **Link up**: A cable is connected to the port. • **Link down**: No cable is connected to the port. • **To be recovered**: For a 4 U device, if the owning controller of a port is faulty, the running status of the port is **To be recovered**.
MAC Address	MAC address of an Ethernet port.
IPv4 Address/ Subnet Mask	IPv4 address and subnet mask of an Ethernet port.
IPv6 Address/Prefix	IPv6 address and prefix length of an Ethernet port.
Working Rate (Gbit/s)	Data transmission rate of an Ethernet port.
Max. Working Rate (Gbit/s)	Maximum data transmission rate of an Ethernet port.
MTU (Bytes)	Maximum size of a data packet that can be transferred between an Ethernet port and an application server.
Bond Name	Bond name of an Ethernet port.
Logical Type	Logical type of an Ethernet port. Possible values are **Front-end port**, **Management port**, **Maintenance port**, **Expansion port**, **Scale-out interconnect port**, **Container front-end port**, and **Container back-end port**.
Port State	State of an Ethernet port. An Ethernet port disconnects after it is disabled.
Initiators	Number of initiators connected to an Ethernet port.

NOTE

You can click the name of an Ethernet port to view its details.

----End

4.4.1.2 Viewing Bit Error Statistics

A port's bit error statistics reflect the data transmission efficiency of this port. A high bit error rate compromises the read and write performance of the application server using this port.

Procedure

Step 1 Choose **Services** > **Network** > **Ethernet Network** > **Ethernet Ports**.

Step 2 Click **Bit Error Statistics**.

The **Bit Error Statistics** page is displayed on the right.

Step 3 Query the bit error statistics of the Ethernet ports.

NOTE

You can click **Clear** to clear bit error statistics.

----End

4.4.2 Managing Bond Ports

This section describes how to manage bond ports.

4.4.2.1 Viewing Bond Ports

This operation enables you to view information about bond ports.

Procedure

Step 1 Choose **Services** > **Network** > **Ethernet Network** > **Bond Ports**.

Step 2 View information about bond ports in the function pane. **Table 4-13** describes the parameters.

Table 4-13 Bond port parameters

Parameter	Description
Name	Name of a bond port.
ID	ID of a bond port.
Health Status	Health status of a bond port. • **Unknown**: The system fails to query the port status. • **Normal**: Functions and running performance of the port are normal and without error. • **Faulty**: The port is functioning improperly and cannot work normally. • **Partially damaged**: The bond port has a faulty member port.

Parameter	Description
Running Status	Running status of a bond port. • **Unknown**: The system fails to query the port status. • **Link up**: A cable is connected to a member port. • **Link down**: No cable is connected to a member port. • **To be recovered**: For a 4 U device, if the owning controller of a port is faulty, the running status of the port is **To be recovered**.
IPv4 Address/ Subnet Mask	IPv4 address and subnet mask of a bond port.
IPv6 Address/Prefix	IPv6 address and prefix length of a bond port.
MTU (Bytes)	Maximum size of a data packet that can be transferred between a bond port and an application server.
Ports	Number of ports bonded to a bond port.
Initiators	Number of initiators connected to a bond port.

NOTE

You can click the name of a bond port to view its details and modify it.

----End

4.4.2.2 Modifying a Bond Port

This operation enables you to modify a bond port.

Prerequisites

- A bond port has been created.
- After the MTU is changed to a non-default value, ensure that the MTU is the same as that of the peer device (switch or network adapter).

Procedure

Step 1 Choose **Services** > **Network** > **Ethernet Network** > **Bond Ports**.

Step 2 Click **More** on the right of the desired bond port and select **Modify**.

The **Modify** page is displayed.

NOTE

Alternatively, click the name of the desired port. In the upper right corner of the page that is displayed, select **Modify** from the **Operation** drop-down list.

Step 3 Set **MTU (Bytes)** of the bond port. The value ranges from 1280 to 9000.

Step 4 In **Logical Port**, specify **Name**, **IP Address**, and **Subnet Mask/Prefix** of a logical port bonded to the bond port.

NOTE

You can click + to add more ports to the bond port.

Step 5 Click **OK**.

----End

4.4.2.3 Deleting a Bond Port

This operation enables you to delete a bond port.

Prerequisites

- All services on the bond port to be deleted have been stopped.
- No VLAN or logical port is created for the bond port to be deleted.

Precautions

After a bond port is deleted, the IP addresses of the bonded Ethernet ports are cleared. You must reset IP addresses for the Ethernet ports if needed.

Procedure

Step 1 Choose **Services** > **Network** > **Ethernet Network** > **Bond Ports**.

Step 2 Select one or more desired bond ports and click **Delete**.

NOTE

You can also click **More** on the right of a desired bond port and select **Delete**.

Confirm your operation as prompted.

----End

4.4.3 Managing VLANs

This section describes how to add Ethernet ports or bond ports in the storage system to multiple independent VLANs. You can configure different services in different VLANs to ensure the security and reliability of service data.

4.4.3.1 Viewing VLANs

This operation enables you to view information about created VLANs.

Procedure

Step 1 Choose **Services** > **Network** > **Ethernet Network** > **VLANs**.

Step 2 View information about VLANs in the function pane. **Table 4-14** describes the parameters.

Table 4-14 VLAN parameters

Parameter	Description
Name	Name of a VLAN.
ID	ID of a VLAN.
Running Status	Running status of a VLAN. • **Unknown**: The system fails to query the VLAN status. • **Link up**: The running status of the home port of a VLAN is link up. • **Link down**: The running status of the home port of a VLAN is link down. • **To be recovered**: When the home port of a VLAN is in the **To be recovered** state, the running status of the VLAN is refreshed to **To be recovered**.
MTU (Bytes)	Maximum transmission unit of a VLAN.

----End

4.4.3.2 Modifying a VLAN

This operation enables you to modify a VLAN.

Procedure

Step 1 Choose **Services** > **Network** > **Ethernet Network** > **VLANs**.

Step 2 Click **More** on the right of the desired VLAN and select **Modify**.

The **Modify VLAN** page is displayed.

Step 3 Set **MTU (Bytes)**.

Step 4 Click **OK**.

----End

4.4.3.3 Deleting a VLAN

This operation enables you to delete an unnecessary VLAN.

Prerequisites

All services in the VLAN to be deleted have been stopped.

Procedure

Step 1 Choose **Services** > **Network** > **Ethernet Network** > **VLANs**.

Step 2 Select one or more desired VLANs and click **Delete**.

NOTE

You can also click **More** on the right of a desired VLAN and select **Delete**.

Confirm your operation as prompted.

----End

4.4.4 Managing Logical Ports

This section describes how to manage logical ports. A logical port is created based on an Ethernet port, a bond port, a VLAN, or a RoCE port.

4.4.4.1 Viewing Logical Ports

This section describes how to view information about logical ports.

Procedure

Step 1 Choose **Services** > **Network** > **Logical Ports**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 View information about logical ports in the function pane. **Table 4-15** describes the parameters.

Table 4-15 Logical port parameters

Parameter	Description
Name	Name of a logical port.
ID	ID of a logical port.
Owning vStore	Name of the vStore to which a logical port belongs.
vStore ID	ID of the vStore to which a logical port belongs.
Running Status	Running status of a logical port. • **Unknown**: The system fails to query the port status. • **Link up**: The running status of the home port of a logical port is link up. • **Link down**: The running status of the home port of a logical port is link down. • **Standby**: In a HyperMetro scenario, when a logical port works at the owning site of the primary or secondary end, the running status of the logical port at the non-owning site of the peer end is **Standby**. • **To be recovered**: When the home port of a logical port is in the **To be recovered** state or a logical port used for the file service fails to be failed over, the running status of the logical port changes to **To be recovered**.

Parameter	Description
Activation Status	Indicates whether a logical port is activated.
Role	Role of a logical port.
Data Protocol	Data protocol of a logical port.
IP Address	IP address of a logical port.
Subnet Mask/ Prefix	Subnet mask of a logical port's IPv4 address or prefix length of a logical port's IPv6 address.
Gateway	Gateway of a logical port's IP address.
Home Port/ Current Port	Home port and current port of a logical port. **NOTE** The icon in the table indicates that port failover occurs and the home port is inconsistent with the current port.
Current Port	Current port of a logical port.
Home Controller/ Current Controller	Home controller and current controller of a logical port.
Failover Group	Failover group of a logical port.
Owning Site	Site to which the logical port belongs. Site to which the logical port in the HyperMetro vStore pair that processes service access belongs.

NOTE

You can click the name of a logical port to view its details and manage it.

----End

4.4.4.2 Modifying a Logical Port

This section describes how to modify a logical port.

Procedure

Step 1 Choose **Services** > **Network** > **Logical Ports**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Click **More** on the right of the desired logical port and select **Modify**.

The **Modify Logical Port** page is displayed.

Step 4 Set the parameters listed in **Table 4-16**.

Table 4-16 Logical port parameters

Parameter	Description
Name	Name of the logical port. The name must meet the following requirements: • The name must be unique. • The name can contain only letters, digits, underscores (_), hyphens (-), and periods (.). • The name contains 1 to 255 characters.
IP Address Type	IP address type of the logical port, which can be **IPv4** or **IPv6**.
IP Address	IPv4 or IPv6 address of the logical port.
Subnet Mask	Subnet mask of the logical port's IPv4 address. **NOTE** This parameter is available only when **IP Address Type** is set to **IPv4**.
Prefix	Prefix length of the logical port's IPv6 address. **NOTE** This parameter is available only when **IP Address Type** is set to **IPv6**.
Gateway	Gateway of a logical port's IP address.
Port Type	Type of the port to which the logical port belongs. The value can be **Ethernet port**, **Bond port**, or **VLAN**. **NOTE** This parameter is modifiable when **Data Protocol** is set to **NFS**, **CIFS**, or **NFS + CIFS**.
Home Port	Ethernet port, bond port, VLAN, or RoCE port to which the logical port belongs.
Activation Status	Determine whether to activate the logical port. **NOTE** This parameter is modifiable when **Data Protocol** is set to **NFS**, **CIFS**, or **NFS + CIFS**.
Failover Group	Name of a failover group. **NOTE** • This parameter is available only when **Data Protocol** is set to **NFS**, **CIFS**, or **NFS + CIFS**. • If a failover group is specified, services on the failed home port will be taken over by an available port in the specified failover group. • If no failover group is specified, services on the failed home port will be taken over by an available port in the default failover group. • It is recommended that the logical ports of the same vStore use the same failover group. This ensures that the fault domains of the logical ports are the same.

Parameter	Description
IP Address Failover	After IP address failover is enabled, services on the failed home port will be taken over by other available ports in the failover group. In the entire process, the IP address used by services remains unchanged. **NOTE** • This parameter is available only when **Data Protocol** is set to **NFS**, **CIFS**, or **NFS + CIFS**. • Shares of file systems do not support the multipathing mode. They use IP address failover to improve the reliability of links.
Failback Mode	After the fault of the home port is rectified, services fail back to the home port. Possible values are **Automatic** and **Manual**. **NOTE** • This parameter is available only when **Data Protocol** is set to **NFS**, **CIFS**, or **NFS + CIFS**. • If **Failback Mode** is **Manual**, ensure that the link to the home port is normal before the failback. You can manually switch services back to the home port only when the link to the home port keeps normal for over five minutes. • If **Failback Mode** is **Automatic**, ensure that the link to the home port is normal before the failback. Services will automatically fail back to the home port only when the link to the home port keeps normal for over five minutes.
Listen for DNS Query	With this function enabled, external NEs can access the DNS service provided by the storage system by using the IP address of this logical port. **NOTE** This parameter is available only when **Data Protocol** is set to **NFS**, **CIFS**, or **NFS + CIFS**.

Parameter	Description
DNS Zone	Name of a DNS zone. **NOTE** • This parameter is available only when **Data Protocol** is set to **NFS**, **CIFS**, or **NFS + CIFS**. • If the value is blank, the logical port is not used for DNS-based load balancing. • One logical port can be associated with only one DNS zone. One DNS zone can be associated with multiple logical ports. • It is recommended that a DNS zone be associated with only logical ports with the same IP address type (IPv4 or IPv6). If the host interface card supports both IPv4 and IPv6 protocols, the DNS client initiates IPv4 and IPv6 resolution requests. If the storage system is associated with both IPv4 and IPv6 logical ports in the same DNS zone and the host interface card is configured with only IPv4 addresses, the host may fail to access the domain name. • The load balancing effect varies with the distribution of logical ports associated with a DNS zone. To obtain a better load balancing effect, ensure that logical ports associated with a DNS zone are evenly distributed among controllers. • If a HyperMetro vStore pair has been created for the owning vStore, you can only select the DNS zones with the same owning site.

Step 5 Click **OK**.

----End

4.4.4.3 Managing Routes

This section describes how to configure route information for a logical port.

Prerequisites

A logical port has been configured with an IP address.

Procedure

Step 1 Choose **Services** > **Network** > **Logical Ports**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Select the desired logical port and click **Manage Route**.

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

NOTE

Alternatively, perform either of the following operations to go to the **Manage Route** page:

- Click **More** on the right of the desired logical port and select **Manage Route**.
- Click the name of the desired logical port. In the upper right corner of the page that is displayed, click **Manage Route** from the **Operation** drop-down list.

Step 4 Configure the route information for the logical port.

1. In the **IP Address** drop-down list, select the IP address of the logical port for which you want to add a route.
2. Click **Add**.
3. Set the parameters listed in **Table 4-17**.

Table 4-17 Route parameters

Parameter	Description
Type	Three types of routes are available: – **Default route** A route through which data is forwarded by default if no preferred route is available. The destination address and mask (IPv4) or prefix (IPv6) of the default route are automatically set to 0. To use this option, you only need to add a gateway. – **Host route** A route to a host. The destination mask (IPv4) or prefix (IPv6) of the host route are automatically set to 255.255.255.255 or 128. To use this option, you only need to add the destination address and gateway. – **Network segment route** A route to a network segment. You must add the destination address, destination mask (IPv4) or prefix (IPv6), and gateway.
Destination Address	IPv4 address, IPv6 address, or network segment of the destination service network port on the application server or destination logical port on another storage system.
Subnet Mask/ Prefix	Subnet mask of the IPv4 address or prefix of the IPv6 address for the destination service network port on the application server or destination logical port on another storage system.
Gateway	Gateway where the local logical port's IP address resides. **NOTE** The IP address of the gateway must be different from all internal heartbeat IP addresses. Otherwise, routing will fail.

4. Click ✓. The route information is added to the list.

NOTE

Click 🗑 on the right of a desired route to delete it.

Step 5 Click **Close**.

----End

4.4.4.4 Failing Back a Logical Port

After a fault of the home port is rectified, you can fail back services to the home port.

Procedure

Step 1 Choose **Services** > **Network** > **Logical Ports**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Select the desired logical port and click **Fail Back**.

NOTE

Alternatively, perform either of the following operations to fail back a logical port:

- Click **More** on the right of the desired logical port, and select **Fail Back**.
- Click the name of the desired logical port. In the upper right corner of the page that is displayed, click **Fail Back** from the **Operation** drop-down list.

----End

4.4.4.5 Deleting a Logical Port

This section describes how to delete a logical port that is no longer used.

Prerequisites

All services on the logical port to be deleted have been stopped.

Procedure

Step 1 Choose **Services** > **Network** > **Logical Ports**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Select one or more desired logical ports and click **Delete**.

NOTE

Alternatively, perform either of the following operations to delete a logical port:

- Click **More** on the right of the desired logical port, and select **Delete**.
- Click the name of the desired logical port. In the upper right corner of the page that is displayed, click **Delete** from the **Operation** drop-down list.

Confirm your operation as prompted.

----End

4.5 Managing Local Authentication Users and User Groups

4.5.1 Managing UNIX Users

4.5.1.1 Managing Local Authentication User Groups

This section describes how to manage and maintain created local authentication user groups.

4.5.1.1.1 Viewing Local Authentication User Groups

This operation enables you to view information about local authentication user groups. The information includes the user group name, description, and users in the group.

Context

- On the local authentication user group management page, you can click to refresh local authentication user group information.
- On the local authentication user group management page, you can click next to a parameter and enter a keyword to search for the required local authentication user groups.
- On the local authentication user group management page, you can click to select the local authentication user group parameters you want to view.

Procedure

Step 1 Choose **Services** > **File Service** > **Authentication Users** > **UNIX Users** > **Local Authentication User Groups**.

Step 2 Select a vStore from the **vStore** drop-down list in the upper left corner.

Step 3 View information about the local authentication user groups of the selected vStore in the function pane. **Table 4-18** describes the parameters.

Table 4-18 Local authentication user group parameters

Parameter	Description
Name	Name of a local authentication user group.
ID	ID of a local authentication user group.

----End

4.5.1.1.2 Modifying Local Authentication User Groups

This section describes how to modify the ID and description of a local authentication user group.

Procedure

Step 1 Choose **Services** > **File Service** > **Authentication Users** > **UNIX Users** > **Local Authentication User Groups**.

Step 2 Select the vStore to which the desired local authentication user group belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Click **More** on the right of the desired local authentication user group and select **Modify**.

The **Modify Local UNIX Authentication User Group** page is displayed on the right.

Step 4 Modify attributes of the local authentication user group.

Table 4-19 describes the parameters.

Table 4-19 Basic local authentication user group parameters

Parameter	Description
ID	ID of the local authentication user group. [Value range] 0 to 4294967295
Description	Description of the local authentication user group. [Value range] The description can be left blank or contain up to 255 characters.

Step 5 Click **OK**.

----End

4.5.1.1.3 Deleting Local Authentication User Groups

After a local authentication user group is deleted, the user group can no longer access a share. However, users in the user group can access the shared resources as authentication users.

Procedure

Step 1 Choose **Services** > **File Service** > **Authentication Users** > **UNIX Users** > **Local Authentication User Groups**.

Step 2 Select the vStore to which the desired local authentication user groups belong from the **vStore** drop-down list in the upper left corner.

Step 3 Select one or more desired local authentication user groups and click **Delete**.

NOTE

You can also click **More** on the right of a desired local authentication user group and select **Delete**.

Step 4 Confirm your operation as prompted.

----End

4.5.1.2 Managing Local Authentication Users

This section describes how to manage and maintain created local authentication users.

4.5.1.2.1 Viewing Local Authentication Users

This operation enables you to view information about local authentication users. The information includes the user name, ID, owning primary group, and description.

Context

- On the local authentication user management page, you can click to refresh local authentication user information.
- On the local authentication user management page, you can click next to a parameter and enter a keyword to search for the required local authentication users.
- On the local authentication user management page, you can click to select the local authentication user parameters you want to view.

Procedure

Step 1 Choose **Services** > **File Service** > **Authentication Users** > **UNIX Users** > **Local Authentication Users**.

Step 2 Select a vStore from the **vStore** drop-down list in the upper left corner.

Step 3 View information about local authentication users of the selected vStore in the function pane. **Table 4-20** describes the parameters.

Table 4-20 Local authentication user parameters

Parameter	Description
Name	Name of a local authentication user.
ID	ID of a local authentication user.
Primary Group	Primary user group to which a local authentication user belongs.

----End

4.5.1.2.2 Modifying Local Authentication Users

This section describes how to modify the ID, primary group, and description of a local authentication user.

Context

Changes in information about local authentication users or domain users accessing an NFS share (for example, a user's the owning group is changed or a user is deleted) will take effect after the next authentication (can be triggered by remounting).

Procedure

Step 1 Choose **Services** > **File Service** > **Authentication Users** > **UNIX Users** > **Local Authentication Users**.

Step 2 Select the vStore to which the desired local authentication user belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Click **More** on the right of the desired local authentication user and select **Modify**.

The **Modify Local UNIX Authentication User** page is displayed on the right.

Step 4 Modify attributes of the local authentication user.

Table 4-21 describes the parameters.

Table 4-21 Basic local authentication user parameters

Parameter	Description
ID	ID of the local authentication user. [Value range] 0 to 4294967295
Primary Group	Primary user group to which the local authentication user belongs. You can click **Choose** and select a group on the **Select Primary Group** page that is displayed.
Description	Description of the local authentication user. [Value range] The description can be left blank or contain up to 255 characters.

Step 5 Click **OK**.

----End

4.5.1.2.3 Deleting Local Authentication Users

After a local authentication user is deleted, it can no longer access a share.

Procedure

Step 1 Choose **Services** > **File Service** > **Authentication Users** > **UNIX Users** > **Local Authentication Users**.

Step 2 Select the vStore to which the desired local authentication users belong from the **vStore** drop-down list in the upper left corner.

Step 3 Select one or more desired local authentication users and click **Delete**.

NOTE

You can also click **More** on the right of a desired local authentication user and select **Delete**.

Step 4 Confirm your operation as prompted.

----End

4.5.2 Managing Windows Users

4.5.2.1 Managing Local Authentication User Groups

This section describes how to manage and maintain created local authentication user groups.

4.5.2.1.1 Viewing Local Authentication User Groups

This operation enables you to view information about local authentication user groups. The information includes the user group name and RID.

Context

- On the local authentication user group management page, you can click to refresh local authentication user group information.
- On the local authentication user group management page, you can click next to a parameter and enter a keyword to search for the required local authentication user groups.
- On the local authentication user group management page, you can click to select the local authentication user group parameters you want to view.

Procedure

Step 1 Choose **Services** > **File Service** > **Authentication Users** > **Windows Users** > **Local Authentication User Groups**.

Step 2 Select a vStore from the **vStore** drop-down list in the upper left corner.

Step 3 View information about local authentication user groups of the selected vStore in the function pane. **Table 4-22** describes the parameters.

Table 4-22 Local authentication user group parameters

Parameter	Description
Name	Name of a local authentication user group.
RID	RID of a local authentication user group.

----End

4.5.2.1.2 Modifying a Local Authentication User Group

This section describes how to modify the name and description of a local authentication user group.

Procedure

Step 1 Choose **Services** > **File Service** > **Authentication Users** > **Windows Users** > **Local Authentication User Groups**.

Step 2 Select the vStore to which the desired local authentication user group belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Click **More** on the right of the desired local authentication user group and select **Modify**.

The **Modify Local Windows Authentication User Group** page is displayed on the right.

Step 4 Modify attributes of the local authentication user group.

Table 4-23 describes the parameters.

Table 4-23 Basic local authentication user group parameters

Parameter	Description
Name	Name of the local authentication user group. [Value range] • The name must be unique. • The name cannot contain "/[]:|<>+=;?*@, or control characters, and cannot end with a period (.). If the name starts or ends with a space, the space is not displayed after the name is created. • The name can contain case-insensitive letters. For example, **aa** and **AA** cannot be created at the same time. • The user group name cannot be the same as the name of a local authentication user. • The name contains 1 to 256 characters.
Description	Description of the local authentication user group. [Value range] The description can be left blank or contain up to 255 characters.

Step 5 Select privileges for the local authentication user group. You can view details about the privileges in the description.

Step 6 Click **OK**.

----End

4.5.2.1.3 Adding a Member

This operation enables you to add a local authentication user, an AD domain user, or an AD domain user group to a local authentication user group.

Procedure

Step 1 Choose **Services** > **File Service** > **Authentication Users** > **Windows Users** > **Local Authentication User Groups**.

Step 2 Select the vStore to which the desired local authentication user group belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Click the name of the desired local authentication user group.

The details page is displayed on the right.

Step 4 Add a local authentication user, an AD domain user, or an AD domain user group.

- Adding a local authentication user
  a. On the **Local Authentication Users** tab page, click **Add**.
  The **Add Local Authentication User** page is displayed on the right.
  b. In the **Available** list, select a local authentication user and add it to the **Selected** area.
  c. Click **OK**.
- Adding an AD domain user
  a. On the **AD Domain Users** tab page, click **Add**.
  The **Add AD Domain User** page is displayed on the right.
  b. In **Name**, enter the AD domain user name.

  NOTE

  - The name contains 1 to 256 characters.
  - The name format is *Domain name**Domain user name*.
  - You can enter multiple names separated by commas (,) or carriage returns.

  c. Click **OK**.
- Adding an AD domain user group
  a. On the **AD Domain User Groups** tab page, click **Add**.
  The **Add AD Domain User Group** page is displayed on the right.
  b. In **Name**, enter the AD domain user group name.

  NOTE

  - The name contains 1 to 256 characters.
  - The name format is *Domain name**Domain user group name*.
  - You can enter multiple names separated by commas (,) or carriage returns.

  c. Click **OK**.

----End

4.5.2.1.4 Removing a Member

This operation enables you to remove a local authentication user, an AD domain user, or an AD domain user group from a local authentication user group.

Procedure

Step 1 Choose **Services** > **File Service** > **Authentication Users** > **Windows Users** > **Local Authentication User Groups**.

Step 2 Select the vStore to which the desired local authentication user group belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Click the name of the desired local authentication user group.

The details page is displayed on the right.

Step 4 Remove a local authentication user, an AD domain user, or an AD domain user group.

- Removing a local authentication user

  On the **Local Authentication Users** tab page, select a local authentication user and click **Remove** above the list.

- Removing an AD domain user

  On the **AD Domain Users** tab page, select an AD domain user and click **Remove** above the list.

- Removing an AD domain user group

  On the **AD Domain User Groups** tab page, select an AD domain user group and click **Remove** above the list.

NOTE

Alternatively, click **Remove** on the right of a user or user group.

----End

4.5.2.1.5 Deleting a Local Authentication User Group

After a local authentication user group is deleted, the user group can no longer access a share. However, users in the user group can access the shared resources as authentication users.

Procedure

Step 1 Choose **Services** > **File Service** > **Authentication Users** > **Windows Users** > **Local Authentication User Groups**.

Step 2 Select the vStore to which the desired local authentication user group belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Select one or more desired local authentication user groups and click **Delete**.

NOTE

You can also click **More** on the right of a desired local authentication user group and select **Delete**.

Step 4 Confirm your operation as prompted.

----End

4.5.2.2 Managing Local Authentication Users

This section describes how to manage and maintain created local authentication users.

4.5.2.2.1 Viewing Local Authentication Users

This section describes how to view information about local authentication users, including the name, RID, status, and password validity period.

Context

- On the local authentication user management page, you can click to refresh local authentication user information.
- On the local authentication user management page, you can click next to a parameter and enter a keyword to search for the required local authentication users.
- On the local authentication user management page, you can click to select the local authentication user parameters you want to view.
- On the local authentication user management page, you can click or next to a parameter to change the display order of local authentication users.

Procedure

Step 1 Choose **Services** > **File Service** > **Authentication Users** > **Windows Users** > **Local Authentication Users**.

Step 2 Select a vStore from the **vStore** drop-down list in the upper left corner.

Step 3 View information about local authentication users of the selected vStore in the function pane. **Table 4-24** describes the parameters.

Table 4-24 Local authentication user parameters

Parameter	Description
Name	Name of a local authentication user.
RID	RID of a local authentication user.
Status	Status of a local authentication user, that is, whether the user is enabled.
Password Validity Period	Password validity period of a local authentication user. After the password expires, the user cannot access shares.

Step 4 (Optional) Click the name of a local authentication user to view basic information about the user and manage the groups to which the user belongs.

----End

4.5.2.2.2 Modifying a Local Authentication User

This section describes how to modify the name, password, status, and description of a local authentication user.

Context

Changes in information about local authentication users or domain users accessing a CIFS share (for example, a user is disabled, a password has expired or is changed, the owning group is changed, or a user is deleted) will take effect after the next authentication, which can be triggered by share re-mounting.

Procedure

Step 1 Choose **Services** > **File Service** > **Authentication Users** > **Windows Users** > **Local Authentication Users**.

Step 2 Select the vStore to which the desired local authentication user belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Click **More** on the right of the desired local authentication user and select **Modify**.

The **Modify Local Windows Authentication User** page is displayed on the right.

Step 4 Modify attributes of the local authentication user.

Table 4-25 describes the parameters.

Table 4-25 Basic local authentication user parameters

Parameter	Description
Name	Name of the local authentication user. [Value range] • The name must be unique. • The name cannot contain "/\][:;|=,+*?<>@, spaces, or control characters, and cannot end with a period (.). • The name can contain case-insensitive letters. For example, **aaaaaaaa** and **AAAAAAAA** cannot be created at the same time. • The name cannot be the same as the name of a local authentication user group. • The name contains 3 to 20 characters. **NOTE** You can modify the minimum length of the user name on the **Set Security Policy** page.

Parameter	Description
Password	Click **Modify**, and set **Password** and **Confirm Password** for the local authentication user. [Value range] • The password contains 6 to 32 characters. • The password must contain at least one of the following types: special characters, uppercase letters, lowercase letters, and digits. Special characters include !"#$%&'()*+,-./:;<=>?@[\]^`{_|}~ and spaces. • The password cannot contain three consecutive identical characters. • The password cannot be the same as the user name or the user name spelled backward. **NOTE** You can modify the password security policy on the **Set Security Policy** page.
Status	Indicates whether to enable the user.
Description	Description of the local authentication user. [Value range] The description can be left blank or contain up to 255 characters.

Step 5 Click **OK**.

----End

4.5.2.2.3 Enabling a Local Authentication User

A disabled local authentication user cannot access any share. This operation enables you to enable a local authentication user to allow it to access shares.

Prerequisites

Status of a local authentication user is **Disabled**.

Procedure

Step 1 Choose **Services** > **File Service** > **Authentication Users** > **Windows Users** > **Local Authentication Users**.

Step 2 Select the vStore to which the desired local authentication user belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Select one or more desired local authentication users and click **Enable**.

NOTE

You can also click **More** on the right of a desired local authentication user and select **Enable**.

----End

4.5.2.2.4 Disabling a Local Authentication User

To prevent a local authentication user from accessing a share, you can disable the user. A disabled local authentication user cannot access any share. You can enable it to allow it to access shares.

Prerequisites

Status of a local authentication user is **Enabled**.

Procedure

Step 1 Choose **Services** > **File Service** > **Authentication Users** > **Windows Users** > **Local Authentication Users**.

Step 2 Select the vStore to which the desired local authentication user belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Select one or more desired local authentication users and click **Disable**.

NOTE

You can also click **More** on the right of a desired local authentication user and select **Disable**.

----End

4.5.2.2.5 Adding an Owning Group

This operation enables you to add a group to which a local authentication user belongs.

Procedure

Step 1 Choose **Services** > **File Service** > **Authentication Users** > **Windows Users** > **Local Authentication Users**.

Step 2 Select the vStore to which the desired local authentication user belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Click **More** on the right of the desired local authentication user and select **Add Owning Group**.

The **Add Owning Group** page is displayed on the right.

NOTE

Alternatively, click the name of the desired local authentication user. On the details page that is displayed, click **Add** in the **Owning Groups** area.

Step 4 In the **Available Groups** list, select groups and add them to the **Selected Groups** area.

Step 5 Click **OK**.

----End

4.5.2.2.6 Removing an Owning Group

This operation enables you to remove a group to which a local authentication user belongs.

Procedure

Step 1 Choose **Services** > **File Service** > **Authentication Users** > **Windows Users** > **Local Authentication Users**.

Step 2 Select the vStore to which the desired local authentication user belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Click the name of the desired local authentication user. On the details page that is displayed, select a group in the **Owning Groups** area and click **Remove** above the list.

NOTE

Alternatively, click **Remove** on the right of a group.

----End

4.5.2.2.7 Setting Security Policies for a Local Authentication User

Security policies for a local authentication user contain password and login policies. Proper settings of the security policies improve system security.

Procedure

Step 1 Choose **Services** > **File Service** > **Authentication Users** > **Windows Users** > **Local Authentication Users**.

Step 2 Select the vStore to which the desired local authentication user belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Click **Set Security Policy**.

The **Set Security Policy** page is displayed on the right.

Step 4 Configure the user name policy for local authentication users.

Set **Min. Length** of user names to prevent you from setting overly short user names.

NOTE

The value is an integer ranging from 1 to 20.

Step 5 Configure the password policy for local authentication users.

Table 4-26 describes the parameters.

Table 4-26 Password policy parameters

Parameter	Description
Length	Minimum and maximum lengths of a password, preventing you from setting overly short or long passwords. [Value range] The value is an integer ranging from 6 to 32.
Complexity	Complexity of a password, preventing you from setting overly simple passwords. Possible values are: • A password must contain at least two of the following types: special characters, uppercase letters, lowercase letters, and digits. Special characters include !"#$%&'()*+,-./:;<=>?@[\]^`{_\|}~ and spaces. • A password must contain special characters and at least two of the following types: uppercase letters, lowercase letters, and digits. Special characters include !"#$%&'()*+,-./:;<=>?@[\]^`{_|}~ and spaces.
Max. Consecutive Duplicate Characters	Maximum number of consecutive duplicate characters allowed in a password. **0** indicates unlimited. [Value range] The value is an integer ranging from 0 to 9.
Validity Period	Password validity period, in days. **0** indicates unlimited. After the validity period of a password expires, the system prompts you to change the password. [Value range] The value is an integer ranging from 0 to 999.
Change Interval	Minimum interval for changing a password. **0** indicates unlimited. [Value range] The value is an integer ranging from 0 to 9999.

Step 6 Set the login policy for local authentication users.

Table 4-27 describes the parameters.

Table 4-27 Login policy parameters

Parameter	Description
Incorrect Password Attempts	Maximum number of consecutive incorrect password attempts allowed during login. **0** indicates unlimited. If the number of consecutive incorrect password attempts in 1 minute exceeds the value, the system automatically locks the user. The user will be unlocked after 1 minute. [Value range] The value is an integer ranging from 0 to 9.
Idle Time Before Lockout	If a user account has not been used to log in to the system for the specified number of days, the account will be locked. You need to manually enable the account. **0** indicates unlimited. [Value range] The value is an integer ranging from 0 to 999.

Step 7 Click **OK**.

----End

4.5.2.2.8 Deleting a Local Authentication User

After a local authentication user is deleted, it can no longer access CIFS shares.

Context

If the local authentication user that you want to delete has been added to a local authentication user group, the user is removed from the user group after being deleted.

Deleting a local authentication user will take effect after the next authentication, which can be triggered by share re-mounting.

Procedure

Step 1 Choose **Services** > **File Service** > **Authentication Users** > **Windows Users** > **Local Authentication Users**.

Step 2 Select the vStore to which the desired local authentication user belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Select one or more desired local authentication users and click **Delete**.

NOTE

You can also click **More** on the right of a desired local authentication user and select **Delete**.

Step 4 Confirm your operation as prompted.

----End

4.6 Managing NFS Shares

This section describes how to manage and maintain created NFS shares.

4.6.1 Viewing NFS Shares

This operation enables you to view the path and description of an NFS share.

Context

- On the NFS share management page, you can click to refresh NFS share information.
- On the NFS share management page, you can click to select the NFS share parameters you want to view.

Prerequisites

You have created an NFS share.

Procedure

Step 1 Choose **Services** > **File Service** > **Shares** > **NFS Shares**.

Step 2 Select a vStore from the **vStore** drop-down list in the upper left corner.

Step 3 View information about the NFS shares of the selected vStore in the function pane. **Table 4-28** describes the parameters.

Table 4-28 NFS share parameters

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

Step 4 (Optional) Click the path of an NFS share to view its basic information.

----End

4.6.2 Modifying an NFS Share

This section describes how to modify an NFS share.

Prerequisites

- You have created an NFS share.
- When **Share Path** is set to global root directory **/**, the NFS share properties cannot be modified.

Procedure

Step 1 Choose **Services** > **File Service** > **Shares** > **NFS Shares**.

Step 2 Select the vStore to which the desired NFS share belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Click **More** on the right of the desired NFS share and select **Modify**.

The **Modify NFS Share** page is displayed on the right.

NOTE

You can also click the path of the desired NFS share. In the upper right corner of the page that is displayed, click **Operation** and select **Modify**.

Step 4 Set basic NFS share parameters.

Table 4-29 describes the parameters.

Table 4-29 Basic NFS share parameters

Parameter	Description
Description	Description of the NFS share. [Value range] The description can be left blank or contain up to 255 characters.

Parameter	Description
Character Encoding	Clients communicate with the storage system using codes. Codes configured on the NFS share must be the same as that of the clients. These codes apply to names and metadata of shared files, but do not change the codes of file data. Codes include: • UTF-8 International code set • EUC-JP euc-j*[ja] code set • JIS JIS code set • S-JIS cp932*[ja_jp.932] code set • ZH Simplified Chinese code set, in compliance with GB 2312 • GBK Simplified Chinese code set, in compliance with GB 2312 • EUC-TW Traditional Chinese code set, in compliance with CNS 11643 • BIG5 cp950 traditional Chinese code set • DE German character set, in compliance with ISO 8859-1 • PT Portuguese character set, in compliance with ISO 8859-1 • ES Spanish character set, in compliance with ISO 8859-1 • FR French character set, in compliance with ISO 8859-1 • IT Italian character set, in compliance with ISO 8859-1 • KO cp949 Korean code set • AR Arabic character set, in compliance with ISO 8859-6 • CS Czech character set, in compliance with ISO 8859-2 • DA Danish character set, in compliance with ISO 8859-1 • FI Finnish character set, in compliance with ISO 8859-1 • HE Hebrew character set, in compliance with ISO 8859-8

Parameter	Description
	• HR Croatian character set, in compliance with ISO 8859-2 • HU Hungarian character set, in compliance with ISO 8859-2 • NO Norwegian character set, in compliance with ISO 8859-1 • NL Dutch character set, in compliance with ISO 8859-1 • PL Polish character set, in compliance with ISO 8859-2 • RO Romanian character set, in compliance with ISO 8859-2 • RU Russian character set, in compliance with ISO 8859-5 • SK Slovak character set, in compliance with ISO 8859-2 • SL Slovenian character set, in compliance with ISO 8859-2 • SV Swedish character set, in compliance with ISO 8859-1 • TR Turkish character set, in compliance with ISO 8859-9 • EN-US English character set, in compliance with ISO 8859-1 **NOTE** – Method of querying character encoding on clients (for example, in Linux): Run the **locale** command to view character encoding of the current system. – NFSv4 supports only UTF-8. If NFSv4 is used, ensure that the host uses UTF-8 character encoding.
Show Snapshot	This function allows clients to show and traverse snapshot directories.

Step 5 Click **OK**.

----End

4.6.3 Modifying an NFS Share Client

This operation enables you to modify the attributes of an NFS share client.

Prerequisites

- You have added a client to an NFS share.
- When **Share Path** is set to global root directory **/**, the properties of the NFS share client cannot be modified.

Procedure

Step 1 Choose **Services** > **File Service** > **Shares** > **NFS Shares**.

Step 2 Select the vStore to which the desired NFS share belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Click the path of the desired NFS share. The page displaying the share's details is displayed on the right.

Step 4 In the **Permissions** area, click **More** on the right of the desired client and select **Modify**.

The **Modify Client** page is displayed.

Step 5 Change the permission of the client. **Table 4-30** describes the parameters.

Table 4-30 Client permission parameters

Parameter	Description
UNIX Permission	Indicates the permission level for a UNIX client to access the NFS share. Possible options are: • **Read-only**: The client can only read files in the NFS share. • **Read-write**: The client can read and write files in the NFS share. • **None**: No operation is allowed on the NFS share.
Kerberos5 Permission	Indicates the permission level for the Kerberos5 client to access the NFS share. Possible options are: • **Read-only**: The client can only read files in the NFS share. • **Read-write**: The client can read and write files in the NFS share. • **None**: No operation is allowed on the NFS share. This parameter applies only to the scenario where the NFS Kerberos service is configured.
Kerberos5i Permission	Indicates the permission level for the Kerberos5i client to access the NFS share. Possible options are: • **Read-only**: The client can only read files in the NFS share. • **Read-write**: The client can read and write files in the NFS share. • **None**: No operation is allowed on the NFS share. This parameter applies only to the scenario where the NFS Kerberos service is configured.

Parameter	Description
Kerberos5p Permission	Indicates the permission level for the Kerberos5p client to access the NFS share. Possible options are: • **Read-only**: The client can only read files in the NFS share. • **Read-write**: The client can read and write files in the NFS share. • **None**: No operation is allowed on the NFS share. This parameter applies only to the scenario where the NFS Kerberos service is configured.
root Permission Constraint	Controls the **root** permission of the clients. • **root_squash**: does not allow a client to access the share as user **root**. Otherwise, the client will be mapped as an anonymous user. • **no_root_squash**: allows a client to access the share as user **root** that has full control and access permissions for shared directories. **NOTE** • If a VM needs to be created in the NFS share, select **no_root_squash**. Otherwise, the VM may run abnormally. • For a file system or dtree whose security mode is UNIX, the default UNIX permission is **755**. If **root_squash** is enabled for the NFS share permission of the file system or dtree, user **root** only has the read and execute permissions. You can run the **change file_system general file_system_id=? unix_permissions=?** or **change dtree dtree_id=? unix_permissions=?** command to modify the UNIX permission of the file system or dtree.

Step 6 Modify advanced client parameters. Select **Advanced** in the upper right corner.

Table 4-31 describes the parameters.

Table 4-31 Advanced client parameters

Parameter	Description
Permission Constraint	Indicates whether to retain the UID and GID of a shared directory. • **all_squash**: The UID and GID of a shared directory are mapped to user **nobody**, which is applicable to public directories. • **no_all_squash**: retains the UID and GID of a shared directory.

Parameter	Description
Source Port Verification Constraint	Indicates whether to enable source port verification. • **secure**: allows clients to access the NFS share using ports 1 to 1023. • **insecure**: allows the clients to access the NFS share using any port.
Anonymous User ID	Indicates the UID and GID of a user who accesses the shared directory after the user is mapped as an anonymous user.

Step 7 Click **OK**.

----End

4.6.4 Creating an NFS Share from a Template

This section describes how to create an NFS share based on the parameters set for an existing NFS share. The system presets the parameters of the newly created NFS share based on the parameters set for the existing NFS share. However, you can also modify the parameters.

Prerequisites

If **Share Path** is set to global root directory **/**, you cannot create a template for it.

Procedure

Step 1 Choose **Services** > **File Service** > **Shares** > **NFS Shares**.

Step 2 Select the vStore to which the NFS share to be used as the template belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Select the NFS share to be used as a template and click **Create From**.

The **Create NFS Share from Template** page is displayed on the right.

NOTE

Alternatively, perform either of the following operations to go to the **Create NFS Share from Template** page:

- Click **More** on the right of the desired NFS share and select **Create From**.
- Click the name of the desired NFS share. In the upper right corner of the page that is displayed, click **Operation** and select **Create From**.

Step 4 Select the file system for which the NFS share is created from the **File System** drop-down list.

NOTE

If the selected file system is the secondary storage system in a remote replication pair, data in the file system is probably being modified when it is accessed. Before performing this operation, confirm that the application allows possible data inconsistency.

Step 5 Select the dtree for which the NFS share is created from the **Dtree** drop-down list. If you do not select a dtree, the NFS share is created for the entire file system.

Step 6 Except **File System** and **Dtree**, other parameters are preset by the system. You can modify them as required.

1. Select **Advanced** in the upper right corner and set advanced parameters for the NFS share.

   Table 4-32 describes the parameters.

Table 4-32 Advanced NFS share parameters

Parameter	Description
Description	Description of the NFS share. [Value range] The description can be left blank or contain up to 255 characters.

Parameter	Description
Character Encoding	Clients communicate with the storage system using codes. Codes configured on the NFS share must be the same as that of the clients. These codes apply to names and metadata of shared files, but do not change the codes of file data. Codes include: – UTF-8 International code set – EUC-JP euc-j*[ja] code set – JIS JIS code set – S-JIS cp932*[ja_jp.932] code set – ZH Simplified Chinese code set, in compliance with GB 2312 – GBK Simplified Chinese code set, in compliance with GB 2312 – EUC-TW Traditional Chinese code set, in compliance with CNS 11643 – BIG5 cp950 traditional Chinese code set – DE German character set, in compliance with ISO 8859-1 – PT Portuguese character set, in compliance with ISO 8859-1 – ES Spanish character set, in compliance with ISO 8859-1 – FR French character set, in compliance with ISO 8859-1 – IT Italian character set, in compliance with ISO 8859-1 – KO cp949 Korean code set – AR Arabic character set, in compliance with ISO 8859-6 – CS Czech character set, in compliance with ISO 8859-2 – DA Danish character set, in compliance with ISO 8859-1 – FI Finnish character set, in compliance with ISO 8859-1

Parameter	Description
	– HE Hebrew character set, in compliance with ISO 8859-8 – HR Croatian character set, in compliance with ISO 8859-2 – HU Hungarian character set, in compliance with ISO 8859-2 – NO Norwegian character set, in compliance with ISO 8859-1 – NL Dutch character set, in compliance with ISO 8859-1 – PL Polish character set, in compliance with ISO 8859-2 – RO Romanian character set, in compliance with ISO 8859-2 – RU Russian character set, in compliance with ISO 8859-5 – SK Slovak character set, in compliance with ISO 8859-2 – SL Slovenian character set, in compliance with ISO 8859-2 – SV Swedish character set, in compliance with ISO 8859-1 – TR Turkish character set, in compliance with ISO 8859-9 – EN-US English character set, in compliance with ISO 8859-1 **NOTE** ■ Method of querying character encoding on clients (for example, in Linux): Run the **locale** command to view character encoding of the current system. ■ NFSv4 supports only UTF-8. If NFSv4 is used, ensure that the host uses UTF-8 character encoding.
Show Snapshot	This function allows clients to show and traverse snapshot directories.

2. Configure access permissions for the NFS share.

   Click **Add** to add a client. For details, see **3.8.1.10 Adding an NFS Share Client**.

NOTE

- You can click **More** on the right of a client and select **Modify** to modify its information.
- You can select one or more clients and click **Remove**, or click **More** on the right of a client and select **Remove**, to remove clients.

Step 7 Click **OK**.

Confirm your operation as prompted.

----End

4.6.5 Removing an NFS Share Client

This operation enables you to remove an NFS share client.

Prerequisites

You have added a client to an NFS share.

Procedure

Step 1 Choose **Services** > **File Service** > **Shares** > **NFS Shares**.

Step 2 Select the vStore to which the desired NFS share belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Click the path of the desired NFS share. The page displaying the share's details is displayed on the right.

Step 4 In the **Permissions** area, select one or more desired clients and click **Remove**.

NOTE

You can also click **More** on the right of a desired client and select **Remove**.

Step 5 Confirm your operation as prompted.

----End

4.6.6 Adding a File Name Extension Filtering Rule

After file name extension filtering rules are configured, the types of files that users access in an NFS share are controlled.

Prerequisites

If **Share Path** is set to global root directory **/**, you cannot add a file name extension filtering rule.

Context

- For NFSv4.0 and NFSv4.1 protocols, if a file has been opened when you add a filtering rule, the newly-added filtering rule does not take effect for the file immediately. The filtering rule takes effect only after the file is closed on the client.

- For the NFSv3 protocol, if a handle in the cache is being used on the client to perform operations on a file when you add a filtering rule, the newly-added filtering rule does not take effect immediately for the file. The filtering rule takes effect only when the file name is used to initiate an operation request for the file again on the client.

Procedure

Step 1 Choose **Services** > **File Service** > **Shares** > **NFS Shares**.

Step 2 Select the vStore to which the desired NFS share belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Click the path of the desired NFS share. The page displaying the share's details is displayed on the right.

Step 4 On the **File Name Extension Filtering Rules** tab page, click **Add**.

The **Add File Name Extension Filtering Rule** page is displayed on the right.

NOTE

After a file name extension filtering rule is added, it takes effect only after the next NFS service request (such as refreshing directories, creating files, opening files, renaming files, and querying file attributes) is initiated.

Step 5 Add a file name extension filtering rule.

NOTE

The file name extension filtering rule is valid only for the current share.

1. In **File Name Extension**, specify the file name extensions (file types) to be filtered.

   NOTE

   - You can enter multiple file name extensions and separate them with commas (,) or carriage returns. The total length (including the separators) cannot exceed 127 characters.
   - A single file name extension can contain only digits, letters, spaces, and special characters (!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~). Wildcards ? and * are supported, and wildcard * must be the last character. For example, **txt**, **TXT**, **T?X**, or **Tx***.
   - It is recommended that one share have a maximum of seven file name extension filtering rules. A single file name extension filtering rule contains a maximum of 32 characters excluding wildcards. The recommended configurations minimize the adverse impact on NFS service performance. If the recommended configurations are not used, the NFS service performance may greatly deteriorate.
   - When configuring a file name extension filtering rule, ensure that the rule does not affect the storage of temporary files that may be generated when application software is running. For example, some application software may generate files with the **.tmp** file name extension. In this case, add the **.tmp** extension to the file name extension filtering rule. For details about the temporary file name extensions generated by specific application software, contact the corresponding software vendor.

2. Select a permission rule from the **Rule Type** drop-down list.

NOTE

- **Denied only**: Users do not have permissions to access files with the specified extensions.
- **Allowed only**: Users have permissions to access files with the specified extensions.

3. Select one or more operation types on the right of **Operation Type** to deny or allow users to perform specified operations on files with specified file name extensions.

NOTE

For example, set **File Name Extension** to **txt**, **Rule Type** to **Allowed only**, and **Operation Type** to **Create** and **Delete**. That is, users can create and delete only TXT files.

Step 6 Click **OK**.

----End

4.6.7 Modifying a File Name Extension Filtering Rule

This section describes how to modify a file name extension filtering rule.

Procedure

Step 1 Choose **Services** > **File Service** > **Shares** > **NFS Shares**.

Step 2 Select the vStore to which the desired NFS share belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Click the path of the desired NFS share. The page displaying the share's details is displayed on the right.

Step 4 On the **File Name Extension Filtering Rules** tab page, click **More** on the right of the desired file name extension filtering rule and select **Modify**.

The **Modify File Name Extension Filtering Rule** page is displayed on the right.

NOTE

After a file name extension filtering rule is modified, it takes effect only after the next NFS service request (such as refreshing directories, creating files, opening files, renaming files, and querying file attributes) is initiated.

Step 5 Modify an existing file name extension filtering rule.

NOTE

The file name extension filtering rule is valid only for the current share.

1. In **File Name Extension**, specify the file name extensions (file types) to be filtered.

NOTE

- You can enter multiple file name extensions and separate them with commas (,) or carriage returns. The total length (including the separators) cannot exceed 127 characters.
- A single file name extension can contain only digits, letters, spaces, and special characters (!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~). Wildcards ? and * are supported, and wildcard * must be the last character. For example, **txt**, **TXT**, **T?X**, or **Tx***.
- It is recommended that one share have a maximum of seven file name extension filtering rules. A single file name extension filtering rule contains a maximum of 32 characters excluding wildcards. The recommended configurations minimize the adverse impact on NFS service performance. If the recommended configurations are not used, the NFS service performance may greatly deteriorate.
- When configuring a file name extension filtering rule, ensure that the rule does not affect the storage of temporary files that may be generated when application software is running. For example, some application software may generate files with the **.tmp** file name extension. In this case, add the **.tmp** extension to the file name extension filtering rule. For details about the temporary file name extensions generated by specific application software, contact the corresponding software vendor.

2. Select a permission rule from the **Rule Type** drop-down list.

NOTE

- **Denied only**: Users do not have permissions to access files with the specified extensions.
- **Allowed only**: Users have permissions to access files with the specified extensions.

3. Select one or more operation types on the right of **Operation Type** to deny or allow users to perform specified operations on files with specified file name extensions.

NOTE

For example, set **File Name Extension** to **txt**, **Rule Type** to **Allowed only**, and **Operation Type** to **Create** and **Delete**. That is, users can create and delete only TXT files.

Step 6 Click **OK**.

----End

4.6.8 Removing a File Name Extension Filtering Rule

This section describes how to remove a file name extension filtering rule.

Procedure

Step 1 Choose **Services** > **File Service** > **Shares** > **NFS Shares**.

Step 2 Select the vStore to which the desired NFS share belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Click the path of the desired NFS share. The page displaying the share's details is displayed on the right.

Step 4 On the **File Name Extension Filtering Rules** tab page, select one or more file name extension filtering rules to be deleted and click **Remove**.

NOTE

You can also click **More** on the right of a desired file name extension filtering rule and select **Remove**.

Step 5 Confirm your operation as prompted.

----End

4.6.9 Deleting an NFS Share

This operation enables you to delete an NFS share that is no longer used. After an NFS share is deleted, it becomes unavailable and all services on the NFS share are interrupted. Exercise caution when deleting an NFS share.

Prerequisites

No services are running on the NFS share.

Procedure

Step 1 Choose **Services** > **File Service** > **Shares** > **NFS Shares**.

Step 2 Select the vStore to which the desired NFS shares belong from the **vStore** drop-down list in the upper left corner.

Step 3 Select one or more desired NFS shares and click **Delete**.

NOTE

Alternatively, perform either of the following operations to delete an NFS share:

- Click **More** on the right of a desired NFS share and select **Delete**.
- Click the path name of a desired NFS share. In the upper right corner of the page that is displayed, click **Operation** and select **Delete**.

Step 4 Confirm your operation as prompted.

----End

4.7 Managing CIFS and Homedir Shares

This section describes how to manage and maintain created CIFS shares.

4.7.1 Viewing CIFS Shares

The operation enables you to view paths, users or users groups, and access permissions of CIFS shares.

Context

- On the CIFS share management page, you can click to refresh CIFS share information.
- On the CIFS share management page, you can click next to a parameter and enter a keyword to search for the required CIFS shares.

- On the CIFS share management page, you can click to select the CIFS share parameters you want to view.

Prerequisites

You have created a CIFS share.

Procedure

Step 1 Choose **Services** > **File Service** > **Shares** > **CIFS Shares**.

Step 2 Select a vStore from the **vStore** drop-down list in the upper left corner.

Step 3 View information about the CIFS shares of the selected vStore in the function pane. **Table 4-33** describes the parameters.

Table 4-33 CIFS share parameters

Parameter	Description
Share Name	Name of a CIFS share.
ID	ID of a CIFS share.
Path	Share path of the file system, which is generated based on the **File System** and **Dtree** parameters. [Example] /Filesystem001/Dtree_test
Homedir	Indicates whether the share mode is Homedir share.
Notify	Indicates whether the Notify function is enabled for a share.
Continuously Available	Indicates whether the **Continuously Available** function of a share is enabled. This option is the SMB continuous availability feature. This feature relies on Oplock, which is enabled by default. If Oplock is disabled, enable it on the CLI.
SMB3 Encryption	Indicates whether SMB3 encryption is enabled for a share. After this function is enabled, the system encrypts the share to ensure data security. However, the performance deteriorates. **NOTE** After SMB3 encryption is enabled, only SMB3 clients can access shares by default.
Unencrypted Client Access	Indicates whether a share is accessed by non-encrypted clients. After this function is enabled, clients that do not have encryption capabilities can access the share. **NOTE** This function takes effect only after the SMB3 encryption function is enabled.

Parameter	Description
ABE	Indicates whether the ABE function is enabled for a share.

Step 4 (Optional) Click the name of a CIFS share to view its basic information.

----End

4.7.2 Modifying a CIFS Share

This operation enables you to modify attributes of a CIFS share.

Prerequisites

You have created a CIFS share.

Procedure

Step 1 Choose **Services** > **File Service** > **Shares** > **CIFS Shares**.

Step 2 Select the vStore to which the desired CIFS share belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Click **More** on the right of the desired CIFS share and select **Modify**.

The **Modify CIFS Share** page is displayed on the right.

NOTE

You can also click the name of the desired CIFS share. In the upper right corner of the page that is displayed, click **Operation** and select **Modify**.

Step 4 Configure properties of the CIFS share.

Table 4-34 describes the parameters.

Table 4-34 Advanced parameters of a CIFS share

Parameter	Description
Description	Indicates the description of a CIFS share. **NOTE** The description can be left blank or contain up to 255 characters.
Notify	Determine whether to enable **Notify**. After this function is enabled, a client's operations on a directory, such as adding a sub-directory, adding a file, modifying the directory, and modifying a file, can be detected by other clients that are accessing this directory or the parent directory of this directory. The created or modified directories and files are visible after the page automatically refreshes.

Parameter	Description
Continuously Available	Determine whether to enable **Continuously Available**. This option provides the SMB continuous availability feature. This feature depends on Oplock which is enabled by default. If Oplock is disabled, choose **Settings** > **File Service** > **CIFS Service** to enable it.
SMB3 Encryption	Specifies whether to enable SMB3 encryption. After this function is enabled, the system encrypts the CIFS share to ensure data security, but the performance deteriorates. **NOTICE** Enabling this function affects SMB3 service performance. Check whether this function needs to be enabled. **NOTE** After SMB3 encryption is enabled, only SMB3 clients can access shares by default.
Unencrypted Client Access	After this function is enabled, clients that do not have encryption capabilities can access the share. **NOTICE** After this function is enabled, clients of earlier versions (for example, Windows 7) are allowed to access shares where SMB3 encryption is enabled in plaintext. Check whether this function needs to be enabled. **NOTE** This function takes effect only after the SMB3 encryption function is enabled.
ABE	After ABE is enabled, files and folders that users have no access permission are not displayed. **NOTE** SMB2 and SMB3 support this function but SMB1 does not.
Show Snapshot	This function allows clients to show and traverse snapshot directories.

Step 5 Click **OK**.

----End

4.7.3 Modifying a User or User Group in a CIFS Share

This operation enables you to modify attributes of a user or user group in a CIFS share.

Prerequisites

You have added a user or user group to a CIFS share.

Procedure

Step 1 Choose **Services** > **File Service** > **Shares** > **CIFS Shares**.

Step 2 Select the vStore to which the desired CIFS share belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Click the name of the desired CIFS share.

Step 4 In the **Permissions** area on the page that is displayed, click **More** on the right of the desired user or user group and select **Modify**.

The **Modify User or User Group** page is displayed.

Step 5 In **Permission**, select the permission granted to the user or user group for accessing the CIFS share.

Table 4-35 describes the permissions.

Table 4-35 CIFS share permissions

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

NOTE

- The permission priority from high to low is **Forbidden** > **Full control** > **Read-write** > **Read-only**. The highest permission prevails. If a user is granted with a higher permission than its original one, 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 changed to **Full control** and it can access the CIFS share immediately without re-authentication.
- You can run the **change service cifs administrators_privilege=?** command on the CLI to modify permissions of members in the **Administrators** user group. For details about the command, see *Command Reference* of the desired version. In the command, the value of the **administrators_privilege** parameter can be **admin** (default), **default_group**, or **owner**.

  For local authentication users whose primary user group is **Administrators**, users with different **administrators_privilege** values have different permissions.

  – **admin**: When members in the **Administrators** user group access a shared file system in the storage system, they do not need to be authenticated by share-level ACLs and NT ACLs. They can operate any file in any share with administrator permissions without the need to be authenticated.

  – **default_group**: Members in the **Administrators** user group have the same permissions as members in the **default_group** user group.

  – **owner**: Members in the **Administrators** user group have the permissions to query and set file or directory ACLs and modify file or directory owners. When the group members access shared file systems, they need to be authenticated by directory- or file-level NT ACLs, but do not need to be authenticated by share-level ACLs.

  Modified permissions take effect only after users are re-authenticated on clients.

  You can run the **show service cifs** command on the CLI and check permissions of the **Administrators** user group in the **Administrators Privilege** field.

Step 6 Click **OK**.

----End

4.7.4 Creating a CIFS Share from a Template

This section describes how to create a CIFS share based on the parameters set for an existing CIFS share. The system presets the parameters of the newly created CIFS share based on the parameters set for the existing CIFS share. However, you can also modify the parameters.

Procedure

Step 1 Choose **Services** > **File Service** > **Shares** > **CIFS Shares**.

Step 2 Select the vStore to which the CIFS share to be used as the template belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Select the CIFS share to be used as a template and click **Create From**.

The **Create CIFS Share from Template** page is displayed on the right.

NOTE

Alternatively, perform either of the following operations to go to the **Create CIFS Share from Template** page:

- Click **More** on the right of the desired CIFS share and select **Create From**.
- Click the name of the desired CIFS share. In the upper right corner of the page that is displayed, click **Operation** and select **Create From**.

Step 4 Set basic CIFS share parameters.

Table 4-36 describes the parameters.

Table 4-36 Basic CIFS share parameters

Parameter	Description
File System	File system for which you want to create a CIFS share. **NOTE** If the selected file system is the secondary storage system in a remote replication pair or remote storage system in a HyperMetro pair, data in the file system is probably being modified when it is accessed. Before performing this operation, confirm that the application allows possible data inconsistency. [Example] Filesystem001
Dtree	Dtree for which you want to create a CIFS share. If you do not select a dtree, the CIFS share is created for the entire file system. [Example] Dtree_test
Share Name	Name of the share, which is used by users to access shared resources. [Value range] • The name must be unique. • The name cannot contain characters " / \ [ ] : | < > + ; , ? * =. The name cannot be **ipc$**, **autohome**, **~**, or **print$** reserved by the system. • The name contains 1 to 80 characters. [Example] share_for_user1
Share Path	Share path of the file system, which is generated based on the **File System** and **Dtree** parameters. [Example] /Filesystem001/Dtree_test

Step 5 Except **File System**, **Dtree**, and **Share Name**, other parameters are preset by the system. You can modify them as required.

1. Set advanced properties of the CIFS share. Select **Advanced** in the upper right corner.

   Table 4-37 describes the parameters.

Table 4-37 Advanced parameters of a CIFS share

Parameter	Description
Description	Indicates the description of a CIFS share. **NOTE** The description can be left blank or contain up to 255 characters.
Notify	Determine whether to enable **Notify**. After this function is enabled, a client's operations on a directory, such as adding a sub-directory, adding a file, modifying the directory, and modifying a file, can be detected by other clients that are accessing this directory or the parent directory of this directory. The created or modified directories and files are visible after the page automatically refreshes.
Continuously Available	Determine whether to enable **Continuously Available**. This option provides the SMB continuous availability feature. This feature depends on Oplock which is enabled by default. If Oplock is disabled, choose **Settings** > **File Service** > **CIFS Service** to enable it.
SMB3 Encryption	Specifies whether to enable SMB3 encryption. After this function is enabled, the system encrypts the share to ensure data security, but the performance deteriorates. **NOTICE** Enabling this function affects SMB3 service performance. Check whether this function needs to be enabled. **NOTE** After SMB3 encryption is enabled, only SMB3 clients can access shares by default.
Unencrypted Client Access	After this function is enabled, clients that do not have encryption capabilities can access the share. **NOTICE** After this function is enabled, clients of earlier versions (for example, Windows 7) are allowed to access shares where SMB3 encryption is enabled in plaintext. Check whether this function needs to be enabled. **NOTE** This function takes effect only after the SMB3 encryption function is enabled.
ABE	After ABE is enabled, files and folders that users have no access permission are not displayed. **NOTE** SMB2 and SMB3 support this function but SMB1 does not.

Parameter	Description
Show Snapshot	This function allows clients to show and traverse snapshot directories.

2. Select user or user groups that can access the CIFS share.
   a. In the **Permissions** area, click **Add**.

      The **Add User or User Group** page is displayed.
   b. Select the type of the users or user groups.

      The value can be **Everyone**, **Local Windows authentication user**, **Local Windows authentication user group**, **AD domain user**, or **AD domain user group**.

      - If you select **Local Windows authentication user** or **Local Windows authentication user group**, select the users or user groups to be added from the list.
      - If you select **AD domain user** or **AD domain user group**, enter the names of the users or user groups in **Name**.

        NOTE

        - A domain user name is in the format of *Domain name*|*Domain user name* and a domain user group name is in the format of *Domain name*|*Domain user group name*.
        - 1 to 256 characters are allowed.
        - You can also enter multiple domain user or domain user group names separated by semicolons (;), spaces, or carriage returns.
   c. In **Permission**, select the permission granted for the users or user groups.

      Table 4-38 describes the permissions.

Table 4-38 CIFS share permissions

Permission	Forbidden	Read-Only	Read-Write	Full Control
Viewing files and subdirectories	X[a]	√[b]	√	√
Viewing file contents	X	√	√	√
Running executable files	X	√	√	√
Adding files or subdirectories	X	-[c]	√	√

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

NOTE

- The permission priority from high to low is **Forbidden** > **Full control** > **Read-write** > **Read-only**. The highest permission prevails. If a user is granted with a higher permission than its original one, 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 changed to **Full control** and it can access the CIFS share immediately without re-authentication.
- You can run the **change service cifs administrators_privilege=?** command on the CLI to modify permissions of members in the **Administrators** user group. For details about the command, see *Command Reference* of the desired version. In the command, the value of the **administrators_privilege** parameter can be **admin** (default), **default_group**, or **owner**.

  For local authentication users whose primary user group is **Administrators**, users with different **administrators_privilege** values have different permissions.

  - **admin**: When members in the **Administrators** user group access a shared file system in the storage system, they do not need to be authenticated by share-level ACLs and NT ACLs. They can operate any file in any share with administrator permissions without the need to be authenticated.
  - **default_group**: Members in the **Administrators** user group have the same permissions as members in the **default_group** user group.
  - **owner**: Members in the **Administrators** user group have the permissions to query and set file or directory ACLs and modify file or directory owners. When the group members access shared file systems, they need to be authenticated by directory- or file-level NT ACLs, but do not need to be authenticated by share-level ACLs.

  Modified permissions take effect only after users are re-authenticated on clients.

  You can run the **show service cifs** command on the CLI and check permissions of the **Administrators** user group in the **Administrators Privilege** field.

d. Click **OK**.

The system adds the selected users or user groups to the **Permissions** list.

Step 6 Click **OK**.

----End

4.7.5 Adding a User or User Group

This section describes how to add users or user groups for accessing a share.

Prerequisites

You have created a CIFS share.

Procedure

Step 1 Choose **Services** > **File Service** > **Shares** > **CIFS Shares**.

Step 2 Select the vStore to which the desired CIFS share belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Click **More** on the right of the desired CIFS share and select **Add User or User Group**.

The **Add User or User Group** page is displayed on the right.

NOTE

Alternatively, perform either of the following operations to add users or user groups:

- Click the name of the desired CIFS share. On the page that is displayed, click **Add** in the **Permissions** area.
- Click the name of the desired CIFS share. In the upper right corner of the page that is displayed, click **Operation** and select **Add User or User Group**.

NOTE

For some device models, you can click  in the upper right corner of the page to enable SmartGUI. SmartGUI mines users' historical operation data and builds a configuration parameter recommendation model based on user profiles to recommend configuration parameters for the block service and file service. After SmartGUI is enabled, the system presets the **Type** and **Permission** parameters based on recommendations when you add a user or user group. You can directly use the parameters or modify them as required.

Step 4 Set **Type** for the users or user groups.

The value can be **Everyone**, **Local Windows authentication user**, **Local Windows authentication user group**, **AD domain user**, or **AD domain user group**.

- If you select **Local Windows authentication user** or **Local Windows authentication user group**, select the users or user groups to be added from the list.

  NOTE

  You can click **Create** below the list to create a local Windows authentication user or local Windows authentication user group.

- If you select **AD domain user** or **AD domain user group**, enter the names of the users or user groups in **Name**.

  NOTE

  - If you select **AD domain user** or **AD domain user group**, the system automatically detects whether the AD domain has been configured. If no AD domain is configured, the system prompts you to configure an AD domain first.
  - A domain user name is in the format of *Domain name*|*Domain user name* and a domain user group name is in the format of *Domain name*|*Domain user group name*.
  - **Name** contains 1 to 256 characters. An AD domain user name cannot start with an at sign (@).
  - You can also enter multiple names separated by pressing **Enter**.

Step 5 In **Permission**, select the permission granted for the users or user groups.

Table 4-39 describes the permissions.

Table 4-39 CIFS share permissions

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

NOTE

- The permission priority from high to low is **Forbidden** > **Full control** > **Read-write** > **Read-only**. The highest permission prevails. If a user is granted with a higher permission than its original one, 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 changed to **Full control** and it can access the CIFS share immediately without re-authentication.
- You can run the **change service cifs administrators_privilege=?** command on the CLI to modify permissions of members in the **Administrators** user group. For details about the command, see *Command Reference* of the desired version. In the command, the value of the **administrators_privilege** parameter can be **admin** (default), **default_group**, or **owner**.

  For local authentication users whose primary user group is **Administrators**, users with different **administrators_privilege** values have different permissions.

  - **admin**: When members in the **Administrators** user group access a shared file system in the storage system, they do not need to be authenticated by share-level ACLs and NT ACLs. They can operate any file in any share with administrator permissions without the need to be authenticated.
  - **default_group**: Members in the **Administrators** user group have the same permissions as members in the **default_group** user group.
  - **owner**: Members in the **Administrators** user group have the permissions to query and set file or directory ACLs and modify file or directory owners. When the group members access shared file systems, they need to be authenticated by directory- or file-level NT ACLs, but do not need to be authenticated by share-level ACLs.

  Modified permissions take effect only after users are re-authenticated on clients.

  You can run the **show service cifs** command on the CLI and check permissions of the **Administrators** user group in the **Administrators Privilege** field.

Step 6 Click **OK**.

----End

4.7.6 Modifying the Mapping Rule of a CIFS Homedir Share

This section describes how to modify the mapping rule of a CIFS Homedir share.

Procedure

Step 1 Choose **Services** > **File Service** > **Shares** > **CIFS Shares**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Click the name of the desired CIFS share.

Step 4 On the page that is displayed, select the **Mapping Rules** tab. Click **More** on the right of the desired mapping rule and select **Modify**.

The **Modify Mapping Rule** page is displayed on the right.

Step 5 In **Priority**, set the priority of the mapping rule.

NOTE

- The value of **Priority** ranges from 1 to 1024.
- Mapping rules are sorted in descending order of priorities. A smaller value indicates a higher priority. Rules with the same priority are sorted based on the creation sequence. Users match mapping rules in sequence.

Step 6 Determine whether to enable **Auto Create Path**. After this function is enabled, if a relative path does not exist under the CIFS Homedir share, the system creates the relative path automatically.

NOTE

When **Auto Create Path** is disabled, if the user path does not exist, the current mapping rule fails to be matched, and the system continues to match the next mapping rule.

Step 7 Click **OK**.

Confirm your operation as prompted.

----End

4.7.7 Removing a Mapping Rule from a CIFS Homedir Share

This section describes how to remove a mapping rule from a CIFS Homedir share.

Procedure

Step 1 Choose **Services** > **File Service** > **Shares** > **CIFS Shares**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Click the name of the desired CIFS share.

Step 4 On the page that is displayed, select the **Mapping Rules** tab. Select one or more desired mapping rules and click **Remove**.

NOTE

You can also click **More** on the right of a desired mapping rule and select **Remove**.

Step 5 Confirm your operation as prompted.

----End

4.7.8 Removing a User or User Group from a CIFS Share

This operation enables you to remove a user or user group from a CIFS share.

Prerequisites

You have added a user or user group to a CIFS share.

Procedure

Step 1 Choose **Services** > **File Service** > **Shares** > **CIFS Shares**.

Step 2 Select the vStore to which the desired CIFS share belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Click the name of the desired CIFS share.

Step 4 In the **Permissions** area, select one or more desired users or user groups and click **Remove**.

NOTE

You can also click **More** on the right of a desired user or user group and select **Remove**.

Step 5 Confirm your operation as prompted.

----End

4.7.9 Adding a File Name Extension Filtering Rule

After file name extension filtering rules are configured, the types of files that users access in a CIFS share are controlled.

Procedure

Step 1 Choose **Services** > **File Service** > **Shares** > **CIFS Shares**.

Step 2 Select the vStore to which the desired CIFS share belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Click the path of the CIFS share to go to the details page.

Step 4 On the **File Name Extension Filtering Rules** tab page, click **Add**.

The **Add File Name Extension Filtering Rule** page is displayed on the right.

NOTE

After a file name extension filtering rule is added, it takes effect only after the next CIFS service request (such as refreshing directories, creating files, opening files, renaming files, and querying file attributes) is initiated.

Step 5 Add a file name extension filtering rule.

NOTE

The file name extension filtering rule is valid only for the current share.

1. In **File Name Extension**, specify the file name extensions (file types) to be filtered.

NOTE

- You can enter multiple file name extensions and separate them with commas (,) or carriage returns. The total length (including the separators) cannot exceed 127 characters.
- A single file name extension can contain only digits, letters, spaces, and special characters (!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~). Wildcards ? and * are supported, and wildcard * must be the last character. For example, **txt**, **TXT**, **T?X**, or **Tx***.
- It is recommended that one share have a maximum of seven file name extension filtering rules. A single file name extension filtering rule contains a maximum of 32 characters excluding wildcards. The recommended configurations minimize the adverse impact on CIFS service performance. If the recommended configurations are not used, the CIFS service performance may greatly deteriorate.
- When configuring a file name extension filtering rule, ensure that the rule does not affect the storage of temporary files that may be generated when application software is running. For example, some application software may generate files with the **.tmp** file name extension. In this case, add the **.tmp** extension to the file name extension filtering rule. For details about the temporary file name extensions generated by specific application software, contact the corresponding software vendor.

2. Select a permission rule from the **Rule Type** drop-down list.

   NOTE

   - **Denied only**: Users do not have permissions to access files with the specified extensions.
   - **Allowed only**: Users have permissions to access files with the specified extensions.

3. Select one or more operation types on the right of **Operation Type** to deny or allow users to perform specified operations on files with specified file name extensions.

   NOTE

   For example, set **File Name Extension** to **txt**, **Rule Type** to **Allowed only**, and **Operation Type** to **Read** and **Write**. That is, users can read and write only TXT files.

Step 6 Click **OK**.

----End

4.7.10 Modifying a File Name Extension Filtering Rule

This section describes how to modify a file name extension filtering rule.

Procedure

Step 1 Choose **Services** > **File Service** > **Shares** > **CIFS Shares**.

Step 2 Select the vStore to which the desired CIFS share belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Click the path of the desired CIFS share. The page displaying the share's details is displayed on the right.

Step 4 On the **File Name Extension Filtering Rules** tab page, click **More** on the right of the desired file name extension filtering rule and select **Modify**.

The **Modify File Name Extension Filtering Rule** page is displayed on the right.

NOTE

After a file name extension filtering rule is modified, it takes effect only after the next CIFS service request (such as refreshing directories, creating files, opening files, renaming files, and querying file attributes) is initiated.

Step 5 Modify an existing file name extension filtering rule.

NOTE

The file name extension filtering rule is valid only for the current share.

1. In **File Name Extension**, specify the file name extensions (file types) to be filtered.

   NOTE

   - You can enter multiple file name extensions and separate them with commas (,) or carriage returns. The total length (including the separators) cannot exceed 127 characters.
   - A single file name extension can contain only digits, letters, spaces, and special characters (!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~). Wildcards ? and * are supported, and wildcard * must be the last character. For example, **txt**, **TXT**, **T?X**, or **Tx***.
   - It is recommended that one share have a maximum of seven file name extension filtering rules. A single file name extension filtering rule contains a maximum of 32 characters excluding wildcards. The recommended configurations minimize the adverse impact on CIFS service performance. If the recommended configurations are not used, the CIFS service performance may greatly deteriorate.
   - When configuring a file name extension filtering rule, ensure that the rule does not affect the storage of temporary files that may be generated when application software is running. For example, some application software may generate files with the **.tmp** file name extension. In this case, add the **.tmp** extension to the file name extension filtering rule. For details about the temporary file name extensions generated by specific application software, contact the corresponding software vendor.

2. Select a permission rule from the **Rule Type** drop-down list.

   NOTE

   - **Denied only**: Users do not have permissions to access files with the specified extensions.
   - **Allowed only**: Users have permissions to access files with the specified extensions.

3. Select one or more operation types on the right of **Operation Type** to deny or allow users to perform specified operations on files with specified file name extensions.

   NOTE

   For example, set **File Name Extension** to **txt**, **Rule Type** to **Allowed only**, and **Operation Type** to **Read** and **Write**. That is, users can read and write only TXT files.

Step 6 Click **OK**.

----End

4.7.11 Removing a File Name Extension Filtering Rule

This section describes how to remove a file name extension filtering rule.

Procedure

Step 1 Choose **Services** > **File Service** > **Shares** > **CIFS Shares**.

Step 2 Select the vStore to which the desired CIFS share belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Click the path of the CIFS share to go to the details page.

Step 4 On the **File Name Extension Filtering Rules** tab page, select one or more file name extension filtering rules to be deleted and click **Remove**.

NOTE

You can also click **More** on the right of a desired file name extension filtering rule and select **Remove**.

Step 5 Confirm your operation as prompted.

----End

4.7.12 Adding an Accessible IP Address or IP Address Segment (Applicable to 6.1.5 and Later Versions)

This section describes how to add an IP address or IP address segment that can be used to access a CIFS share.

Context

- If no accessible IP address or IP address segment is configured, any IP address can access the shared directory.
- If accessible IP addresses or IP address segments are configured, only the configured IP addresses or IP address segments are allowed to access the shared directory.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Services** > **File Service** > **Shares** > **CIFS Shares**.

Step 3 Select the vStore to which the desired CIFS share belongs from the **vStore** drop-down list in the upper left corner.

Step 4 Click the path of the CIFS share to go to the details page.

Step 5 On the **Accessible IP Addresses/Address Segments** tab, click **Add**.

The **Add Accessible IP Address/Address Segment** page is displayed on the right.

Step 6 In **IP Address/Address Segment**, specify the IP addresses or IP address segments.

NOTE

- You can enter multiple IP addresses or IP address segments and separate them with commas (,) or by pressing **Enter**.
- The format of IP address segments is as follows:

  IPv4 address/mask or IPv6 address/prefix

  For example, **192.168.1.100/16** or **192.168.1.10-192.168.1.11/30**. A mask ranges from 1 to 32, and a prefix ranges from 1 to 128.
- The IP address or IP address segment can be:

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

  An IP address segment, for example, 192.168.1.100/1 or 192.168.1.10-192.168.1.11/30.
- The start and end IP addresses of an IP address segment must be on the same network segment.
- You can enter a maximum of 1024 IP addresses or IP address segments.

Step 7 Click **OK**.

Confirm your operation as prompted.

----End

4.7.13 Modifying an Accessible IP Address or IP Address Segment (Applicable to 6.1.5 and Later Versions)

This section describes how to modify the IP addresses or IP address segments that can be used to access a CIFS share.

Procedure

Step 1 Choose **Services** > **File Service** > **Shares** > **CIFS Shares**.

Step 2 Select the vStore to which the desired CIFS share belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Click the path of the CIFS share to go to the details page.

Step 4 On the **Accessible IP Addresses/Address Segments** tab, find the desired IP address or address segment, click **More**, and select **Modify**.

The **Modify Accessible IP Address/Address Segment** page is displayed on the right.

Step 5 In **IP Address/Address Segment**, specify the new IP addresses or IP address segments.

NOTE

- The format of IP address segments is as follows:

  IPv4 address/mask or IPv6 address/prefix

  For example, **192.168.1.100/16** or **192.168.1.10-192.168.1.11/30**. A mask ranges from 1 to 32, and a prefix ranges from 1 to 128.
- The IP address or IP address segment can be:

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

  An IP address segment, for example, 192.168.1.100/1 or 192.168.1.10-192.168.1.11/30.
- The start and end IP addresses of an IP address segment must be on the same network segment.

Step 6 Click **OK**.

----End

4.7.14 Removing an Accessible IP Address or IP Address Segment (Applicable to 6.1.5 and Later Versions)

This section describes how to remove the IP addresses or IP address segments that can be used to access a CIFS share.

Procedure

Step 1 Log in to DeviceManager.

Step 2 Choose **Services** > **File Service** > **Shares** > **CIFS Shares**.

Step 3 Select the vStore to which the desired CIFS share belongs from the **vStore** drop-down list in the upper left corner.

Step 4 Click the path of the CIFS share to go to the details page.

Step 5 On the **Accessible IP Addresses/Address Segments** tab, select the desired IP address or address segment and click **Remove**.

NOTE

Alternatively, click **More** on the right of the desired IP address or address segment and select **Remove**.

Step 6 Confirm your operation as prompted.

----End

4.7.15 Deleting a CIFS Share

This operation enables you to delete a CIFS share. After the CIFS share is deleted, users can no longer access it.

Prerequisites

No services are running on the CIFS share.

Procedure

Step 1 Choose **Services** > **File Service** > **Shares** > **CIFS Shares**.

Step 2 Select the vStore to which the desired CIFS shares belong from the **vStore** drop-down list in the upper left corner.

Step 3 Select one or more desired CIFS shares and click **Delete**.

NOTE

Alternatively, perform either of the following operations to delete a CIFS share:

- Click **More** on the right of a desired CIFS share and select **Delete**.
- Click the name of a desired CIFS share. In the upper right corner of the page that is displayed, click **Operation** and select **Delete**.

Step 4 Confirm your operation as prompted.

----End

4.8 Managing HTTP Shares

The storage system supports HTTPS-based file system sharing. With the HTTPS service enabled, you can share a file system in HTTPS mode.

4.8.1 Configuring the HTTP Service

This operation enables you to start the HTTP service by modifying the configuration file.

Prerequisites

- Configure the listening port of the front-end service IP address of the container to control the HTTP and HTTPS services:
  - If port 80 of the front-end service IP address of the container is listened on, the HTTP service can be enabled.
  - If port 443 of the front-end service IP address of the container is listened on, the HTTPS service can be enabled.
  - If ports 80 and 443 of the front-end service IP address of the container are listened on, the HTTP and HTTPS services can be enabled at the same time.
- As configured in **4.8.3 (Optional) Configuring the Firewall**, the ports allowed by the firewall to be accessed must be consistent with the listening ports of the front-end service IP address of the container.

Configuration Process

Step 1 Log in to the CLI as an administrator or super administrator.

Step 2 Access the container where the HTTPS service is running by running the following command:

change container_application view pod_name=http-pod-0 namespace=http

NOTE

To obtain the value of **pod_name**:

In versions earlier than 6.1.5, run the **show container_application general name=http-chart** command.

In 6.1.5 and later versions, run the **show container_application general name=http-chart namespace=http** command.

Step 3 Configure the listening port number.

1. Run the **ifconfig** command to check the front-end service IP address of the container.

   NOTE

   The front-end service IP address of the container is determined by the network segment bound to the network plane during the application creation:

   - When you configure the network plane, if the IP segment specified by the **ipv4_subset_range** or **ipv6_subset_range** parameter contains only one IP address, this IP address is the front-end service IP address of the container.
   - When you configure the network plane, if the IP segment specified by the **ipv4_subset_range** or **ipv6_subset_range** parameter contains multiple IP addresses, one of the IP addresses is randomly selected as the front-end service IP address of the container.

2. Run the **vi prohttpd/conf/httpd.conf** command to open the configuration file of the HTTPS service.

   a. Press **i** to enter the editing mode.

   b. Change the IP address following **Listen** to the front-end service IP address of the container with the port number, and set the port number to **80** used by the HTTP service.

   c. Type **:wq** and press **Enter** to save the settings and exit.

   The command output is as follows:

```
#Listen 80
#Listen 443

Listen x.x.0.13:80
Listen [1::99]:80
Listen x.x.0.13:443
Listen [1::99]:443

#
# Dynamic Shared Object (DSO) Support
```


NOTE

- Configure the listening port of the front-end service IP address of the container to control the HTTP and HTTPS services:
  - If port 80 of the front-end service IP address of the container is listened on, the HTTP service can be enabled.
  - If port 443 of the front-end service IP address of the container is listened on, the HTTPS service can be enabled.
  - If ports 80 and 443 of the front-end service IP address of the container are listened on, the HTTP and HTTPS services can be enabled at the same time.
- As configured in **4.8.3 (Optional) Configuring the Firewall**, the ports allowed by the firewall to be accessed must be consistent with the listening ports of the front-end service IP address of the container.

3. Run the **httpd -k restart** command to enable the modified HTTPS service configuration.

Step 4 Run the **vi /mnt/nfs/http/net_cnet_firewall.ini** command to open the firewall configuration file.

1. Press **i** to enter the editing mode.
2. Type **80** after **tcp_allow_ports** to allow the firewall to access IPv4 port 80.
3. Then, type **:wq** and press **Enter** to save the settings and exit.

   The command output is as follows:

```
#such as:"21,53,200:300,305"
tcp_allow_ports="443, 80"
udp_allow_ports=""
tcp_allow_ports_ipv6="443, 80"
udp_allow_ports_ipv6=""
```

Table 4-40 Parameter description

Parameter	Description
tcp_allow_ports	Number of the IPv4 port that can be accessed when the TCP protocol is used to transmit data.
udp_allow_ports	Number of the IPv4 port that can be accessed when the UDP protocol is used to transmit data.
tcp_allow_ports_ipv6	Number of the IPv6 port that can be accessed when the TCP protocol is used to transmit data.
udp_allow_ports_ipv6	Number of the IPv6 port that can be accessed when the UDP protocol is used to transmit data.

Step 5 Run the **cd /http/** command to go to the **/http/** directory.

Step 6 Run the **sh /http/startup.sh firewall** command to make the firewall configuration changes to take effect.

NOTE

- Common configuration items of the HTTPS service are managed by the files **httpd.conf**, **httpd-ssl.conf**, and **httpd-dav.conf**. You can modify these configuration files to manage the HTTPS service.
- The configuration files of the HTTPS service are stored in the **/mnt/nfs/http** directory by default. You can modify the configuration files in this directory to make the configuration result persistent.
- This section describes only some basic configurations of the HTTP service. For details about the HTTP service configurations, see related commands of the open-source software httpd.

----End

4.8.2 Managing Common HTTPS Service Items

This section describes how to manage common HTTPS service items using a configuration file and configure a firewall for them.

Configuration Process

Step 1 Log in to the CLI as an administrator or super administrator.

Step 2 Access the container where the HTTPS service is running by running the following command:

change container_application view pod_name=http-pod-0 namespace=http

NOTE

To obtain the value of **pod_name**:

In versions earlier than 6.1.5, run the **show container_application general name=http-chart** command.

In 6.1.5 and later versions, run the **show container_application general name=http-chart namespace=http** command.

Step 3 (Optional) Manage the WebDAV service.

1. Run the **vi /mnt/nfs/http/prohttpd/conf/extra/http-dav.conf** command to open the **http-dav.conf** configuration file of the HTTPS service.
2. Press **i** to enter the editing mode.
3. Manage the WebDAV service by modifying the parameter values after the **Directory** configuration item.
4. Then, type **:wq** and press **Enter** to save the settings and exit.

   The command output is as follows:

```
<Directory "/mnt/nfs/http/prohttpd/uploads/">
    Dav On
    Order Allow,Deny
    Allow from all
    Options Indexes SymLinksIfOwnerMatch
    AllowOverride AuthConfig
    AuthType Digest
    AuthName DAV-upload
    AuthUserFile "/mnt/nfs/http/prohttpd/user.passwd"
    Require valid-user
    <LimitExcept GET POST PUT OPTIONS PROFIND REPORT HEAD CONNECT PROPPATCH MKCOL
COPY MOVE LOCK UNLOCK TRACE>
        Require valid-user
```



```
    </LimitExcept>
</Directory>
```

Table 4-41 Parameter description

Parameter	Description
Directory	Used to set the page access attributes for the root directory.
Dav	Whether to enable the WebDAV service.
Order	The default access state and the order in which the **Allow** and **Deny** parameters take effect.
Allow	Hosts that can access the zone of the server.
Options	Available functions in the directory.
AllowOverride	User access authentication.
AuthType	Authentication mode.
AuthName	Prompt name of the security zone.
AuthUserFile	Method of storing access authentication. The default value is a system file.
Require	Restricts user access.
LimitExcept	When the owner and owner group of the link file are the same as those of the original file, the original file to which the symbolic link points can be followed.

5. Run the **httpd -k restart** command to reload the configuration file for the modification to take effect.

   NOTE

   - Common configuration items of the HTTPS service are managed by the files **httpd.conf**, **httpd-ssl.conf**, and **httpd-dav.conf**. You can modify these configuration files to manage the HTTPS service.
   - The configuration files of the HTTPS service are stored in the **/mnt/nfs/http** directory by default. You can modify the configuration files in this directory to make the configuration result persistent.
   - This section describes only some basic configurations of the HTTPS service. For details about the HTTPS service configurations, see related commands of the open-source software httpd.

----End

4.8.3 (Optional) Configuring the Firewall

This section describes how to manage the firewall of the HTTPS service using the configuration file.

Configuration Process

Step 1 Run the **vi /mnt/nfs/http/net_cnet_firewall.ini** command to open the firewall configuration file. Press **i** to enter the editing mode and set parameters. Then, type **:wq** and press **Enter** to save the settings and exit.

The command output is as follows:

```
#such as:"21,53,200:300,305"
tcp_allow_ports="443"
udp_allow_ports=""
tcp_allow_ports_ipv6=""
udp_allow_ports_ipv6=""
```

Table 4-42 Parameter description

Parameter	Description
tcp_allow_ports	Number of the IPv4 port that can be accessed when the TCP protocol is used to transmit data.
udp_allow_ports	Number of the IPv4 port that can be accessed when the UDP protocol is used to transmit data.
tcp_allow_ports_ipv6	Number of the IPv6 port that can be accessed when the TCP protocol is used to transmit data.
udp_allow_ports_ipv6	Number of the IPv6 port that can be accessed when the UDP protocol is used to transmit data.

Step 2 Run the **cd /http/** command to go to the **/http/** directory.

Step 3 Run the **sh /http/startup.sh firewall** command for the firewall configuration changes to take effect.

----End

4.9 Managing FTP Shares

After the FTPS server function is configured on the device, users can securely access the remote device through the web page.

4.9.1 Configuring the FTP Service

This operation enables you to start the FTP service by modifying the configuration file.

Configuration Process

Step 1 Log in to the CLI as an administrator or super administrator.

Step 2 Access the container where the FTPS service is running by running the following command:

change container_application view pod_name=ftp-pod-0 namespace=ftp

NOTE

To obtain the value of **pod_name**:

In versions earlier than 6.1.5, run the **show container_application general name=ftp-chart** command.

In 6.1.5 and later versions, run the **show container_application general name=ftp-chart namespace=ftp** command.

Step 3 Open the configuration file of the FTPS service by running the **vi /mnt/nfs/etc/config/proftpd.conf** command.

Press **i** to enter the editing mode and set parameters. Then, type **:wq** and press **Enter** to save the settings and exit.

Step 4 Comment out the configuration related to the FTPS service in the configuration file.

The command output is as follows:

```
#TLSEngine on
#TLSLog /mnt/nfs/etc/log/tls.log
#TLSProtocol TLSv1.2
#TLSRequired on
#TLSVerifyClient off
#TLSRSACertificateFile /mnt/cert/FTPS_Cert.crt
#TLSRSACertificateKeyFile /mnt/cert/FTPS_PriKey.key
```

Step 5 Run the **startup.sh reload** command to reload the configuration file for the modification to take effect.

NOTE

This section describes only some basic configurations of the FTPS service. For details about the FTPS service configurations, see related commands of the open-source software ftpasswd.

----End

4.9.2 Managing Users and Permissions

This operation ensures that users use the FTPS service within their permission scopes, protecting the security of user information and the FTPS service.

4.9.2.1 Managing Users

This operation ensures that users use the FTPS service within their permission scopes, protecting the security of user information and the FTPS service.

Configuration Process

Step 1 Log in to the CLI as an administrator or super administrator.

Step 2 Access the container where the FTPS service is running by running the following command:

change container_application view pod_name=ftp-pod-0 namespace=ftp

NOTE

To obtain the value of **pod_name**:

In versions earlier than 6.1.5, run the **show container_application general name=ftp-chart** command.

In 6.1.5 and later versions, run the **show container_application general name=ftp-chart namespace=ftp** command.

Step 3 Perform common user management operations.

- Create the home directory of the user.

  Run **mkdir /mnt/nfs/ftpuser1** to create the home directory **ftpuser1** for the user in the **/mnt/nfs/** directory.

  Run the **chmod 777 /mnt/nfs/ftpuser1** command to grant read, write, and execute permissions to all users in the root directory **ftpuser1**. The system performs permission management to control the operation permissions and scope of users. For details, see section **4.9.2.4 Managing User Permissions**.

- Create a user.

  Run the **ftpasswd --sha512 --passwd --file=/mnt/nfs/etc/config/ftpd.passwd --name=user1 --home=/mnt/nfs/ftpuser1 --uid=666 --shell=/usr/sbin/nologin** command to create a user named user1. Enter the password as prompted. The password will be converted into an encrypted character string and saved in the system.

  NOTE

  - The password must meet the following requirements:
    - The password contains at least eight characters.
    - The password cannot be the same as the account name.
    - The password must contain at least four types of the following characters: uppercase letters, lowercase letters, digits, and special characters. The special characters include `~!@#$%^&*()-_=+|[{}];:'",<.>/? and spaces.
  - The parameters are described as follows:
    - **--sha512**: Use the SHA-512 algorithm for encrypting passwords.
    - **--passwd**: Create a file in the passwd(5) format.
    - **--file**: Write output to the specified file.
    - **--name**: Name of the user account.
    - **--home**: Home directory of the user.
    - **--uid**: Numerical user ID.
    - **--shell**: Shell of the user.

- Delete a user.

  Run **ftpasswd --delete-user --name=user1 --passwd --file=/mnt/nfs/etc/config/ftpd.passwd** to delete user1.

NOTE

The parameters are described as follows:

- **--delete-user**: Remove the user.
- **--name**: Name of the user account.
- **--passwd**: Create a file in the passwd(5) format.
- **--file**: Write output to the specified file.

- Change the user password.

  Run **ftpasswd --change-password --passwd --file=/mnt/nfs/etc/config/ftpd.passwd --name=user1** to change the password of user1.

  NOTE

  The parameters are described as follows:

  - **--change-password**: Update the user password.
  - **--passwd**: Create a file in the passwd(5) format.
  - **--file**: Write output to the specified file.
  - **--name**: Name of the user account.

- Change the home directory of a user.

  Run **ftpasswd --change-home --passwd --file=/mnt/nfs/etc/config/ftpd.passwd --name=user1 --home=/mnt/nfs/ftptest1** to change the home directory of user1.

  NOTE

  The parameters are described as follows:

  - **--change-home**: Update the home directory of the user.
  - **--passwd**: Create a file in the passwd(5) format.
  - **--file**: Write output to the specified file.
  - **--name**: Name of the user account.
  - **--home**: Home directory of the user.

----End

4.9.2.2 Managing User Groups

This operation ensures that user groups use the FTPS service within their permission scopes, protecting the security of user information and the FTPS service.

Configuration Process

Step 1 Log in to the CLI as an administrator or super administrator.

Step 2 Access the container where the FTPS service is running by running the following command:

change container_application view pod_name=ftp-pod-0 namespace=ftp

NOTE

To obtain the value of **pod_name**:

In versions earlier than 6.1.5, run the **show container_application general name=ftp-chart** command.

In 6.1.5 and later versions, run the **show container_application general name=ftp-chart namespace=ftp** command.

Step 3 Perform common group management operations.

- Create a group.

  Run **ftpasswd --group --name=Group1 -gid=666 --file=/mnt/nfs/etc/config/ftpd.group** to create a group named Group1.

  NOTE

  The parameters are described as follows:
  - **--group**: Specify a group.
  - **--name**: Name of the group.
  - **-gid**: Primary group ID.
  - **--file**: Write output to the specified file.

- Delete a group.

  Run **ftpasswd --delete-group --group --name=Group1 --file=/mnt/nfs/etc/config/ftpd.group** to delete the group named Group1.

  NOTE

  The parameters are described as follows:
  - **--delete-group**: Remove the entry for the given group name from the file.
  - **--group**: Specify a group.
  - **--name**: Name of the group.
  - **--file**: Write output to the specified file.

- Add a user to a group.

  Run **ftpasswd --group --name=Group1 --add-member=user1 --file=/mnt/nfs/etc/config/ftpd.group** to add user1 to Group1.

  NOTE

  The parameters are described as follows:
  - **--group**: Specify a group.
  - **--name**: Name of the group.
  - **--add-member**: Add the specified member to the file for the given group name.
  - **--file**: Write output to the specified file.

- Remove a member from a group.

  Run **ftpasswd --group --file=/mnt/nfs/etc/config/ftpd.group --name=Group1 --delete-member=user1** to remove user1 from Group1.

NOTE

The parameters are described as follows:

- **--group**: Specify a group.
- **--file**: Write output to the specified file.
- **--name**: Name of the group.
- **--delete-member**: Remove the named member from the given group name from the file.

----End

4.9.2.3 Managing Anonymous Users

This operation ensures that anonymous users use the FTPS service within their permission scopes, protecting the security of user information and the FTPS service.

Configuration Process

Step 1 Log in to the CLI as an administrator or super administrator.

Step 2 Access the container where the FTPS service is running by running the following command:

change container_application view pod_name=ftp-pod-0 namespace=ftp

NOTE

To obtain the value of **pod_name**:

In versions earlier than 6.1.5, run the **show container_application general name=ftp-chart** command.

In 6.1.5 and later versions, run the **show container_application general name=ftp-chart namespace=ftp** command.

Step 3 Perform common operations of anonymous users.

1. Open the configuration file of the FTPS service by running the **vi /mnt/nfs/etc/config/proftpd.conf** command.

   Press **i** to enter the editing mode and set parameters. Then, type **:wq** and press **Enter** to save the settings and exit.

2. In the configuration file, modify values of the parameters after **<Anonymous />** to configure common operations for anonymous users.

   FTP clients are allowed to access the FTPS shared space with the user name **private**. This sample configuration allows clients to change, list, and read all directories, but denies write access of any kind.

   The command output is as follows:

```
<Anonymous /mnt/nfs>
    User private
    Group private
    <Directory *>
        <Limit WRITE>
            DenyAll
        </Limit>
    </Directory>
</Anonymous>
```

----End

4.9.2.4 Managing User Permissions

To prevent misoperations from compromising service system stability and service data security, the system controls user permissions through permission management.

Configuration Process

Step 1 Log in to the CLI as an administrator or super administrator.

Step 2 Access the container where the FTPS service is running by running the following command:

change container_application view pod_name=ftp-pod-0 namespace=ftp

NOTE

To obtain the value of **pod_name**:

In versions earlier than 6.1.5, run the **show container_application general name=ftp-chart** command.

In 6.1.5 and later versions, run the **show container_application general name=ftp-chart namespace=ftp** command.

Step 3 Perform common operations of user permissions.

1. Open the configuration file of the FTPS service by running the **vi /mnt/nfs/etc/config/proftpd.conf** command.

   Press **i** to enter the editing mode and set parameters. Then, type **:wq** and press **Enter** to save the settings and exit.

2. In the configuration file, modify values of the parameters after **<Directory />** to configure common operations of user permissions.

   This sample configuration does not allow users to delete files in the **/mnt/nfs/** directory.

   The command output is as follows:

```
AuthUserFile /usr/local/proftpd/ftpd.passwd
<Directory "/mnt/nfs/">
   <Limit DELE>
      DenyAll
   </Limit>
</Directory>
```


NOTE

1. **Directory** specifies the working directory of a user.
2. **Limit** specifies the user permissions. The values are as follows:
   - CWD: Change the directory.
   - MKD/XMKD: Create a directory.
   - RNFR/RNTO: Rename a directory.
   - DELE: Delete a file.
   - RMD/XRMD: Delete a directory.
   - RETR: Download.
   - STOR: Upload.
   - LOGIN: Log in.
   - READ: Includes RETR, SITE, SIZE, and STAT.
   - WRITE: Includes APPE, DELE, MKD, RMD, RNTO, STOR, XMKD and XRMD.
   - DIRS: Includes DUP, CWD, LIST, MDTM, NLST, PWD, RNFR, XCUP, XCWD and XPWD.
   - ALL: Includes READ, WRITE, and DIRS.
3. Parameters specify users who are allowed or forbidden to perform operations. The options are as follows:
   - AllowUser: Allows a user.
   - DenyUser: Forbids a user.
   - AllowGroup: Allows a user group.
   - DenyGroup: Forbids a user group.
   - AllowAll: Allow all users.
   - DenyAll: Forbid all users.

----End

4.9.3 Managing Common FTPS Service Items

This section describes how to manage the FTPS service using the configuration file.

Configuration Process

Step 1 Log in to the CLI as an administrator or super administrator.

Step 2 Access the container where the FTPS service is running by running the following command:

change container_application view pod_name=ftp-pod-0 namespace=ftp

NOTE

To obtain the value of **pod_name**:

In versions earlier than 6.1.5, run the **show container_application general name=ftp-chart** command.

In 6.1.5 and later versions, run the **show container_application general name=ftp-chart namespace=ftp** command.

Step 3 Run the following command to open the configuration file of the FTPS service:

vi /mnt/nfs/etc/config/proftpd.conf

The command output is as follows:

```
ServerName      "FTP Server"
ServerType      standalone
DefaultServer     on
ServerIdent             off
# Port 21 is the standard FTP port.
Port        21
# Don't use IPv6 support by default.
UseIPv6       off
# Umask 022 is a good standard umask to prevent new dirs and files
# from being group and world writable.
Umask       000
# To prevent DoS attacks, set the maximum number of child processes
# to 30.  If you need to allow more than 30 concurrent connections
# at once, simply increase this value.  Note that this ONLY works
# in standalone mode, in inetd mode you should use an inetd server
# that allows you to limit maximum number of processes per service
# (such as xinetd).
MaxInstances      512
# Set the user and group under which the server will run.
User        root
Group       root
# To cause every FTP user to be "jailed" (chrooted) into their home
# directory, uncomment this line.
DefaultRoot ~
# Normally, we want files to be overwriteable.
AllowOverwrite    on
# Bar use of SITE CHMOD by default
<Limit SITE_CHMOD>
  DenyAll
</Limit>
SystemLog                    /mnt/nfs/etc/log/proftp.log
TransferLog                  /mnt/nfs/etc/log/transfer.log
RequireValidShell off          # important for virtual account.
AuthUserFile                 /mnt/nfs/etc/config/ftpd.passwd
AuthGroupFile                  /mnt/nfs/etc/config/ftpd.group
AllowStoreRestart              on
AllowRetrieveRestart             on
AllowOverwrite                 on
PassivePorts                  51000 52000
MaxClientsPerHost       1
MaxClientsPerUser       1
MaxClients                  10
TimeoutIdle                 10
AllowForeignAddress    on
CommandBufferSize   SocketOptions rcvbuf 32768 sndbuf 32768
UseEncoding                on
TransferRate STOR 150 user tom
</IfModule>
TLSEngine on
TLSLog /mnt/nfs/etc/log/tls.log
TLSProtocol TLSv1.2
TLSRequired on
TLSVerifyClient off
TLSRSACertificateFile /mnt/cert/FTPS_Cert.crt
TLSRSACertificateKeyFile /mnt/cert/FTPS_PriKey.key
```

Table 4-43 Parameter description

Parameter	Description
ServerName	Name of a server. [Example] Serve_1

Parameter	Description
ServerType	Server running mode. [Example] The value can be **standalone** or **dameon**. **standalone**: working independently. **dameon**: being monitored.
DefaultServer	Whether the server is used as the default server. [Example] The value can be **on** or **off**.
ServerIdent	Whether to display client connection information. [Example] The value can be **on** or **off**.
Port	FTP listening port. [Example] Port number. The default value is 21.
UseIPv6	Whether IPv6 is supported. [Example] The value can be **on** or **off**.
Umask	Permission mask for users to upload files. [Example] Mask number, for example, 022.
MaxInstances	Maximum number of concurrent connections. [Example] Number of connections, for example, 30.
User	User account for starting the server. [Example] User_1
Group	Group account used for starting the server. [Example] Group_1
DefaultRoot	Root directory of the default shared directory. [Example] Directory name, for example, /ftp.
AllowOverwrite	Whether to allow users to use files to overwrite permissions. [Example] The value can be **on** or **off**.

Parameter	Description
SystemLog	Path to which logs are redirected. [Example] Path name, for example, **/var/log/proftp.log**.
TransferLog	Path to the transfer logs. [Example] File path name, for example, **/var/log/proftp.log**.
RequireValidShell	Whether to allow connections based on **/etc/shells**. [Example] The value can be **on** or **off**.
AuthUserFile	User data file used to replace the system user. [Example] File path name, for example, **/mnt/nfs/etc/config/ftpd.passwd**.
AuthGroupFile	User group data file used to replace the system group. [Example] File path name, for example, **/mnt/nfs/etc/config/ftpd.group**.
AllowStoreRestart	Whether to allow the client to resume uploads. [Example] The value can be **on** or **off**.
AllowRetrieveRestart	Whether to allow the client to resume downloads. [Example] The value can be **on** or **off**.
AllowOverwrite	Whether existing files can be overwritten. [Example] The value can be **on** or **off**.
PassivePorts	Application scope where the FTP data port can be used. [Example] 51000.
MaxClientsPerHost	Maximum number of clients allowed to connect per host. [Example] Number of connections, for example, 1.

Parameter	Description
MaxClientsPerUser	Maximum number of connections per user. [Example] Number of connections, for example, 1.
MaxClients	Maximum number of authenticated clients. [Example] The value can be **none** or a number, for example, **10**.
TimeoutIdle	Idle connection timeout, in seconds. [Example] for example, 10.
AllowForeignAddress	Whether to allow clients to transmit foreign data connection addresses. [Example] The value can be **on** or **off**.
CommandBufferSize	Maximum command length, in bytes. [Example] SocketOptions rcvbuf 32768 sndbuf 32768. **Rcvbuf** indicates received command and **sndbuf** indicates sent command.
UseEncoding	Character set encoding of the client. [Example] **on**: indicates utf-8 and cannot be changed. The value can also be another encoding format, for example, **gbk**.
TransferRate	Upload and download transfer rates. [Example] TransferRate STOR 150 user tom. TransferRate RETR 100 user tom. The upload rate of user **tom** is limited to 150 KB/s, and the download rate is limited to 100 KB/s.
TLSEngine	Whether to enable TLS/SSL connections. [Example] The value can be **on** or **off**.
TLSLog	A log file for TLS module's reporting on a per-server basis. [Example] File path name, for example, **/mnt/nfs/etc/log/tls.log**.

Parameter	Description
TLSProtocol	SSL/TLS protocol version. [Example] Protocol version, for example, TLSv1.2.
TLSRequired	Configure TLS for data and sessions. [Example] The value can be **on**, **off**, **ctrl**, **data**, **auth**, or **auth +data**.
TLSVerifyClient	Configure how to handle certificates presented by clients. [Example] The value can be **on** or **off**.
TLSRSACertificateFile	File containing the RSA certificate. [Example] File name, for example, **/mnt/cert/FTPS_Cert.crt**.
TLSRSACertificateKey-File	File containing the private RSA key. [Example] File name, for example, **/mnt/cert/FTPS_PriKey.key**.

NOTE

This section describes only some basic configurations of the FTPS service. For details about the FTPS service configurations, see related commands of the open-source software ftpasswd.

Step 4 (Optional) Manage the SSL modes of the FTPS service using the configuration file.

The FTPS service supports the following SSL modes:

- Implicit mode: When the FTP client connects to the server, the server automatically establishes a secure connection.
- Explicit mode: After a connection is set up between an FTP client and an FTP server, the FTP client explicitly instructs the FTP server to initialize the corresponding secure connection by running the **AUTH SSL** or **AUTH TLS** command.

  NOTE

  By default, the SSL mode of the FTPS service is the explicit mode. To configure the implicit mode, perform the following steps:

  a. Access the container where the FTPS service is running by running the following command:

     change container_application view pod_name=ftp-pod-0 namespace=ftp

NOTE

To obtain the value of **pod_name**:

In versions earlier than 6.1.5, run the **show container_application general name=ftp-chart** command.

In 6.1.5 and later versions, run the **show container_application general name=ftp-chart namespace=ftp** command.

b. Run the following command to open the configuration file of the FTPS service:

vi /mnt/nfs/etc/config/proftpd.conf

In the configuration file, add the following parameters after the configuration item **TLSEngine on** to configure the SSL mode:

```
TLSOptions UseImplicitSSL
Port 990
```

NOTE

- **TLSOptions UseImplicitSSL** indicates the implicit mode.
- **Port** indicates the port used for the connection. The value must be the same as the implicit SSL connection port of the client.

c. Run the **startup.sh reload** command to reload the configuration file for the modification to take effect.

d. Enable the firewall to access IPv4 port 990.

i. Press **i** to enter the editing mode.

ii. Type **990** after **tcp_allow_ports** to allow the firewall to access IPv4 port 990.

iii. Then, type **:wq** and press **Enter** to save the settings and exit.

The command output is as follows:

```
#such as:"21,53,200:300,305"
tcp_allow_ports="20,21,990,51000:52000"
udp_allow_ports=""
tcp_allow_ports_ipv6=""
udp_allow_ports_ipv6=""
```

Table 4-44 Parameter description

Parameter	Description
tcp_allow_ports	Number of the IPv4 port that can be accessed when the TCP protocol is used to transmit data.
udp_allow_ports	Number of the IPv4 port that can be accessed when the UDP protocol is used to transmit data.

Parameter	Description
tcp_allow_ports_ipv6	Number of the IPv6 port that can be accessed when the TCP protocol is used to transmit data.
udp_allow_ports_ipv6	Number of the IPv6 port that can be accessed when the UDP protocol is used to transmit data.

iv. Run the **cd /ftp/** command to go to the **/ftp/** directory.

v. Run the **startup.sh firewall** command to make the firewall configuration changes to take effect.

----End

4.9.4 (Optional) Configuring a Firewall

This section describes how to configure a firewall for the FTPS service.

Configuration Process

Step 1 Run the **vi /mnt/nfs/etc/config/net_cnet_firewall.ini** command to open the firewall configuration file. Press **i** to enter the editing mode and set parameters. Then, type **:wq** and press **Enter** to save the settings and exit.

The command output is as follows:

```
#such as:"21,53,200:300,305"
tcp_allow_ports="20,21,989:990,51000:52000"
udp_allow_ports=""
tcp_allow_ports_ipv6="20,21,989:990,51000:52000"
udp_allow_ports_ipv6=""
```

Table 4-45 Parameter description

Parameter	Description
tcp_allow_ports	Number of the IPv4 port that can be accessed when the TCP protocol is used to transmit data.
udp_allow_ports	Number of the IPv4 port that can be accessed when the UDP protocol is used to transmit data.
tcp_allow_ports_ipv6	Number of the IPv6 port that can be accessed when the TCP protocol is used to transmit data.
udp_allow_ports_ipv6	Number of the IPv6 port that can be accessed when the UDP protocol is used to transmit data.

Step 2 Run the **cd /ftp/** command to go to the **/ftp/** directory.

Step 3 Run the **startup.sh firewall** command to make the firewall configuration changes to take effect.

----End

4.10 Managing User Mappings

User mappings enable you to access shares across different operating systems by using the mappings created locally or in the IDMU domain.

4.10.1 Viewing User Mappings

This operation enables you to view created user mappings.

Context

- On the user mapping management page, you can click to refresh user mapping information.
- On the user mapping management page, you can click next to a parameter and enter a keyword to search for the required user mappings.
- On the user mapping management page, you can click to select the user mapping parameters you want to view.
- On the user mapping management page, you can click or next to a parameter to change the display order of user mappings.

Procedure

Step 1 Choose **Services** > **File Service** > **Authentication Users** > **User Mappings**.

Step 2 Select a vStore from the **vStore** drop-down list in the upper left corner.

Step 3 View information about the user mappings of the selected vStore in the function pane. **Table 4-46** describes the parameters.

Table 4-46 User mapping parameters

Parameter	Description
ID	ID of a user mapping.
Source User	Source user in a mapping.
Target User	Target user in a mapping.

Parameter	Description
Mapping Mode	User mapping mode related to the operating system, including: • **Windows to UNIX**: When accessing UNIX shares using Windows, a Windows user has all the permissions granted to the target user. • **UNIX to Windows**: When accessing Windows shares using UNIX, a UNIX user has all the permissions granted to the target user. • **Kerberos to UNIX**: When a client accesses UNIX shares through Kerberos authentication, the Kerberos user has all the permissions granted to the target user.
Priority	When multiple mappings share the same source user, the system uses the mapping with the highest priority. **NOTE** A smaller value indicates a higher priority.

----End

4.10.2 Modifying Attributes of a User Mapping

This operation enables you to modify the mapping mode, source user, target user, priority of a user mapping. The new user mapping can be used to access shares.

Procedure

Step 1 Choose **Services** > **File Service** > **Authentication Users** > **User Mappings**.

Step 2 Select the vStore to which the desired user mapping belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Click **More** on the right of the desired user mapping and select **Modify**.

The **Modify User Mapping** page is displayed on the right.

Step 4 Modify attributes of the user mapping.

Table 4-47 describes the parameters.

Table 4-47 Basic user mapping parameters

Parameter	Description
Mapping Mode	User mapping mode related to the operating system, including: • **Windows to UNIX**: When accessing UNIX shares using Windows, a Windows user has all the permissions granted to the target user. • **UNIX to Windows**: When accessing Windows shares using UNIX, a UNIX user has all the permissions granted to the target user. • **Kerberos to UNIX**: When accessing UNIX shares using Kerberos authentication through a client, a Kerberos user has all the permission granted to the target user.
Source User	Source user in the mapping. **NOTE** • The name of the source user supports the wildcard (*). For example, **user*** indicates all user names starting with **user**. • The user name can be a common or domain user name. An AD domain user name uses a backslash (\) to connect the domain name and user name. Only one backslash (\) is allowed, for example, **china\user001**. The AD domain name can only be a NetBIOS name. You can query the NetBIOS name of a domain by running the **nbtstat -n** command. Alternatively, you can right-click the domain on the **Active Directory Users and Computers** page, choose **Properties** from the shortcut menu, and find the value of **Domain name (pre-Windows 2000)** in the dialog box that is displayed. The value is the NetBIOS name of the domain.
Target User	Target user in the mapping. **NOTE** The user name can be a common or domain user name. An AD domain user name uses a backslash (\) to connect the domain name and user name. Only one backslash (\) is allowed, for example, **china\user001**. The AD domain name can only be a NetBIOS name. You can query the NetBIOS name of a domain by running the **nbtstat -n** command. Alternatively, you can right-click the domain on the **Active Directory Users and Computers** page, choose **Properties** from the shortcut menu, and find the value of **Domain name (pre-Windows 2000)** in the dialog box that is displayed. The value is the NetBIOS name of the domain.
Priority	Priority of the mapping. A smaller value indicates a higher priority. When multiple mappings share the same source user, the system uses the mapping with the highest priority. [Value range] 1 to 32

Step 5 Click **OK**.

----End

4.10.3 Deleting a User Mapping

This operation enables you to delete a user mapping. After the deletion, the source user cannot be mapped to the specified target user or access shares across operating systems.

Procedure

Step 1 Choose **Services** > **File Service** > **Authentication Users** > **User Mappings**.

Step 2 Select the vStore to which the desired user mapping belongs from the **vStore** drop-down list in the upper left corner.

Step 3 Select one or more desired user mappings and click **Delete**.

NOTE

You can also click **More** on the right of a desired user mapping and select **Delete**.

----End

4.10.4 Configuring Mapping Parameters

You can create user mappings in the local storage system as well as use user mappings in the external IDMU domain to access shares across systems. This section describes how to set user mapping parameters.

Context

If only IDMU user mappings are used, you do not need to configure user mappings in the local storage system.

Procedure

Step 1 Choose **Services** > **File Service** > **Authentication Users** > **User Mappings**.

Step 2 Select the vStore for which you want to configure mapping parameters from the **vStore** drop-down list in the upper left corner.

Step 3 Click **Set Mapping Parameter**.

The **Set Mapping Parameter** page is displayed on the right.

Step 4 Enable **Mapping Parameters** and configure user mapping parameters.

Table 4-48 describes the parameters.

Table 4-48 Mapping parameters

Parameter	Description
Mapping Mode	Global parameter of user mappings, including: • **Support only user mapping of this system**: The system only supports user mappings created in this system. • **Support only user mapping in IDMU**: The system only supports user mappings in the IDMU domain. • **Preferentially support user mapping in IDMU**: When user mappings of a specified source user exist both in the system and the IDMU domain, the system preferentially uses the mapping in the IDMU domain. • **Preferentially support user mapping of this system**: When user mappings of a specified source user exist both in the system and the IDMU domain, the system preferentially uses the mapping in this system.
IDMU Search Timeout Duration (s)	Timeout duration for the system to search for a specified user mapping in the IDMU domain. [Value range] 5 to 120
IDMU Search DN	Benchmark directory where the system searches for a specified user mapping in the IDMU domain. The benchmark directory stores the information of user mappings. [Value range] The directory contains 0 to 255 characters.
Map to User with Same Name	Indicates whether to map to users with the same name. After this function is enabled, the system automatically maps UNIX users and Windows users with the same name.
Default UNIX User	When user mapping is enabled and a Windows user fails to be mapped, the Windows user will be mapped to this default UNIX user.

Parameter	Description
Default Windows User	When user mapping is enabled and a UNIX user fails to be mapped, the UNIX user will be mapped to this default Windows user. If the default Windows user is an AD domain user, the naming format is *Domain name**Domain user name*. The AD domain name can only be a NetBIOS name. You can query the NetBIOS name of a domain by running the **nbtstat -n** command. Alternatively, you can right-click the domain on the **Active Directory Users and Computers** page, choose **Properties** from the shortcut menu, and find the value of **Domain name (pre-Windows 2000)** in the dialog box that is displayed. The value is the NetBIOS name of the domain.

NOTE

Map to User with Same Name, **Default UNIX User**, and **Default Windows User** are available only when **Mapping Mode** is set to **Support only user mapping of this system**, **Preferentially support user mapping in IDMU**, or **Preferentially support user mapping of this system**. **IDMU Search Timeout Duration (s)** and **IDMU Search DN** are available only when **Mapping Mode** is set to **Support only user mapping in IDMU**, **Preferentially support user mapping in IDMU**, or **Preferentially support user mapping of this system**.

Step 5 Confirm your operation as prompted.

----End

5 FAQs

This chapter describes frequently asked questions (FAQs) related to basic storage service configuration. You can also refer to this chapter to rectify the faults encountered during configuration or maintenance.

5.1 How Can I Configure and Use DNS Load Balancing?

The following uses a configuration example to describe how to configure and use DNS load balancing.

Context

- As shown in **Table 5-1**, a dual-controller storage system has two logical ports, which are created based on Ethernet ports on controller A and controller B.

  Table 5-1 Logical port information

Logical Port Name	IPv4 Address	Home Port
LogicPort_01	192.168.20.10	CTE0.A.IOM0.P0
LogicPort_02	192.168.20.20	CTE0.B.IOM0.P0

- An NFS share named **/nfs_share** and a CIFS share named **cifs_share** have been created on the storage system.

- A client wants to access the storage system using the domain name **testdns.abc123.com** and uses the port bandwidth usage as the load balancing policy.

Storage System Configuration

NOTE

- The following describes how to configure the storage system on DeviceManager.
- GUIs may vary with product versions and models. The actual GUIs prevail.

1. Create a DNS zone (**testdns.abc123.com** in this example).

   NOTE

   It is recommended that **Listen for DNS Query** be enabled for at least one logical port of each DNS zone.

   a. Choose **Services** > **vStore Service** > **vStores**.
   b. Click the desired vStore name. On the page that is displayed on the right, click the **File Service** tab page. Then click **Configure** in the **DNS Zone** area.

      The **Configure DNS Zone** dialog box is displayed.
   c. Click **Add**.
   d. In **Name**, type the domain name of the DNS zone you want to add. (In this example, enter **testdns.abc123.com**.)
   e. Click **OK**.
2. Configure logical ports to listen to DNS query requests and associate with the DNS zone.
   a. Choose **Services** > **Network** > **Logical Ports**.
   b. Select **LogicPort_01**. Click **More** and select **Modify**.

      The **Modify Logical Port** page is displayed.
   c. Select **Enable** for **Listen to DNS Query Request**.
   d. In **DNS Zone**, select DNS zone **testdns.abc123.com**.
   e. Click **OK**.

      A **Danger** dialog box is displayed.
   f. Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation**.
   g. Click **OK**.
   h. Perform **2.a**, **2.b**, **2.d** to **2.g** to associate LogicPort_02 with the DNS zone.
3. Configure a DNS load balancing policy and enable DNS load balancing.
   a. Choose **Settings** > **Basic Information** > **DNS Service**.
   b. Enable **File Service DNS Load Balancing**.
   c. For **Load Balancing Policy**, select **Port Bandwidth usage** from the drop-down list.
   d. Click **Save**.

      The **Warning** dialog box is displayed.

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

f. Click **OK**.

(Optional) External DNS Server Configuration

If an external DNS server is provided, you can configure it to forward or delegate domain name resolution requests from a client to the storage system. The storage system then selects a proper IP address based on loads and returns the IP address to the client.

NOTE

- Before configuring an external DNS server, ensure that: DNS zones have been created, logical ports have been associated with the DNS zones, logical ports have been enabled to listen to DNS requests, and DNS load balancing has been enabled on the storage system.
- You are advised to configure an external DNS server to connect to a storage system as follows:
  - When the domain name (DNS zone name) of the storage system does not indicate a subdomain of an existing domain configured by the user, configure a forwarder for the DNS server.
  - When the domain has been configured and the domain name (DNS zone name) of the storage system indicates a subdomain of an existing domain configured by the user, configure a delegation for the DNS server.
- The parameter settings in the following steps are examples only. Set the parameters based on site requirements.

This section describes how to configure an external DNS server (Bind 9) that runs the Linux operating system and an external DNS server that runs the Windows operating system.

For an external DNS server that runs the Linux operating system:

- Configure the external DNS server to send domain name resolution requests to the storage system using a forwarder.
  a. Log in to the DNS server as an administrator.
  b. Run the **vim /*path*/named.conf** command to open the configuration file, press **i** to enter the editing mode, and add the following information to the file. Then, type **:wq** and press **Enter** to save the settings and exit.

```
zone "testdns.abc123.com" in {
    type forward;
    forwarders { 192.168.20.10; };
};
```

NOTE

- **/path**: path where the **named.conf** configuration file resides, typically **/etc**. It may vary with the operating system.
- **testdns.abc123.com**: name of the created DNS zone (domain name). If the name of the created DNS zone does not end with **.com**, add a period (.) to the end of the name. For example, if the zone name is **test**, you are advised to change it to **test.** in the configuration file.
- **192.168.20.10**: IP address of the logical port configured on the storage system for listening to DNS query requests. IPv4 is used as an example. The configuration method for IPv6 is similar.

c. Run the **service named restart** command to restart the named service for the settings to take effect.

- Configure the external DNS server to send domain name resolution requests to the storage system using a delegation.

  a. Log in to the DNS server as an administrator.

  b. Run the **cat /*path*/named.conf** command to open the configuration file and check whether any forwarder is configured in **options**.

```
options {
   # The directory statement defines the name server's working directory
   directory "/var/lib/named";
   dump-file "/var/log/named_dump.db";
   statistics-file "/var/log/named.stats";
 forwarders{
    XX.XXX.X.XX;
 };
 forward first;
};
```

  In the preceding command, **/path** indicates the path where the **named.conf** configuration file resides, typically **/etc**. It may vary with the operating system.

  - If any forwarders are configured, contact the DNS environment maintenance administrator to check whether shielding these forwarders imposes any impact on resolving other domain names in the zone. If no impact, go to **c** to shield these forwarders. If you are not sure about the impact, contact technical support engineers.
  - If no forwarder is configured, go to **d**.

  c. Run the **vim /*path*/named.conf** command to open the configuration file. Press **i** to enter the editing mode and add the following information. Then, type **:wq** and press **Enter** to save the settings and exit.

```
zone "abc123.com" in {
      file "/var/lib/named/master/abc123.zone";
      type master;
      allow-update { none; };
     forwarders{};
};
```

  NOTE

  - **abc123.com**: parent domain name of the configured DNS domain name (**testdns.abc123.com**).
  - **abc123.zone**: configured DNS zone name.
  - **/path**: path where the **named.conf** configuration file resides, typically **/etc**. It may vary with the operating system.

  After forwarders are shielded, information can be properly sent to the DNS server corresponding to the storage system instead of other DNS servers during domain name resolution in the zone.

  d. Run the **vim /*path*/named.conf** command to open the configuration file. Press **i** to enter the editing mode and add the following information. Then, type **:wq** and press **Enter** to save the settings and exit.

```
zone "abc123.com" in {
      file "/var/lib/named/master/abc123.zone";
      type master;
      allow-update { none; };
};
```


NOTE

- **abc123.com**: parent domain name of the configured DNS domain name (**testdns.abc123.com**).
- **abc123.zone**: configured DNS zone name.
- **/path**: path where the **named.conf** configuration file resides, typically **/etc**. It may vary with the operating system.

e. Run the **vim /var/lib/named/master/abc123.zone** command to edit the DNS zone file and add the delegation settings.

```
$TTL 2D
@               IN SOA          abc123.com.        root (
                                2020120500      ; serial
                                3H              ; refresh
                                1H              ; retry
                                1W              ; expiry
                                1D )            ; minimum

                        IN NS           abc123.com.
userdefined             IN A            192.168.20.10
testdns.abc123.com.     IN NS           userdefined.abc123.com.
```

NOTE

- **testdns.abc123.com**: subdomain name of the DNS server to be delegated. The subdomain name must be the same as the DNS zone name on the storage system.
- **abc123.com**: parent domain name of the configured DNS domain name (**testdns.abc123.com**).
- **userdefined**: user-defined tag, which is used by **testdns.abc123.com.** for name server (NS) record query.
- **/var/lib/named/master/**: path where the DNS zone file resides, typically **/var/lib/named**. It may vary with the operating system.
- **192.168.20.10**: IP address of the logical port configured on the storage system for listening to DNS query requests. IPv4 is used as an example. The configuration method for IPv6 is similar.

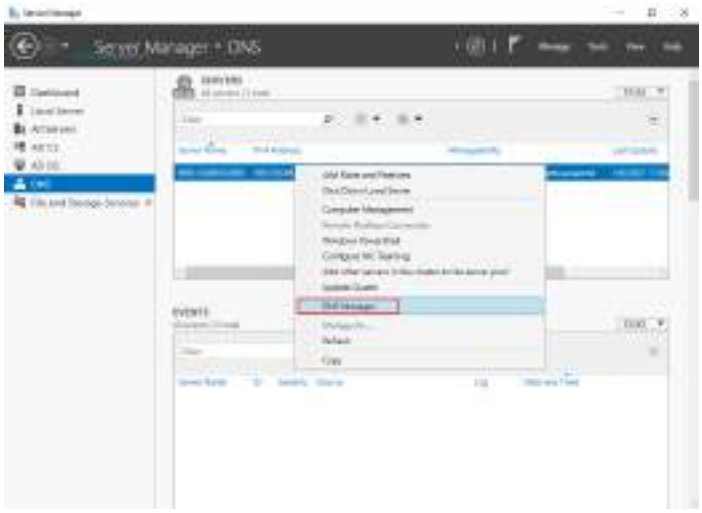
f. Run the **service named restart** command to restart the named service for the settings to take effect.

```
[root@ISM 16:57:15 /var/lib/named]# service named restart
Shutting down name server BIND waiting for named to shut down (28s) done
Starting name server BIND
```

g. Run **exit** to log out.

For an external DNS server that runs the Windows operating system:

- Configure the external DNS server to send domain name resolution requests to the storage system using a forwarder.
  a. Go to the **DNS Manager** window. Windows Server 2016 is used as an example.

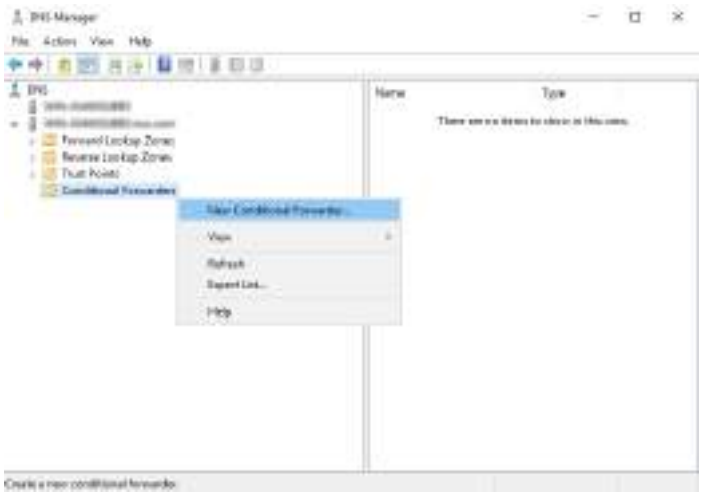


NOTE

The GUI may vary with the client version.

b. In the navigation tree on the left, right-click **Conditional Forwarders** and choose **New Conditional Forwarder** from the shortcut menu.

Figure 5-1 Creating a conditional forwarder



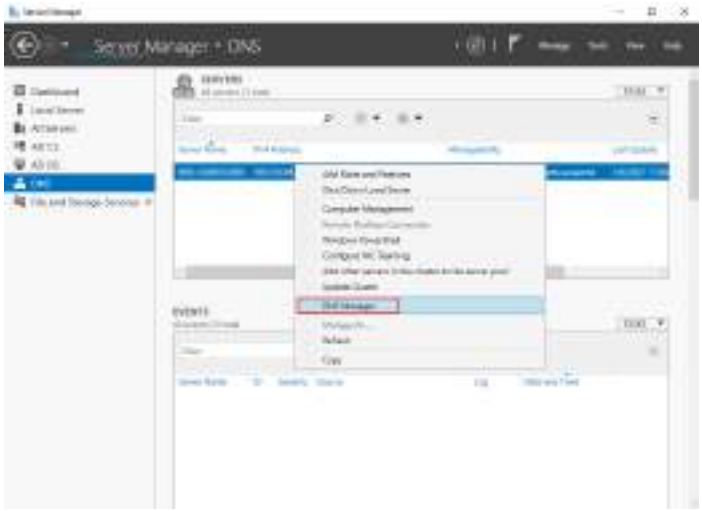
c. Configure the conditional forwarder. Enter the created DNS zone in **DNS Domain** and the IP address of the logical port used to listen to DNS requests in **IP addresses of the master servers**.

Figure 5-2 Configuring the forwarding domain name and DNS server

d. Close the **DNS Manager** window.

- Configure the external DNS server to send domain name resolution requests to the storage system using a delegation.

  a. Go to the **DNS Manager** window. Windows Server 2016 is used as an example.

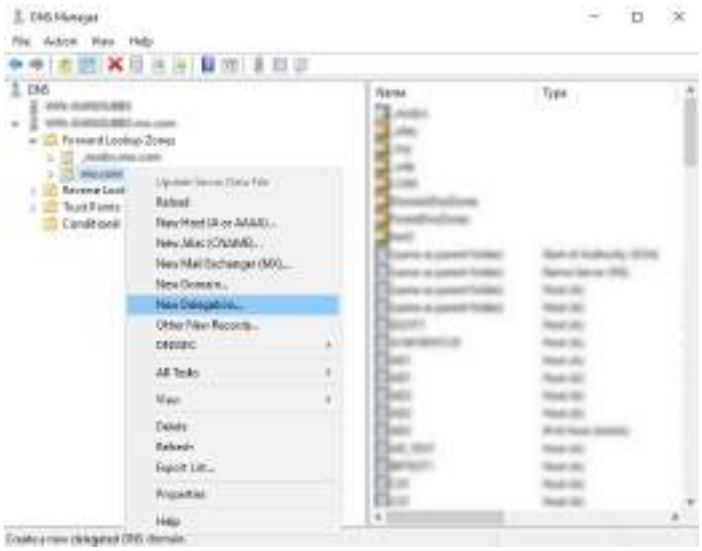


NOTE

The GUI may vary with the client version.

  b. In the navigation tree on the left, click **Forward Lookup Zones**. In the expanded list, right-click the domain controller name and choose **New Delegation** from the shortcut menu.

Figure 5-3 Creating a delegation



c. In the delegation wizard that is displayed, click **Next**. In **Delegated domain**, enter the created DNS zone excluding the domain controller name. Click **Next**.

Figure 5-4 New Delegation Wizard

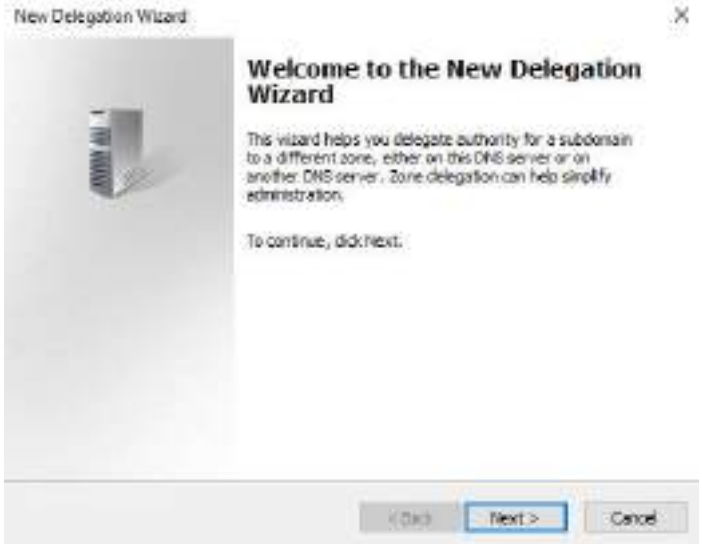
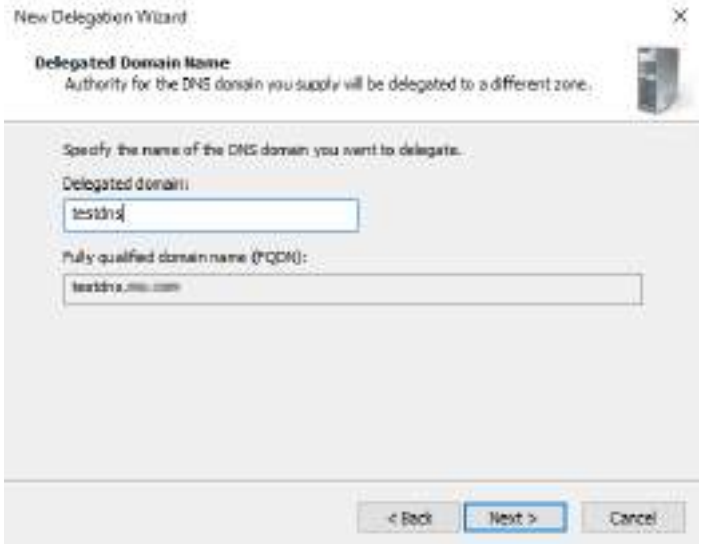
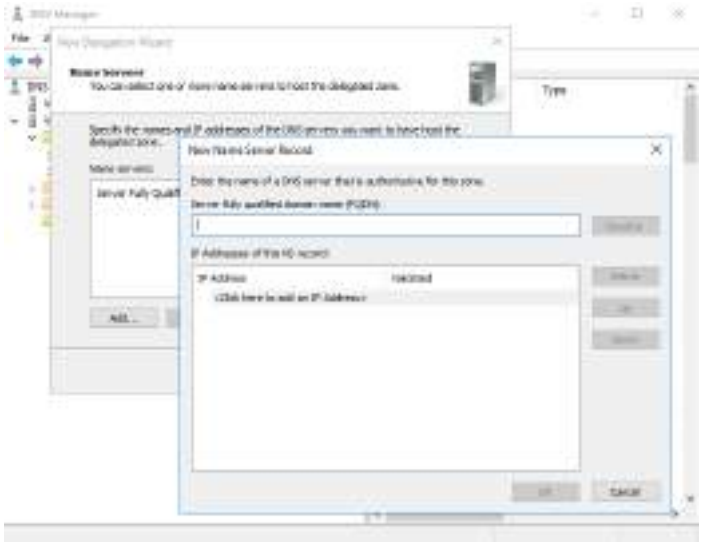


Figure 5-5 Setting the delegated domain name



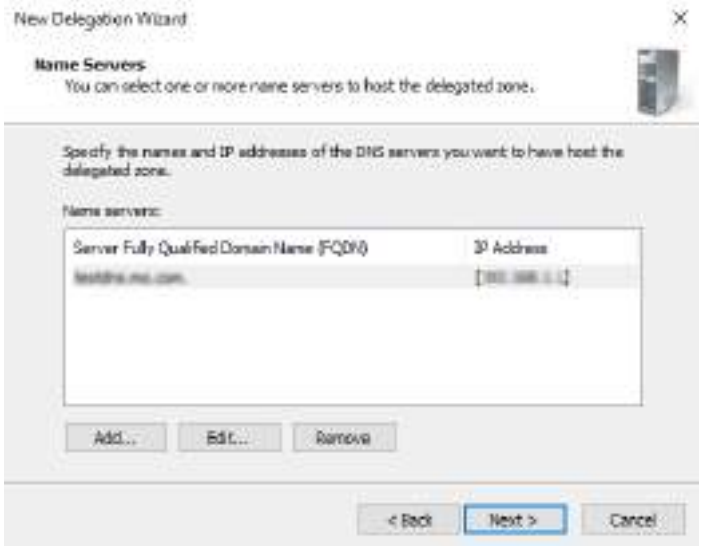
d. Click **Add**. Enter the created DNS zone in **Server fully qualified domain name (FQDN)** and the IP address of the logical port used to listen to DNS requests in **IP addresses of this NS record**.

Figure 5-6 Adding a DNS zone



e. In the **Name Servers** window, confirm the entered configuration and connect to the external DNS server using a delegation as prompted.

Figure 5-7 DNS zone added successfully



Client Configuration

NOTE

The following describes how to configure DNS server addresses and access shares on a Linux client and Windows client (Windows Server 2012).

1. Configure DNS server addresses on the client.
   a. Linux client

      Add **nameserver 192.168.20.10** to the **/etc/resolv.conf** file. If the host does not use other DNS servers, set this parameter to the IP address of the logical port that is enabled on the storage system to listen to DNS query requests. If the host uses another DNS server, set this parameter to the IP address of that DNS server and configure the forwarding policy on that DNS server.

```
[root@localhost ~]# vi /etc/resolv.conf
[root@localhost ~]# cat /etc/resolv.conf
nameserver 192.168.20.10


[root@localhost ~]#
```


NOTE

You can run the **nslookup** <*DNS zone name*> command to check whether the domain name of the DNS zone can be resolved.

If a Linux client is connected to built-in DNS load balancing servers on multiple storage systems, you are advised to optimize the **/etc/resolv.conf** file to prevent ping or mount timeout due to DNS zone name resolution failures between the storage systems. An example is provided as follows:

Before:

```
nameserver x.x.0.1
nameserver x.x.0.2
nameserver x.x.0.3
```

After:

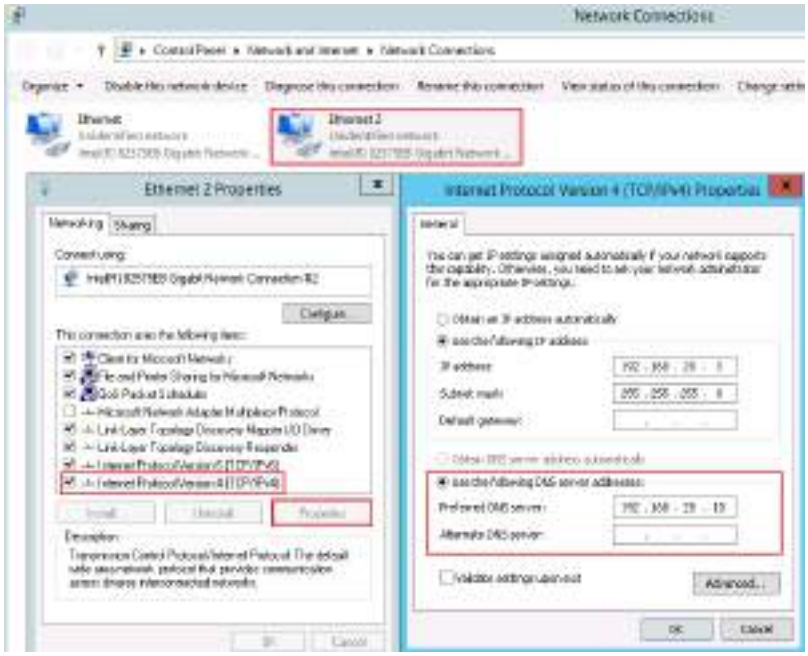
```
options timeout:1 attempts:1 rotate
nameserver x.x.0.1
nameserver x.x.0.2
nameserver x.x.0.3
```

Parameters are described as follows:

- **timeout** indicates the timeout time for querying a name server. It is expressed in seconds. Its default value is 5.
- **attempts** indicates the number of attempts to query the entire name server list. The default value is 2.
- **rotate** indicates that a name server is randomly selected as the preferred DNS server. If **rotate** is not used, the system selects the preferred DNS server from top to bottom by default. If any name server is recommended, do not use **rotate** and place the recommended name server in the first line of the name server list.

b. Windows client

In properties of the Ethernet port, set **Preferred DNS server** to **192.168.20.10**.



NOTE

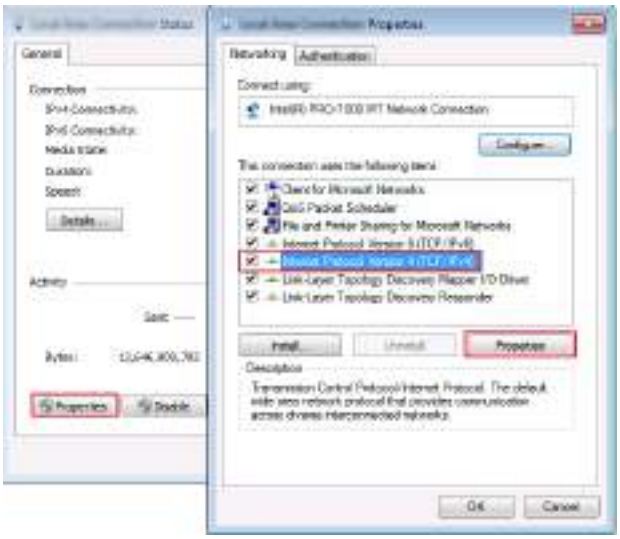
- If a client has multiple NICs and one NIC is configured with an IPv4 DNS server, the other NICs cannot be configured with IPv6 DNS servers.
- If Windows clients cannot identify domain names that do not contain any period (.), you can configure the DNS zone name to contain a period (.).
- If Windows clients automatically add an additional DNS domain name suffix, you can optimize the Windows host configuration.

  For example:

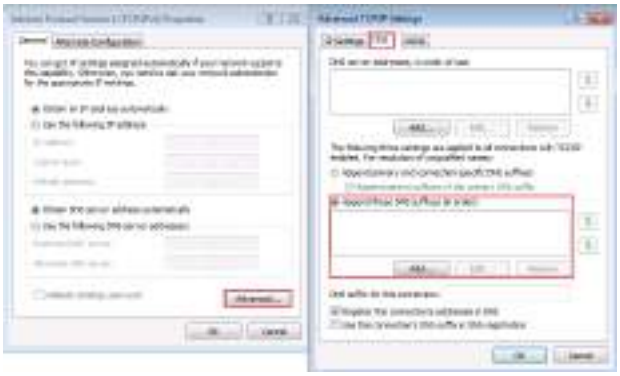
  Choose **Control Panel** > **Network and Internet** > **Network and Sharing Center**. In the **View your active networks** area, click the connected network.

  In the displayed dialog box, click **Properties**. Then select **Internet Protocol Version (TCP/IPv4)** and click **Properties**.

  In the displayed dialog box, click **Advanced**. Then click the **DNS** tab page, and append the DNS suffix (.).

2. Use the client to access shared file systems through the DNS zone domain name.

NOTE

- The following describes how to use a Linux client to access the NFS share **/nfs_share** and a Windows client to access the CIFS share **cifs_share**.
- To access other types of shares, use the similar method. Replace the IP address of the logical port originally used to access shares with the DNS zone domain name (**testdns.abc123.com**).

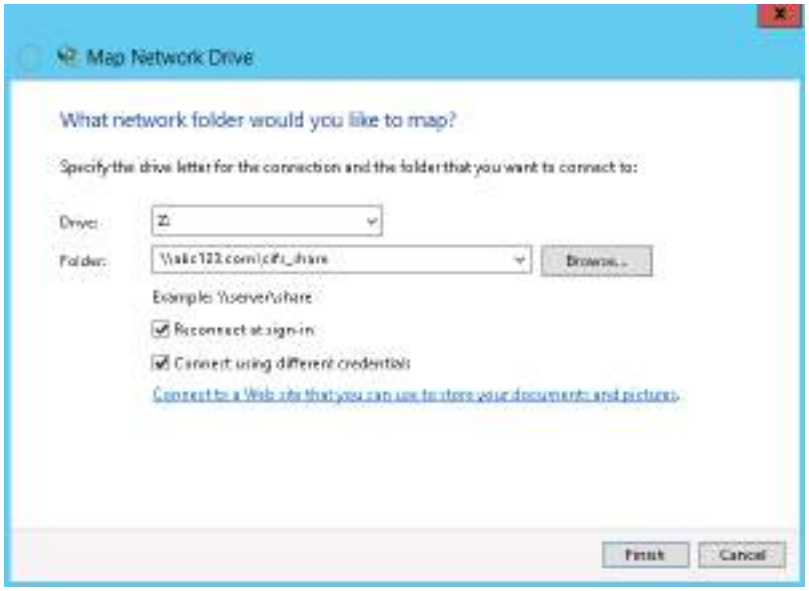
a. Use a Linux client to access an NFS share.

Replace the IP address of the logical port originally used to access the NFS share with the DNS zone domain name (**testdns.abc123.com**).

```
[root@localhost ~]# mount -t nfs -o
vers=3,proto=tcp,rsize=262144,wsize=262144,hard,intr,timeo=50 testdns.abc123.com:/
nfs_share /mnt
```

b. Use a Windows client to access a CIFS share.

In the **Map Network Drive** dialog box, set the mapping network folder in the format of *DNS zone domain name* *sharename*.



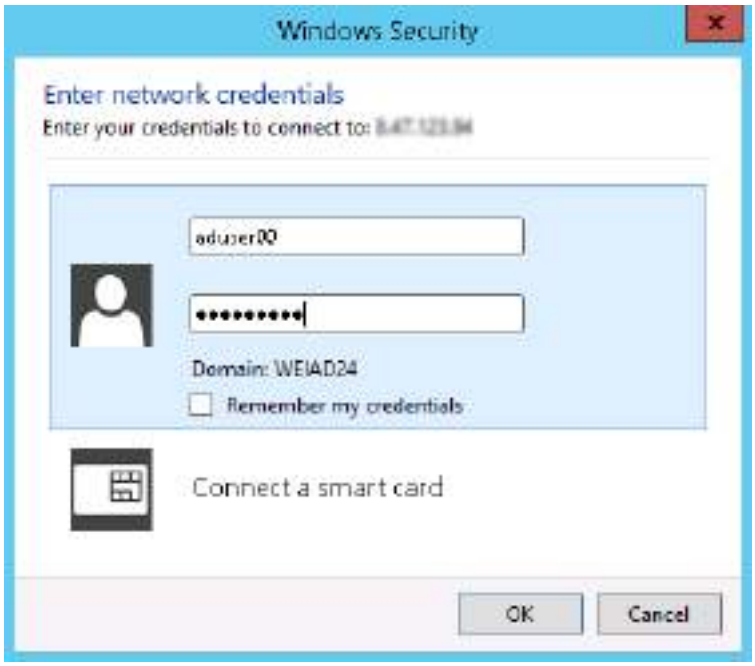
Complete user authentication as prompted. After authentication succeeds, the client can access the shared space.

5.2 How can I Perform Configuration and Verification on the Host After Access Based Enumeration (ABE) Is Enabled When the Storage System Creates a CIFS Share?

After ABE is enabled, the share directory does not display files or file folders on which the user has no access permission. The following shows accessing a CIFS share on the host in the domain environment (also applicable to local authentication users).

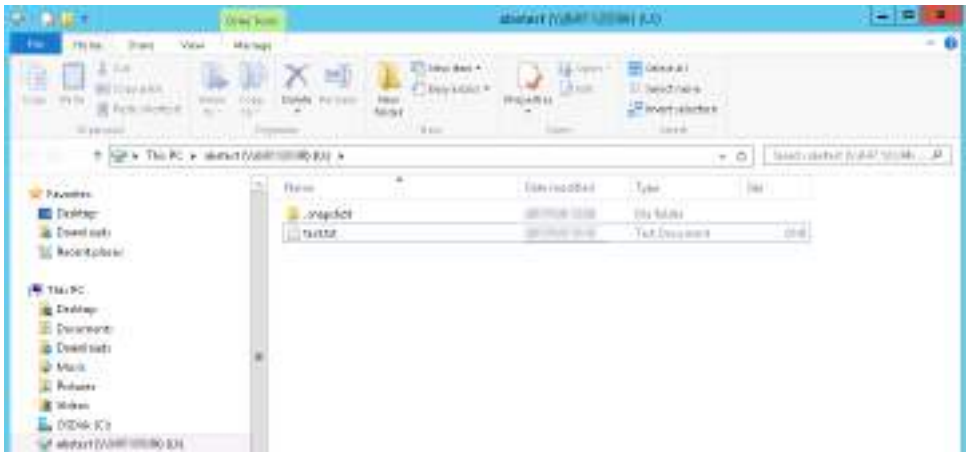
1. The host accesses the CIFS share created by the storage system successfully. Figure 5-8 shows share access by domain user **aduser00**.

   Figure 5-8 The host accesses the CIFS share created by the storage system



2. Create file **test.txt** under the share path. **Figure 5-9** shows the result.

Figure 5-9 Create file under the share path



3. Add permissions to domain users **aduser01** and **24aduser1** and remove the default permission of **Everyone**. If the default permission of **Everyone** is not removed, all users have full control over the file and can still view the file.

   Figure 5-10 shows how to modify the advanced settings of **test.txt**.

Figure 5-10 Modify the advanced settings

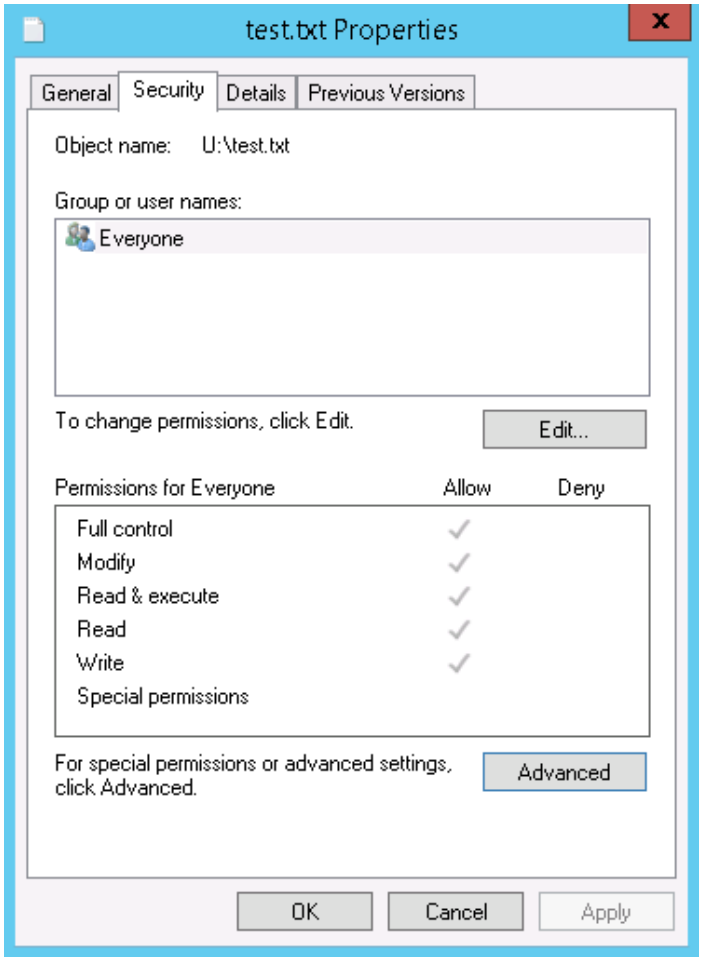


Figure 5-11 shows the advanced security settings before the default permission of **Everyone** is removed.

Figure 5-11 Before the default permission of Everyone is removed

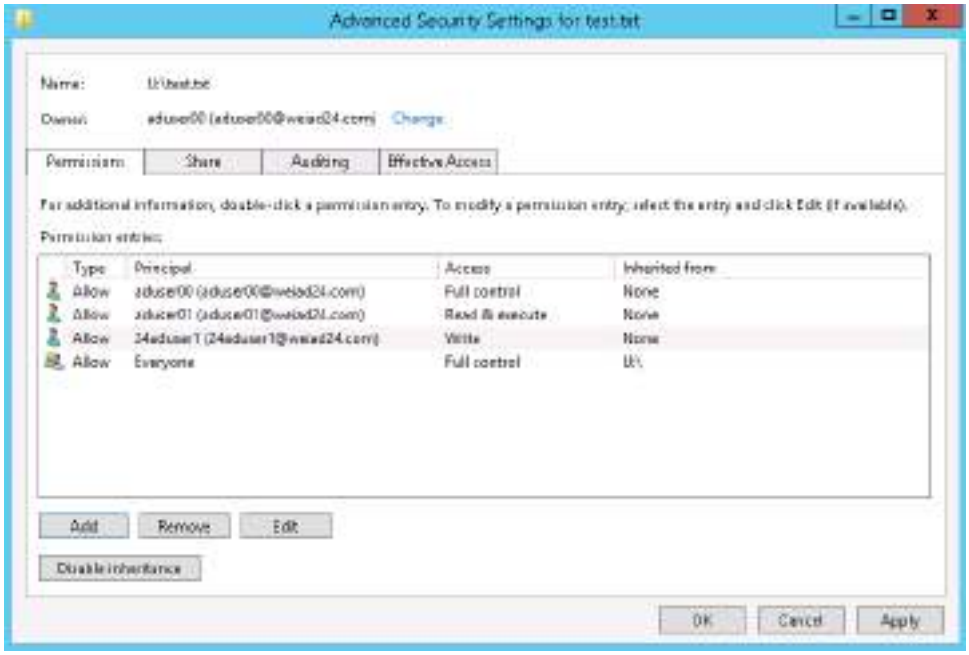


Figure 5-12 shows the advanced security settings after the default permission of **Everyone** is removed.

Figure 5-12 After the default permission of Everyone is removed

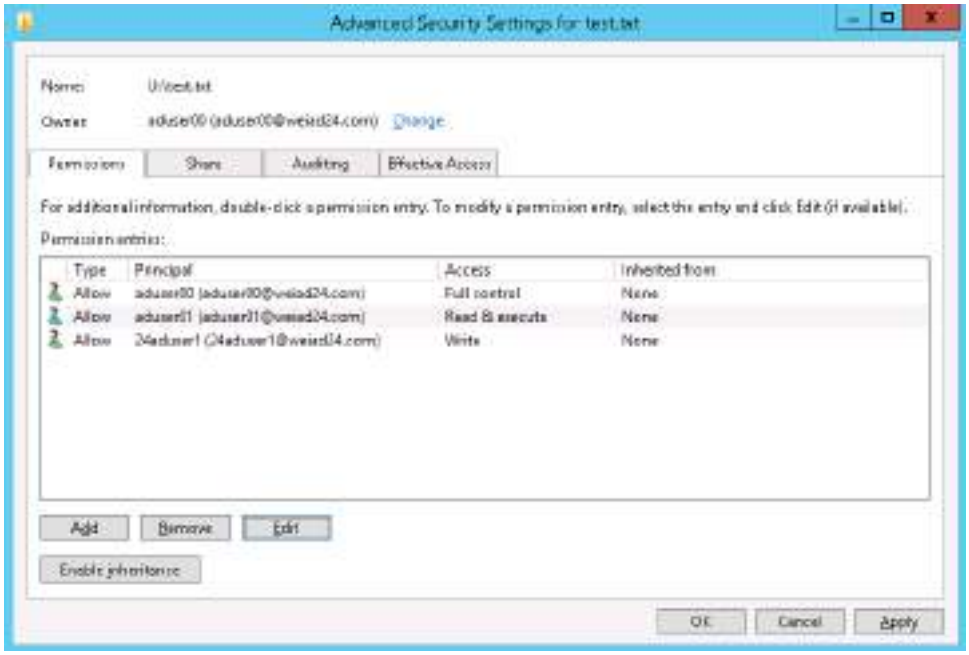
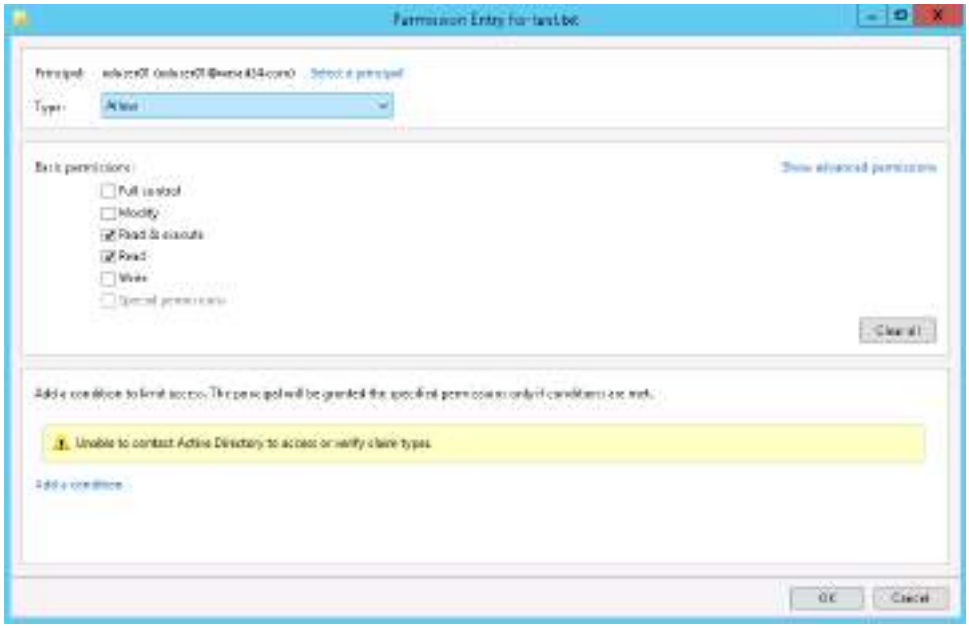


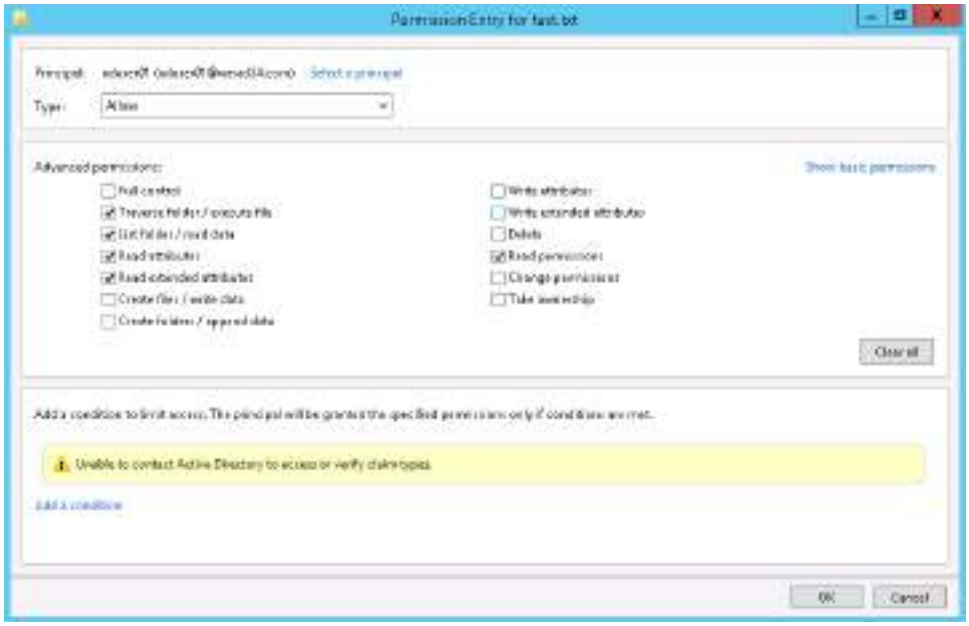
Figure 5-13 shows the permission settings for domain user **aduser01**.

Figure 5-13 Permission settings for domain user aduser01



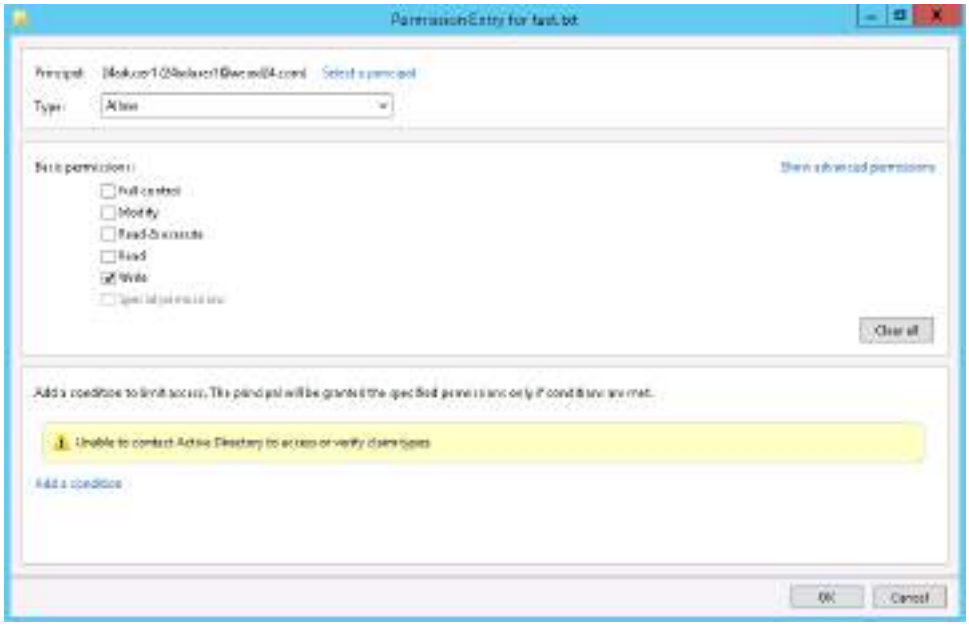
[Figure 5-14](#) shows how to select **read data**, **read attributes**, **read extended attributes**, and **read permissions** to gain full read permissions.

Figure 5-14 Full read permissions



[Figure 5-15](#) shows the permission settings for domain user **24aduser1**.

Figure 5-15 Permission settings for domain user 24aduser1



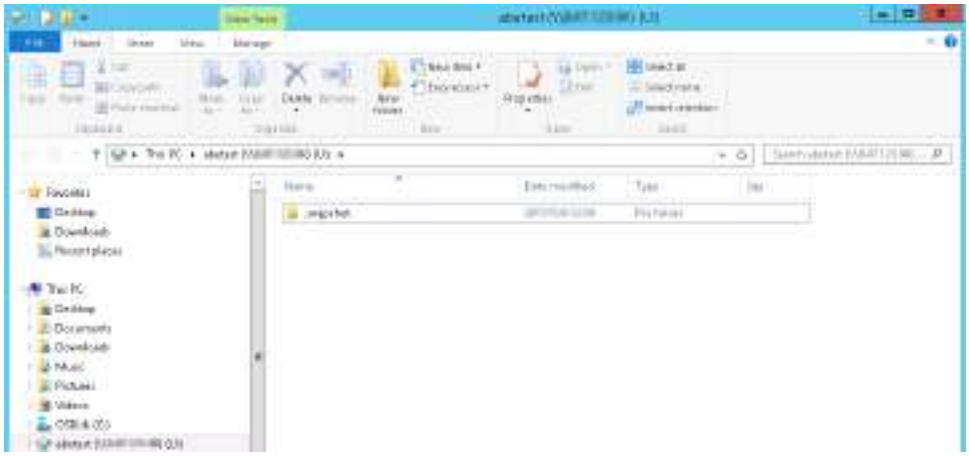
4. View and check the files in the share path as domain users **aduser01** and **24aduser1**. The verification results are as follows:

   Figure 5-16 shows the verification results for domain user **aduser01**.

Figure 5-16 Verification results for domain user aduser01

Figure 5-17 shows the verification results for domain user **24aduser1**.

Figure 5-17 Verification results for domain user 24aduser1



5.3 How Can I Modify Security Policies for Accessing HTTP and FTP Shares?

Modifying the Security Policy for Accessing the HTTP Share

Step 1 Log in to the CLI of the storage system.

Step 2 Access the container where the HTTPS service is running by running the following command:

change container_application view pod_name=http-pod-0 namespace=http

NOTE

To obtain the value of **pod_name**:

In versions earlier than 6.1.5, run the **show container_application general name=http-chart** command.

In 6.1.5 and later versions, run the **show container_application general name=http-chart namespace=http** command.

Step 3 Modify the security policies for accessing the HTTP share.

1. Run the **vi prohttpd/conf/httpd.conf** command to open the configuration file of the HTTP service.
2. Press **i** to enter the editing mode.
3. Modify the **expirevar** setting and related variables.

   Before the modification, the default security policies are as follows:

   - If a user enters incorrect passwords for three consecutive times within 5 minutes, the user is not allowed to log in for 5 minutes.
   - If a host IP address is incorrectly entered for 10 times within 5 minutes, the access to the host IP address is not allowed for 5 minutes.

   The corresponding configuration file code (in bold) is as follows:

```
  SecRule RESPONSE_STATUS "401" \
     "phase:5,pass,id:2000015,chain,logdata:'basic auth de @%{IP}, var: %{IP.begin}, user: %
{USER.name}, ufc: %{USER.user_false_counter}, block: %{USER.bf_block}, IPblock: %{IP.bf_block}, ifc: %
```

```
{IP.ip_false_counter}'"
        SecAction setvar:USER.user_false_counter=+1,setvar:IP.ip_false_counter=
+1,expirevar:USER.user_false_counter=300,expirevar:IP.ip_false_counter=300

    # Check for too many failures for a single username, blocking 30 seconds after 3 tries
    SecRule USER:user_false_counter "@ge 3" \
            "id:'2000020',phase:3,t:none,pass,\
            setvar:USER.bf_block,\
            setvar:!USER.user_false_counter,\
            expirevar:USER.bf_block=300"

    # Check for too many failures from a single IP address. Block for 5 minutes after 10 tries.
        SecRule IP:ip_false_counter "@ge 10" \
            "id:'2000021',phase:3,pass,t:none, \
            setvar:IP.bf_block,\
            setvar:!IP.ip_false_counter,\
            expirevar:IP.bf_block=300"
```

In the preceding code:

- In **expirevar:USER.user_false_counter=300**, **300** indicates the time range (unit: second) for collecting statistics on password input errors for the same user. In **expirevar:IP.ip_false_counter=300**, **300** indicates the time range (unit: second) for collecting statistics on password input errors for the same host IP address.
- In **SecRule USER:user_false_counter "@ge 3"**, **3** indicates the maximum number of incorrect password attempts allowed for the same user. In **SecRule IP:ip_false_counter "@ge 10"**, **10** indicates the maximum number of incorrect password attempts allowed for the same host IP address.
- In **expirevar:USER.bf_block=300**, **300** indicates the duration (unit: second) during which the user is not allowed to log in. In **expirevar:IP.bf_block=300**, **300** indicates the duration (unit: second) during which the access to the host IP address is not allowed.

NOTE

You can change the values of the preceding parameters based on the service requirements.

4. Type **:wq** and press **Enter** to save the settings and exit.

Step 4 Run the **httpd -k restart** command to enable the modified HTTPS service configuration.

----End

Modifying the Security Policy for Accessing the FTP Share

Step 1 Log in to the CLI of the storage system.

Step 2 Access the container where the FTPS service is running by running the following command:

change container_application view pod_name=ftp-pod-0 namespace=ftp

> **NOTE**
>
> To obtain the value of **pod_name**:
>
> In versions earlier than 6.1.5, run the **show container_application general name=ftp-chart** command.
>
> In 6.1.5 and later versions, run the **show container_application general name=ftp-chart namespace=ftp** command.

Step 3 Modify the security policies for accessing the FTP share.

1. Run the **vi /mnt/nfs/etc/config/proftpd.conf** command to open the configuration file of the FTP service.
2. Press **i** to enter the editing mode.
3. Modify the variables related to the **BanOnEvent** field.

   Before the modification, the default security policy of the system is as follows: If a host initiates three or more connections within 1 minute, the host cannot access the FTP share within the next minute.

   The corresponding configuration file code (in bold) is as follows:

```
MaxLoginAttempts 1
<IfModule mod_ban.c>
  BanEngine                  on
  BanLog                    /mnt/nfs/etc/log/ban.log
  BanTable                   /mnt/nfs/etc/ban.tab

  BanOnEvent                 MaxLoginAttempts 3/00:05:00 00:05:00

  # Inform the user that it's not worth persisting
  BanMessage                  "Host %a has been banned"

</IfModule>
```

   In the preceding code:

   - In **BanOnEvent MaxLoginAttempts 3/00:05:00 00:05:00**, **3/00:05:00** indicates the threshold for login failures of a host within a specified period (in the format of hh:mm:ss). In this example, the number of login failures of a host within 5 minutes cannot reach 3.
   - In **BanOnEvent MaxLoginAttempts 3/00:05:00 00:05:00**, **00:05:00** (the latter one) indicates the period (in the format of hh:mm:ss) during which the host is forbidden to access the FTP share if the number of login failures of the host within the specified period reaches the threshold. In this example, the period is 5 minutes.

   > **NOTE**
   >
   > You can change the values of the preceding parameters based on the service requirements.

4. Type **:wq** and press **Enter** to save the settings and exit.

Step 4 Run the **startup.sh reload** command to enable the modified FTPS service configuration.

----End

5.4 How Do I Upgrade a Containerized Application?

The following uses the FTP application as an example. Assume that the versions of the container image and the Helm chart used by the FTP application are v1.0 and

v1.0.0, respectively. We want to upgrade the container image version to v1.1.0 and the Helm chart version to v1.1.0.

Context

If the version of the image used by the HTTP containerized application is v1.0, after the image is updated to v1.1.0 or a later version, you can only run the **htdigest "/mnt/nfs/http/prohttpd/user.passwd" DAV-upload admin** command to create users. You can run the **show container_image general** command to query the image version.

Procedure

Step 1 Check the version of the container image that is being used by the application.

Example command:

```
admin:/>show container_image general
 Application  Version  Upload Time          Size  Is Active
 -----------  -------  -------------------  ----  ---------
 ftp-image    v1.0     2021-12-28 16:11:49  381M  Yes
```

Step 2 Import the container image and Helm chart of the new versions.

1. Run the **import container_image ip=? user=? password=? path=? [port=?] [protocol=?]** command to import the container image of the new version.

   Example command:

   ```
   admin:/>import container_image ip=x.x.0.16 user=admin password=********** path=/home/permitdir/
   XXXX_XXX_ftp_image_signature.tgz
   Download package. SUCCESS
   Command executed successfully.
   ```

   NOTE

   In the preceding command, *XXXX_XXX*_**ftp_image_signature.tgz** is the image software package prepared in advance. The package name varies according to the version.

2. Run the **import helm_chart ip=? user=? password=? path=? [port=?] [protocol=?]** command to import the Helm chart of the new version.

   Example command:

   ```
   admin:/>import helm_chart ip=x.x.0.16 user=admin password=********** path=/home/permitdir/
   XXXX_XXX_ftp_chart_signature.tgz
   Download package. SUCCESS
   Command executed successfully.
   ```

   NOTE

   In the preceding command, *XXXX_XXX*_**ftp_chart_signature.tgz** is the Helm chart software package prepared in advance. The package name varies according to the version.

3. Run the **show container_image general** and **show helm_chart general** commands to view the imported image and chart information, respectively.

   ```
   admin:/>show container_image general
    Application  Version  Upload Time          Size  Is Active
    -----------  -------  -------------------  ----  ---------
    ftp-image    v1.0     2021-12-28 16:11:49  381M  Yes
    ftp-image    v1.1.0   2021-12-28 16:22:35  381M  No

   admin:/>show helm_chart general
    Application  Version  Upload Time
    -----------  -------  -------------------
   ```



```
ftp-chart    1.0.0    2021-12-28 16:11:56
ftp-chart    1.1.0    2021-12-28 16:22:41
```

Step 3 Run the **change container_application general name=? namespace=? version=? dynamic_config=image.tag=?** command to upgrade the application.

To obtain the value of **version**, run the **show helm_chart general** command. To obtain the value of **image.tag**, run the **show container_image general** command.

Example command:

```
admin:/>change container_application general name=ftp-chart namespace=ftp version=1.1.0
dynamic_config=image.tag=v1.1.0
DANGER: You are about to update containerized application. This operation will interrupt services provided by the containerized application during the update, and the services will be restored after the update is complete.
Suggestion: Before performing this operation, ensure that the preceding risk is acceptable.
Have you read danger alert message carefully?(y/n)y
Are you sure you really want to perform the operation?(y/n)y
Command executed successfully.

admin:/>show container_image general
  Application  Version  Upload Time          Size  Is Active
  -----------  -------  -------------------  ----  ---------
  ftp-image    v1.0     2021-12-28 16:11:49  381M  No
  ftp-image    v1.1.0   2021-12-28 16:22:35  381M  Yes
```

If the value of **Is Active** for the new image is **Yes** in the **show container_image general** command output, the application is upgraded successfully.

----End

5.5 How Do I Check the Password Encryption Mode Currently Used by the HTTP Containerized Application?

htdigest and htpasswd are two different password encryption modes. When the HTTP containerized application is upgraded, if you need to create a user after the upgrade, query the password encryption mode currently used by the application and then run the corresponding command for user creation.

Procedure

Step 1 Log in to the CLI of the storage system.

Step 2 Run the **change container_application view pod_name**=*?* **namespace**=*?* command to access the container OS.

To obtain the values of **pod_name** and **namespace**:

In versions earlier than 6.1.5, run the **show container_application general name=http-chart** command.

In 6.1.5 and later versions, run the **show container_application general name=http-chart namespace=http** command.

Example command:

```
admin:/>change container_application view pod_name=http-pod-0 namespace=http
sh-5.0#
```


Step 3 Run the **cat /mnt/nfs/http/prohttpd/conf/extra/httpd-dav.conf | grep AuthType** command to query the password encryption mode used by the HTTP containerized application.

- The application uses the htpasswd password encryption mode, if the command output is displayed as follows:

```
sh-5.0# cat /mnt/nfs/http/prohttpd/conf/extra/httpd-dav.conf | grep AuthType
    AuthType Basic
sh-5.0#
```

  To create a user, run the **htpasswd "/mnt/nfs/http/prohttpd/user.passwd" *username*** command.

- The application uses the htdigest password encryption mode, if the command output is displayed as follows:

```
sh-5.0# cat /mnt/nfs/http/prohttpd/conf/extra/httpd-dav.conf | grep AuthType
    AuthType Digest
sh-5.0#
```

  To create a user, run the **htdigest "/mnt/nfs/http/prohttpd/user.passwd" DAV-upload *username*** command.

----End

A Configuring and Managing BGP

A.1 Overview

Background

When providing NAS services, the storage system communicates with the host through logical interfaces (LIFs). In the event of a port or controller fault, the LIFs automatically fail over to another available port to ensure service continuity. After LIF failover, the switch should send gratuitous Address Resolution Protocol (ARP) packets to instruct the host to update the MAC address of the current port that carries the LIF. To achieve this, you must enable the gratuitous ARP function on the switch. If gratuitous ARP is not enabled on the customer's switch due to security issues, the host is unable to update the ARP entries after the NAS LIF failover. As a result, the connection between the host and the storage system is interrupted.

In addition, in the NAS HyperMetro scenario, the NAS LIF configuration is synchronized between two sites. When a NAS LIF is activated at the other site, the route from the NAS LIF to the host is configured. This route is the same at the two sites. In this case, the two sites must be on the same subnet. However, the next-generation data centers use Layer 3 networking, so the two HyperMetro sites may be deployed on different subnets. This requires LIF failover across subnets.

Definition

The Border Gateway Protocol (BGP) is a distance-vector routing protocol that provides reachable routes between autonomous systems (ASs). BGP selects the optimal routes, prevents routing loops, transmits routes more efficiently, and maintains a large number of routes.

The storage system supports BGP and adds a VIP LIF. The storage system advertises the routing information of the VIP LIF through BGP, which allows the VIP LIF to fail over across subnets.

Benefits

Table A-1 Purposes and benefits of BGP

Benefit	Description
The VIP LIF supports IP address failover.	If the current node or port of a VIP LIF is faulty, the VIP LIF can fail over to another available node to ensure service continuity.
VIP LIF supports HyperMetro switchover.	If a site of HyperMetro is faulty, the VIP LIF is switched to the other site to ensure service continuity.
The VIP LIF supports DNS load balancing.	The VIP LIF is added to the DNS zone and can be accessed through the domain name of the DNS zone.

A.2 Basic Concepts

Autonomous System (AS)

An AS is an IP network that is controlled by a single entity and has the same routing policy.

- Each AS has a unique AS number assigned by the Internet Assigned Numbers Authority (IANA).
- The AS number ranges from 1 to 65535, among which 64512 to 65535 are private AS numbers.

Dynamic Routing Protocols

Routing is to allow two IP nodes on a network to communicate with each other and exchange data.

When a router receives an IP packet, it identifies the destination IP address of the packet, searches its routing table for the best matched routing entry, and then forwards the packet through the outbound interface or next hop IP address indicated by the routing entry.

A router can obtain routing entries in direct, static, or dynamic mode and maintain its own routing table.

Based on the application scope, dynamic routing protocols can be classified into the following types:

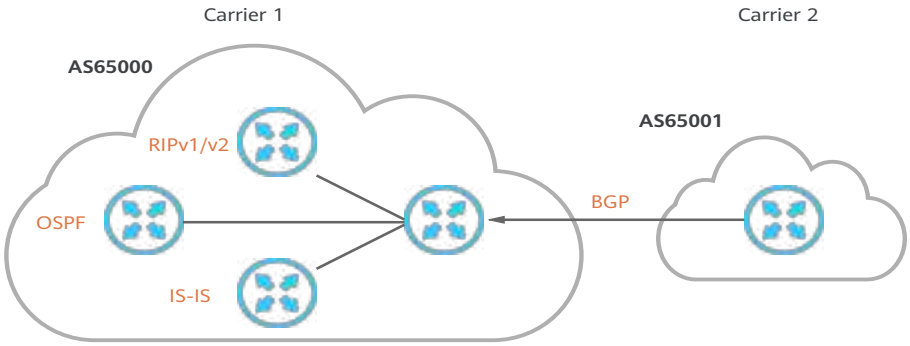
- Interior Gateway Protocol (IGP): This routing protocol exchanges routing information within an AS. It is mainly used to discover and calculate routes.

  Common IGP protocols include Routing Information Protocol (RIP), Open Shortest Path First (OSPF), and Intermediate System to Intermediate System (IS-IS).

- Exterior Gateway Protocol (EGP): This routing protocol works between ASs. It is mainly used to transmit routes.

  Currently, only the Border Gateway Protocol (BGP) is commonly used.

Figure A-1 BGP application scenarios



BGP Overview

BGP is used to exchange routing information between ASs.

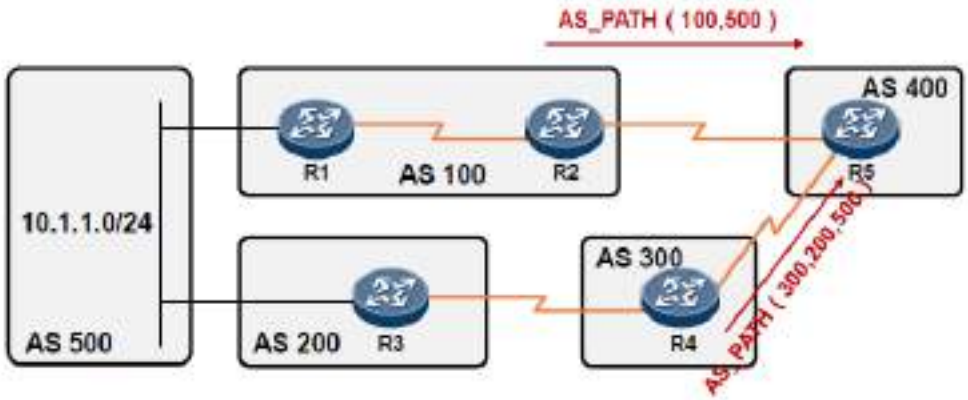
BGP has the following characteristics:

- BGP uses TCP as the transport layer protocol and communicates over TCP port 179. BGP routers establish BGP sessions based on TCP.
- A router that runs BGP is called a BGP speaker or a BGP router.
- Two BGP routers can exchange BGP routes only after a BGP peer relationship is established between them. The BGP routers in the peer relationship do not need to be directly connected.
- After a BGP peer relationship has been established, the BGP routers do not periodically update routes. Instead, they only send incremental BGP route updates or updates BGP routes when it is triggered.
- BGP provides abundant path attributes and powerful routing policy tools.
- BGP can carry a large number of route prefixes for large-scale networks.

Path Vector Characteristics of BGP

BGP is also called the Path-Vector Routing Protocol.

- Each BGP route carries multiple path attributes, among which AS_Path is a key attribute. The AS_Path attribute records the numbers of the ASs that a BGP route passes through during transmission, forming a list of AS numbers.
- The length of the AS_Path attribute (the number of AS numbers) is used as a reference for BGP route selection.



BGP Packet Type

Figure A-2 BGP packet

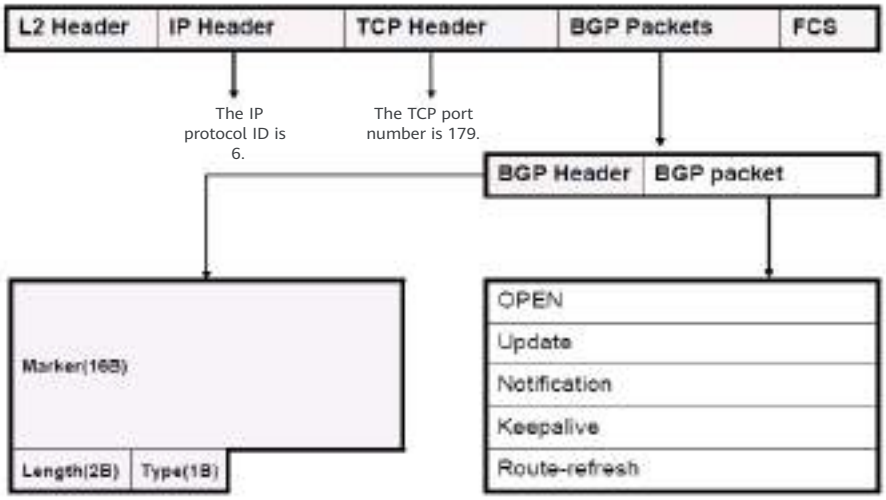


Table A-2 Fields in the BGP header

Field	Length	Description
Marker	16 bytes	Checks the integrity of the synchronization information of BGP peers and calculates BGP authentication.
Length	2 bytes	Total length of a BGP message. The unit is byte. The length ranges from 19 to 409.
Type	1 byte	Type of a BGP message. This field has five possible values, representing the five types of packets following the BGP packet header.

Table A-3 BGP packet types

Packet Name	Usage	When to Send the Packet
Open	Negotiates BGP peer parameters and establishes BGP peer relationships.	A TCP connection must be established between BGP peers. If the TCP connection is established successfully, BGP sends an Open message to the peer.
Update	Advertises BGP routes.	If a route needs to be sent or a route changes after the connection is established, an Update message is sent to notify the peer of the route information.
Notification	Reports errors and terminates the peer relationship.	If a BGP error occurs, a Notification packet is sent to notify the BGP peer.
Keepalive	Maintains the BGP peer relationship.	Keepalive packets are sent periodically to maintain the validity of the BGP peer relationship.
Route-refresh	Requests the peer to resend routes if the routing policy is changed. Only BGP devices with the route-refresh capability can send and respond to this packet.	When the routing policy changes, the BGP device requests the peer to re-advertise routes.

BGP Peer Status

There are six states during the interaction of BGP peers: Idle, Connect, Active, OpenSent, OpenConfirm, and Established.

Figure A-3 BGP peer interaction process

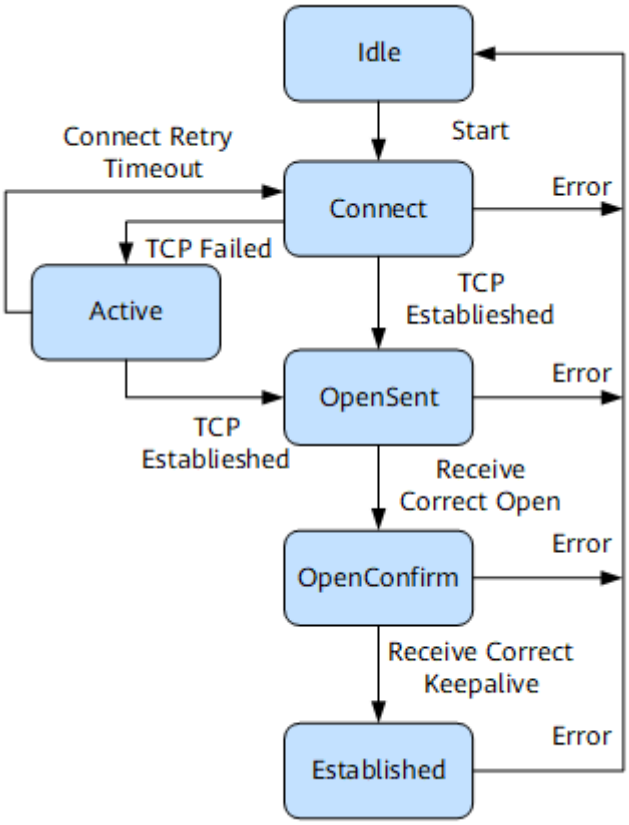


Table A-4 BGP peer status

Status	Packet	Action
Idle	Attempts to set up a TCP connection.	Prepares for the TCP connection and monitors the remote peer to start the TCP connection. Sufficient resources must be prepared before BGP is enabled.
Connect	Sends the TCP packet.	TCP connection setup is in progress. Authentication is performed during TCP connection setup. If TCP connection setup fails, BGP enters the Active state and attempts to set up the connection repeatedly.
Active	Sends the TCP packet.	TCP connection setup fails. BGP attempts to set up the connection repeatedly.
OpenSent	Sends the Open packet.	After the TCP connection has been set up, BGP sends an Open message carrying parameters to negotiate the establishment of the peer relationship.

Status	Packet	Action
OpenConfirm	Sends the Keepalive packet.	After the parameters and capabilities have been negotiated successfully, the local end sends a Keepalive packet and waits for the Keepalive packet from the peer end.
Established	Sends the Update packet.	The local end has received the Keepalive packet from the peer end, and the capabilities of the two ends are the same. Then both ends use Update packets to advertise routing information.

A.3 BGP Configuration

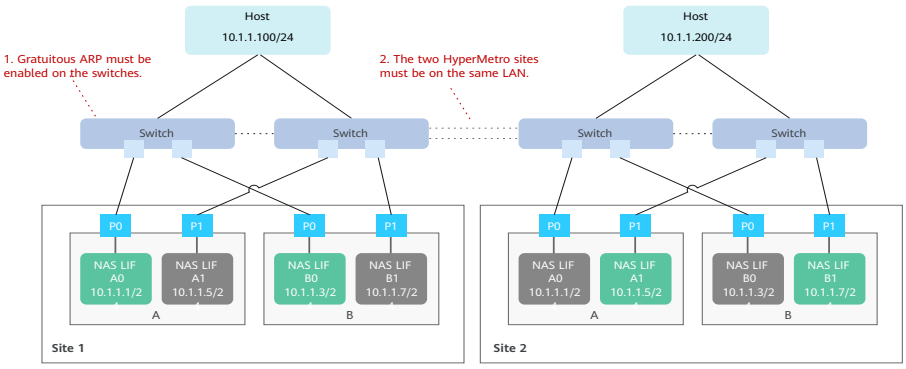
A.3.1 Typical Network Topology

Typical Networking Without Using BGP

The following provides the common networking configurations between storage systems and hosts when BGP is not used.

1. Layer 2 networking solution (IP addresses of the host and storage system are on the same network segment)

   Figure A-4 Layer 2 networking solution (IP addresses of the host and storage system are on the same network segment)



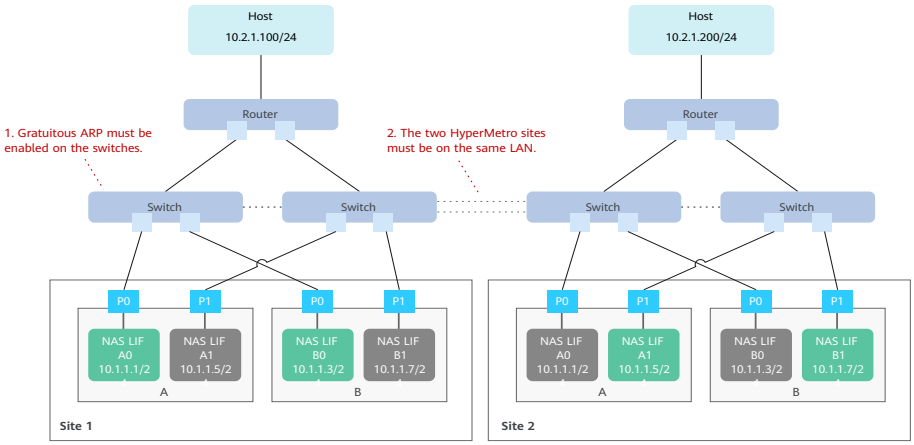
   In this solution, IP address failover is performed as follows:

   a. If a port or node is faulty, the IP address of the storage system fails over to another port or node.

   b. After the failover, the MAC address corresponding to the IP address changes. The storage system sends gratuitous ARP packets to instruct the host to update the ARP cache table, ensuring I/O continuity from the host to the storage system.

2. Layer 2 networking solution (IP addresses of the host and storage system are on different network segments)

Figure A-5 Layer 2 networking solution (IP addresses of the host and storage system are on different network segments)



In this solution, IP address failover is performed as follows:

a. Static routes are configured for NAS LIFs.

b. If a port or node is faulty, the IP address of the storage system fails over to another port or node.

c. After the failover, the MAC address corresponding to the IP address changes. The storage system sends gratuitous ARP packets to instruct the router to update the ARP cache table. Static routes are configured on the new port or node to ensure I/O continuity from the host to the storage system.

Typical Networking with BGP Used

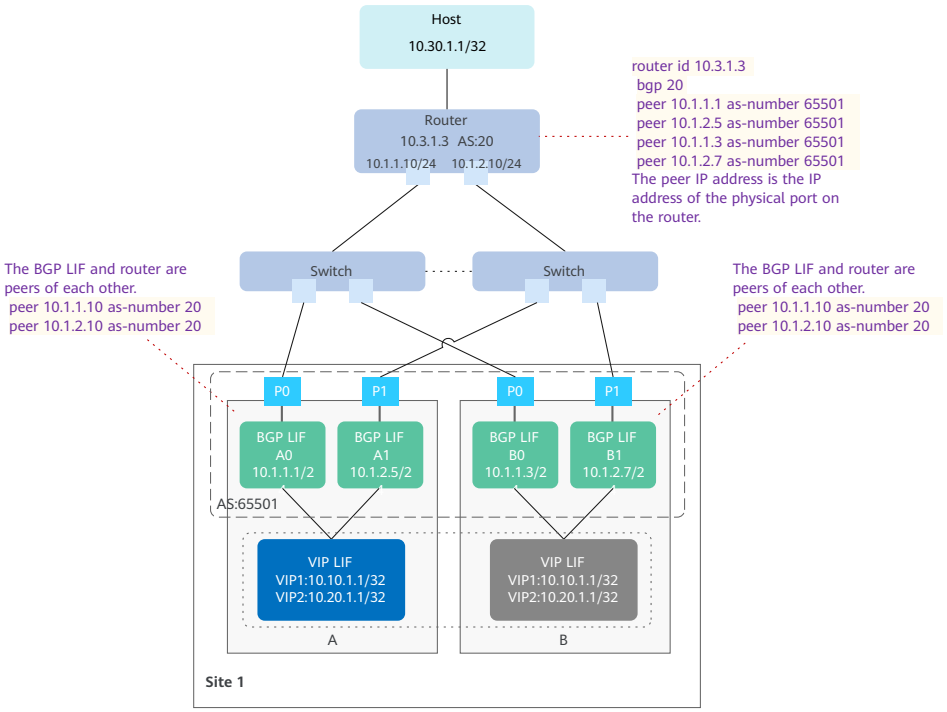
BGP is used in the following scenarios:

1. Gratuitous ARP is not configured on the user switches.
2. The two sites of HyperMetro are deployed on different LANs.

When BGP is used, the typical networking configurations between storage systems and hosts are as follows:

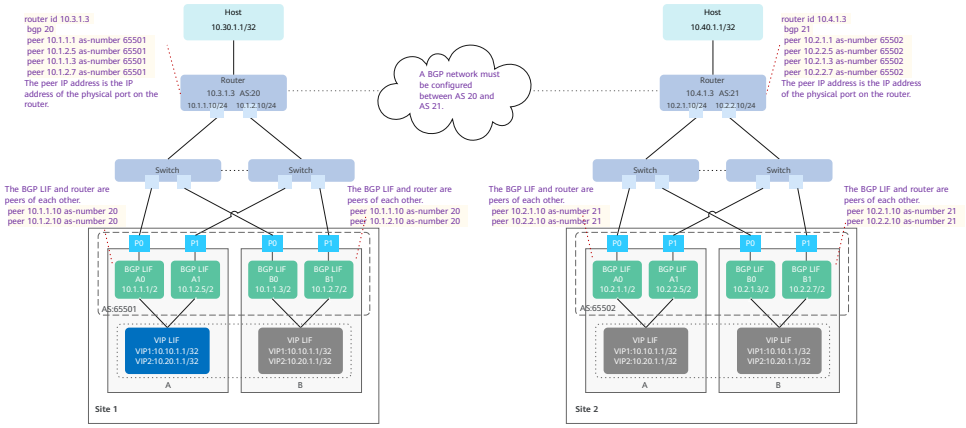
1. Layer 3 networking solution (typical configuration for a single site)
   - On the original Layer 2 networking, configure BGP peers on the egress routes of the storage system.
   - NAS LIFs can be configured on ports P0 and P1 of the storage system. LIFs on Layer 2 and Layer 3 networks can provide services at the same time.

Figure A-6 Example of Layer 3 networking (typical configuration for a single site)



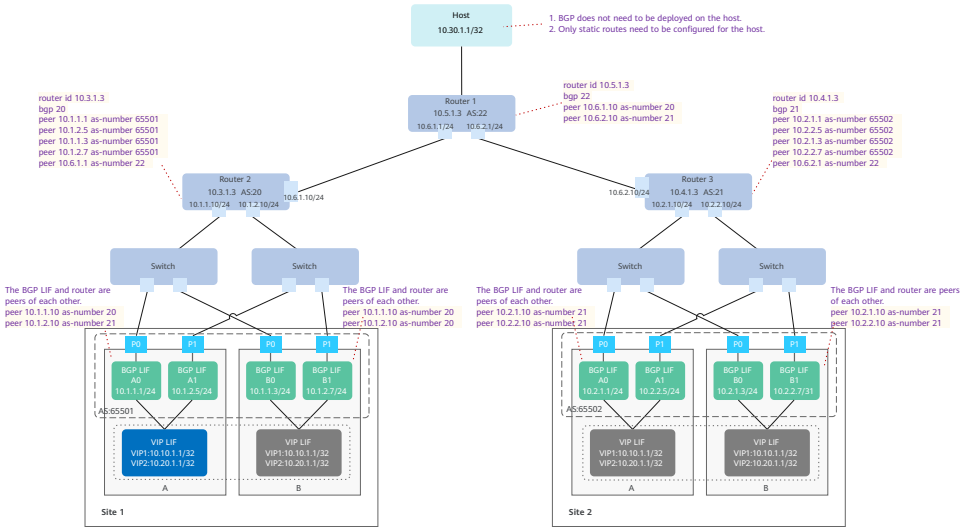
2. Layer 3 networking solution (typical configuration for two sites)
   - On the original Layer 2 networking, configure BGP peers on the egress routes of the storage system.
   - NAS LIFs can be configured on ports P0 and P1 of the storage system. LIFs on Layer 2 and Layer 3 networks can provide services at the same time.

Figure A-7 Example of Layer 3 networking (typical configuration for two sites)



3. Layer 3 networking solution (typical configuration for connecting a storage system to multiple routers)

Figure A-8 Example of Layer 3 networking (typical configuration for connecting a storage system to multiple routers)



NOTE

- The preceding three typical networking modes are recommended.
- If you use BGP ring networking (for example, in **Figure A-8**, a BGP peer is configured between Router 2 and Router 3), you are advised to change the minimum route advertisement interval (MRAI) to avoid long route switchover time in the event of a fault. For example, the default MRAI of a Huawei switch is 30 seconds. You can run the **peer** *ip-address* **route-update-interval 5** command to change it to 5 seconds. The MRAI varies with different switch models. For details, see the product documentation specific to your switch.

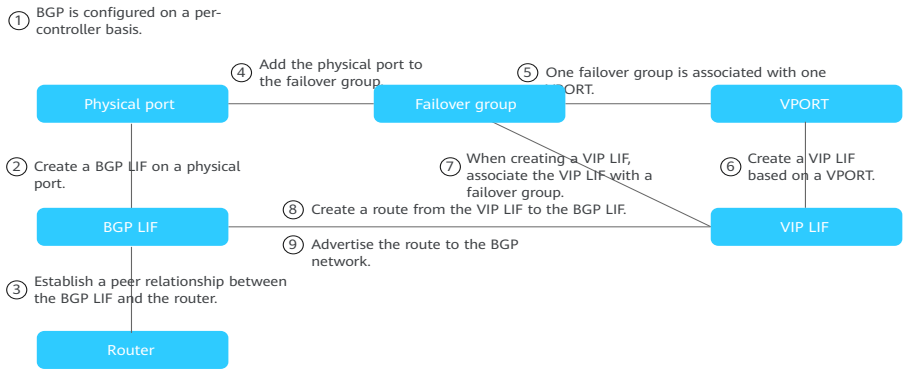
When BGP is used, IP address failover is performed as follows:

1. The BGP LIF does not provide services or synchronize data between sites, and does not support failover. The BGP LIF establishes BGP peer relationships with external routers, and then advertises VIP LIF routes to or withdraws VIP LIF routes from the external routers.
2. The VIP LIF provides services and synchronizes data between sites, and supports failover. The VIP LIF has the same functions as the NAS LIF on the Layer 2 network. If a port or a node is faulty, the VIP LIF fails over to another port or node. New static routes are configured and advertised by using the **network** command of BGP. The routes between the host and the storage system are switched over to ensure I/O continuity from the host to the storage system.

A.3.2 Storage System Configuration

Configuration Process

Figure A-9 Relationships between modules and the configuration process



1. BGP is configured on a per-controller basis.
2. Create a BGP LIF on a front-end service port (Ethernet, VLAN, or bond).
3. Establish a BGP peer relationship between the BGP LIF and the router.
4. Create a user-defined failover group and add physical ports to the group.
5. When you create the failover group, the system automatically creates a virtual port (VPORT). The VPORT status is updated with the status of the members in the failover group.
6. Create a VIP LIF based on the internal VPORT.
7. When creating a VIP LIF, you must specify a failover group and configure BGP LIFs for members in the failover group.
8. The system automatically configures static routes from the VIP LIF to the BGP LIFs corresponding to the failover group members.
9. The system automatically advertises the VIP LIF routes to the user network through BGP.

Procedure

Step 1 Create BGP configurations.

BGP configurations are created on a per-controller basis. Each controller supports only one BGP configuration.

The command is as follows:

create bgp general controller=? router_id=? [asn=?] [hold_time=?]

The **router_id** field indicates the local router ID, which is an IPv4 address. The **asn** field indicates the AS number. The **hold_time** field indicates the BGP hold time, which is an integer ranging from 3 to 65535, measured in seconds.

Example:


```
create bgp general controller=0A router_id=1.1.1.1
create bgp general controller=0B router_id=2.2.2.2 asn=65501 hold_time=180
```

Step 2 Create a BGP LIF.

The BGP LIF is a special-purpose LIF, which cannot provide NAS services independently, does not support failover, cannot be added to a DNS zone, and cannot be synchronized between two HyperMetro sites. Therefore, you must create a BGP LIF at both sites.

The BGP LIF is used to establish a peer relationship with the peer router. The BGP LIF must work with the VIP LIF to transmit and receive NAS data services. The peer router accesses the VIP LIF through the BGP LIF. The VIP LIF accesses the host IP address through the route to the BGP LIF.

The BGP LIF can be created on a front-end Ethernet port, bond port, or VLAN.

The commands are as follows:

- Creation based on a front-end Ethernet port:

  create logical_port eth name=? eth_port_id=? address_family=IPv4 ipv4_address=? ipv4_mask=? ipv4_gateway=? role=service protocol_type=BGP owner_controller=?

- Creation based on a bond port:

  create logical_port bond name=? bond_port_id=? address_family=IPv4 ipv4_address=? ipv4_mask=? ipv4_gateway=? role=service protocol_type=BGP owner_controller=?

- Creation based on a VLAN:

  create logical_port vlan name=? vlan_name=? address_family=IPv4 ipv4_address=? ipv4_mask=? ipv4_gateway=? role=service [protocol_type=BGP owner_controller=?

Example:

```
admin:/>create logical_port eth name=bgpLif eth_port_id=CTE0.B.IOM0.P0 address_family=IPv4
ipv4_address=x.x.x.x ipv4_mask=255.255.255.0 ipv4_gateway=x.x.x.x role=service protocol_type=bgp
owner_controller=0A
```

NOTE

- Set the **address_family** field to **IPv4**. BGP does not support IPv6.
- Set the **protocol_type** field to **bgp**.
- Only one IPv4 BGP LIF can be created for each front-end Ethernet port, bond port, or VLAN.
- The BGP LIFs in the same cluster must be on different network segments.
- When creating a BGP LIF, you must specify a gateway for it, which provides the egress route for the communication between the VIP LIF and host.
- For a 4 U device, you must specify the **owner_controller** parameter when creating a BGP LIF, and create a BGP LIF for each controller.

Step 3 Create a BGP peer.

The BGP LIF must establish a peer relationship with the remote router. After the peer relationship is established, the routing information of the VIP LIF is advertised to the front-end service network.

The storage system only advertises routes to the router network and does not learn external routes. Peers establish a session over the TCP port 179 for data exchange.

The command is as follows:

create bgp peer bgp_peer_name=? peer_asn=? peer_address_family=IPv4 peer_address=? bgp_lif_name=? owner_controller=?

The **bgp_peer_name** field indicates the BGP peer name. The **peer_asn** field indicates the AS number of the peer router. The **peer_address** field indicates the IP address of the peer router. The **bgp_lif_name** field indicates the BGP LIF name. The **owner_controller** field indicates the ID of the owning controller.

Example:

```
create bgp peer bgp_peer_name=test peer_asn=80 peer_address_family=IPv4 peer_address=x.x.3.1
bgp_lif_name=bgpLif owner_controller=0B
```

NOTE

The **peer_address** of the BGP peer must be different from the IP address of the storage system.

Step 4 Create a BGP failover group.

A BGP failover group is a combination of ports that can be used for VIP LIF failover in a storage system.

The commands are as follows:

- To create a BGP failover group: **create failover_group general name=? service_type=BGP ip_type=ipv4**
- To add ports to the created BGP failover group:
  - **add failover_group eth_port failover_group_name=? eth_port_list=?**
  - **add failover_group bond_port failover_group_name=? bond_port_list=?**
  - **add failover_group vlan_port failover_group_name=? vlan_port_list=?**

NOTICE

Only ports configured with a BGP LIF can be added to a BGP failover group.

Example:

```
admin:/>create failover_group general name=bgpfg service_type=BGP ip_type=ipv4
admin:/>add failover_group eth_port failover_group_name=bgpfg eth_port_list=CTE0.B.IOM0.P0
```

After a BGP failover group is created, each controller automatically creates an internal virtual port: VIP_PORT (VPORT for short).

The VPORT status is updated based on the status of the member ports in the associated failover group.

- If all member ports in the failover group associated with the VPORT are in the link down state, the VPORT status changes to link down.

- If any member port in the failover group associated with the VPORT is in the link up state, the VPORT status changes to link up.

VPORT is the home port and current port of the VIP LIF. If the VPORT status is link down, VIP LIF failover is triggered. When the VPORT status changes to link up, VIP LIF failback is triggered.

Step 5 Create a VIP LIF.

The VIP LIF is based on virtual network ports.

The functions of the VIP LIF are almost the same as those of the NAS LIF. Both of them are used for NAS services. The VIP LIF has the following capabilities:

1. Supports failover

   The current port of the VIP LIF is VPORT. The VPORT status is automatically updated with the status of the members in the associated failover group.

   If the VPORT status changes to link down, VIP LIF failover is triggered. When the VPORT status changes to link up, VIP LIF failback is triggered.

   A VIP LIF fails over from the VPORT of one controller to the VPORT of another controller.

2. Supports synchronization between HyperMetro sites by vStore

   When NAS HyperMetro is configured, the system automatically synchronizes all of the VIP LIFs, routes, and DNS zones of the vStore at the primary site to the secondary site.

   In the HyperMetro deployment, creation, deletion, or modification of a VIP LIF is automatically and incrementally synchronized to the peer site.

   If site A of HyperMetro is faulty, the VIP LIF fails over to site B. When site A recovers, the VIP LIF fails back to site A. Failover of the VIP LIF is implemented by controlling its activation status.

   For details on how to configure NAS HyperMetro, see the *HyperMetro Feature Guide for File*.

3. Supports the DNS zone

   Similar to the NAS LIF, the VIP LIF can listen to DNS requests and can be added to a DNS zone to support load balancing.

The command is as follows:

create logical_port vip name=? owner_controller=? address_family=IPv4 ipv4_address=? role=service protocol_type=? failover_group_id=?

Example:

```
create logical_port vip name=vip_b1 owner_controller=0B address_family=IPv4 ipv4_address=x.x.1.1
role=service protocol_type=NFS failover_group_id=1
```


NOTE

- The VIP LIF does not support the gateway or adding routes.
- The mask of the VIP LIF must be 32 bits and use the default configuration.
- The **protocol_type** field specifies the protocol type of the VIP LIF. The value can be **NFS**, **CIFS**, or **NFS and CIFS**.
- When a VIP LIF is created, the system automatically creates static routes from the VIP LIF to the BGP LIFs of the member ports in the failover group. When a VIP LIF is deleted, the system automatically deletes the static routes from the VIP LIF to the BGP LIFs of the member ports in the failover group.
- The system advertises the VIP LIF routes to the user network through BGP.

----End

A.3.3 Router Configuration

NOTE

- This section uses Huawei switches as an example. The configuration method varies with the switch vendor.
- For detailed BGP functions and configurations on the switch, refer to the product documentation of the switch or consult the technical support of the switch vendor.

Context

A.3.3 Router Configuration provides the default BGP configuration on Huawei switches.

Table A-5 Default BGP configuration

Parameter	Default Value
BGP	Disabled
Interval for sending keepalive messages	60 seconds
Hold time of the peer relationship	180 seconds

A.3.3.1 Configuring Basic BGP Functions

Configuring Switch Ports

Step 1 Set an Ethernet port of the switch to work in Layer 3 mode.

Example:

```
<HUAWEI> system-view
[~HUAWEI] interface 10ge 2/0/10
[~HUAWEI-10GE2/0/10]undo portswitch
[*HUAWEI-10GE2/0/10]commit
```


NOTE

- All CE series switches support switching between Layer 2 and Layer 3 modes for Ethernet ports. The ports work in Layer 2 mode by default. You can run the **undo portswitch** command in the port view to switch a port to Layer 3 mode.
- For CE6865EI, CE6855HI, CE6856HI, CE7855EI, CE8861EI, and CE8868EI, before using the **undo portswitch** and **undo portswitch batch** commands, run the **vlan reserved for main-interface** *startvlanid* **to** *endvlanid* command in the system view to configure a reserved VLAN for Layer 3 main ports.

Step 2 Configure the IP address of the Layer 3 port as the gateway address.

Example:

```
[*HUAWEI-10GE2/0/10]ip addr x.x.100.100 24
[*HUAWEI-10GE2/0/10]commit
```

----End

Configuring BGP on the Switch

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **bgp** { *as-number-plain* | *as-number-dot* } command to enable BGP, specify the AS number, and enter the BGP view.

Example:

```
[~HUAWEI]bgp 800
[*HUAWEI-bgp]router-id x.x.100.100
```

NOTE

The AS number must be different from that specified when the peer was created on the storage system.

Step 3 Configure a BGP peer.

Example:

```
[*HUAWEI-bgp]peer x.x.1.1 as-number 800
```

NOTE

The IP address must be set to the BIP LIF IP address configured on the storage system, and **as-number** must be set to the AS number configured for the owning controller of the BGP LIF.

Step 4 Check the status of BGP peer connections.

Example:

```
[~HUAWEI-bgp]disp bgp peer
 BGP local router ID        : x.x.100.100
 Local AS number            : 800
 Total number of peers      : 2
 Peers in established state : 0

  Peer          V         AS  MsgRcvd  MsgSent  OutQ  Up/Down       State  PrefRcv
  172.16.1.2    4         800        0        0     0 00:00:07        Idle        0
  172.16.2.2    4         800        0        0     0 00:00:07        Idle        0
[~HUAWEI-bgp]
```

Step 5 Enter the BGP-IPv4 unicast address family view and set BGP load balancing.

Example:


```
[~HUAWEI-bgp]ipv4-family unicast
[~HUAWEI-bgp-af-ipv4]max load-balancing 8
[*HUAWEI-bgp-af-ipv4]commit
```

After BGP is enabled on the switch, the following information is displayed:

Example:

```
[~HUAWEI-bgp]dis this
#
bgp 80
 peer x.x.3.2 as-number 65501
 peer x.x.4.2 as-number 65501
 #
 ipv4-family unicast
  network x.x.5.0 255.255.255.0
  network x.x.5.5 255.255.255.255
  maximum load-balancing 2
  peer x.x.3.2 enable
  peer x.x.4.2 enable
#

#Port configuration (using the bond port as an example)
#
interface Eth-Trunk1
 undo portswitch
 ip address x.x.10.2 255.255.255.0
 mode lacp-static
#
interface 10GE1/0/2
 eth-trunk 1
 device transceiver 10GBASE-FIBER
#
interface 10GE1/0/10
 eth-trunk 1
 device transceiver 10GBASE-FIBER
#
```

----End

A.3.3.2 Configuring BGP Reliability

Configuring BFD for BGP

BGP periodically sends Keepalive messages to its peers to detect the status of its peers. By default, it takes 3 minutes for this detection mechanism to detect a fault, which cannot meet the requirements for quick switchover of storage services in the event of a fault. BFD for BGP can solve this problem. BFD is a millisecond-level fault detection mechanism. It can fast detect faults on the link between BGP neighbors. Therefore, BFD speeds up BGP route convergence and ensures fast link switching.

When a peer joins a peer group on which BFD is enabled, BFD also takes effect on the peer and a BFD session is created on the peer. To prevent BFD from taking effect on the peer, run the **peer bfd block** command.

By default, Huawei devices establish multi-hop IBGP sessions with each other. When a Huawei device communicates with a non-Huawei device that establishes a single-hop IBGP session by default, you are advised to configure only association between IGP and BFD or association between IBGP and BFD.

NOTE

Refer to the switch product documentation to determine whether the switch supports BFD for BGP.

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **bfd** command to enable BFD globally on the local node.

Step 3 Run the **quit** command to return to the system view.

Step 4 Run the **bgp** { *as-number-plain* | *as-number-dot* } command to enter the BGP view.

Step 5 Run the **peer** { *group-name* | *ipv4-address* } **bfd enable** [**single-hop-prefer**] command to configure BFD for a peer or peer group and use default BFD parameters to establish a BFD session.

single-hop-prefer takes effect only on IBGP peers. By default, **single-hop-prefer** is not specified, and multi-hop sessions are established between directly connected IBGP peers for Huawei devices. When a Huawei device is connected to a non-Huawei device that establishes single-hop IBGP sessions by default, the **single-hop-prefer** parameter must be configured to establish single-hop IBGP sessions.

If BFD is configured on a peer group, BFD sessions are established for the peers on which **peer bfd block** is not enabled in the peer group.

Step 6 Run the **peer** { *group-name* | *ipv4-address* } **bfd min-tx-interval** *min-tx-interval* **min-rx-interval** *min-rx-interval* **detect-multiplier** *multiplier* command to set BFD detection parameters for a peer. In the command:

- The **min-tx-interval** field specifies the interval for sending BFD packets, in milliseconds. The recommended value is **600**.
- The **min-rx-interval** field specifies the interval for receiving BFD packets, in milliseconds. The recommended value is **600**.
- The **detect-multiplier** field specifies the local detection time multiplier. The recommended value is **3**.

Example:

```
[~HUAWEI-bgp] peer x.x.x.x bfd min-tx-interval 600 min-rx-interval 600 detect-multiplier 3
```

Step 7 (Optional) Run the **peer** { *ipv4-address* } **bfd block** command to prevent peers from inheriting the BFD settings of the peer group.

NOTE

- A BFD session can be established only when the BGP session is in the **Established** state.
- If BFD parameters are set on a peer, the BFD session is established based on the configurations on the peer.
- The **peer** { *ipv4-address* } **bfd block** command and **peer** { *group-name* | *ipv4-address* } **bfd enable** [**single-hop-prefer**] command are mutually exclusive.

Step 8 Verify the configuration result.

- Run the **display bgp bfd session** { [**vpnv4 vpn-instance** *vpn-instance-name*] **peer** *ipv4-address* | **all** } command to check information about the BFD session established by BGP.
- Run the **display bgp** [**vpnv4 vpn-instance** *vpn-instance-name*] **peer** [[*ipv4-address*] **verbose**] command to check BGP peer information.

- Run the **display bgp group** [*group-name*] command to check information about the BGP peer group.
- Run the **display bgp vpnv4** { **all** | **vpn-instance** *vpn-instance-name* } **group** [*group-name*] command to check information about the BGP peer group of VPNv4.

----End

Configuring BGP GR

BGP restart causes peer relationship reestablishment and traffic interruption. Graceful restart (GR) ensures uninterrupted traffic forwarding in the case of BGP restart.

BGP graceful restart (GR) is high availability solutions that minimize the impact of device failures on user services.

BGP GR ensures that the forwarding plane continues to guide data forwarding during a device restart or active/standby switchover. The operations on the control plane, such as reestablishing peer relationships and performing route calculation, do not affect the forwarding plane. This mechanism prevents service interruptions caused by route flapping and improves network reliability.

GR concepts are as follows:

- GR restarter

  The device that is restarted by the administrator or triggered by failures to perform GR.
- GR Helper

  The neighbor that helps the GR restarter to perform GR.
- GR Time

  The time during which the GR helper retains forwarding information after detecting the restart or active/standby switchover of the GR restarter.

The BGP GR process is as follows:

1. Using the BGP capability negotiation mechanism, the GR restarter and helper know each other's GR capability and establish a GR session.
2. When detecting the restart or active/standby switchover of the GR restarter, the GR helper waits to reestablish a BGP connection with the GR restarter. It does not delete the routing information and forwarding entries of the GR restarter or notify other neighbors of the restart or switchover.
3. The GR restarter reestablishes neighbor relationships with all GR helpers before the GR time expires.

Step 1 Run the **system-view** command to enter the system view.

Step 2 Run the **bgp** { *as-number-plain* | *as-number-dot* } command to enter the BGP view.

Step 3 Run the **graceful-restart** command to enable BGP GR.

By default, BGP GR is disabled.

Step 4 (Optional) Run the **graceful-restart timer wait-for-rib** *timer* command to set the time for the restarting speaker and receiving speaker to wait for the End-of-RIB message.

The default time for waiting for an End-of-RIB message is 600 seconds.

Step 5 (Optional) Run the **graceful-restart peer-reset** command to enable the device to reset a BGP connection in GR mode.

By default, a device cannot reset a BGP connection in GR mode.

Step 6 Verify the configuration result.

Run the **display bgp peer verbose** command to check the BGP GR status.

----End

A.4 Managing BGP

This section provides some CLI commands for managing BGP.

NOTE

For more CLI commands and their description, see the Command Reference specific to your product model and version.

Managing BGP Configurations

Table A-6 Commands for managing BGP configurations

Operation	Command
Creating BGP configurations	create bgp general controller=? asn=? hold_time=? router_id=?
Querying BGP configurations	show bgp general controller=?
Modifying BGP configurations	change bgp general controller=? asn=? hold_time=? router_id=?
Deleting BGP configurations	delete bgp general controller=?

Managing BGP LIFs

Table A-7 Commands for managing BGP LIFs

Operation	Command
Creating a BGP LIF	• Creation based on a front-end Ethernet port: create logical_port eth name=? eth_port_id=? address_family=IPv4 ipv4_address=? ipv4_mask=? ipv4_gateway=? role=service protocol_type=BGP owner_controller=? • Creation based on a bond port: create logical_port bond name=? bond_port_id=? address_family=IPv4 ipv4_address=? ipv4_mask=? ipv4_gateway=? role=service protocol_type=BGP owner_controller=? • Creation based on a VLAN: create logical_port vlan name=? vlan_name=? address_family=IPv4 ipv4_address=? ipv4_mask=? ipv4_gateway=? role=service protocol_type=BGP owner_controller=?
Querying a BGP LIF	show logical_port general protocol_type=BGP
Modifying a BGP LIF	change logical_port general
Deleting a BGP LIF	delete logical_port general logical_port_name=?

Managing BGP Peers

Table A-8 Commands for managing BGP peers

Operation	Command
Creating a BGP peer	create bgp peer peer_name=? logical_port_name=? peer_asn=? peer_address=?
Querying a BGP peer	show bgp peer peer_name=?
Modifying a BGP peer	change bgp peer peer_name=? logical_port_name=? peer_asn=? peer_address=?
Deleting a BGP peer	delete bgp peer peer_name=?

Managing BGP Failover Groups

Table A-9 Commands for managing BGP failover groups

Operation	Command

Creating a BGP failover group	• To create a BGP failover group:
	`create failover_group general name=? service_type=BGP ip_type=ipv4`
	• To add ports to the created BGP failover group:
	– Adding an Ethernet port:
	`add failover_group eth_port failover_group_name=? eth_port_list=?`
	– Adding a bond port:
	`add failover_group bond_port failover_group_name=? bond_port_list=?`
	– Adding a VLAN:
	`add failover_group vlan_port failover_group_name=? vlan_port_list=?`

Querying a BGP failover group	`show failover_group general service_type=BGP`
Modifying a BGP failover group	`change failover_group general failover_group_name=? name=?`

Removing a port from a user-defined BGP failover group:	• To remove an Ethernet port:
	`remove failover_group eth_port failover_group_name=? eth_port_list=?`
	• To remove a bond port:
	`remove failover_group bond_port failover_group_name=? bond_port_list=?`
	• To remove a VLAN:
	`remove failover_group vlan_port failover_group_name=? vlan_port_list=?`

Deleting a BGP failover group	`delete failover_group general failover_group_name=?`

Managing VIP LIFs

Table A-10 Commands for managing VIP LIFs

Operation	Command
Creating a VIP LIF	`create logical_port vip name=? owner_controller=? address_family=IPv4 ipv4_address=? role=service protocol_type=? failover_group_id=?`
Querying a VIP LIF	`show logical_port general home_port_type=VIP`
Modifying a VIP LIF	`change logical_port general`
Deleting a VIP LIF	`delete logical_port general logical_port_name=?`

B Obtaining and Configuring Manila Driver

Manila Driver is a plug-in that is deployed on the OpenStack Manila module. The plug-in can be used to provide functions such as the sharing configuration for virtual machines (VMs) in OpenStack.

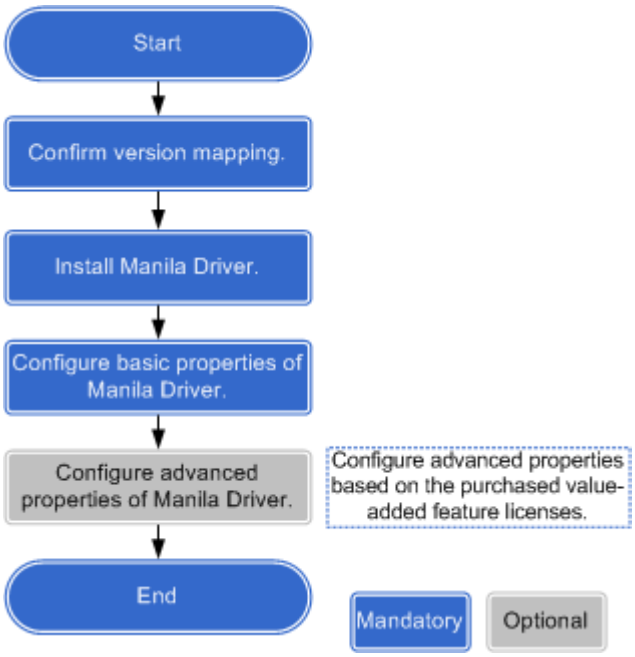
Obtaining Manila Driver

You can obtain the plug-in from Huawei OpenStack Driver repository (**https://github.com/Huawei/OpenStack_Driver**).

Configuration Roadmap

Figure B-1 shows the configuration roadmap of Manila Driver.

Figure B-1 Manila Driver configuration roadmap



For the specific steps of configuring Manila Driver, see the configuration guide released with Manila Driver.

C Configuring Basic Storage Services Using the CLI

This section provides some CLI commands for configuring basic file storage services.

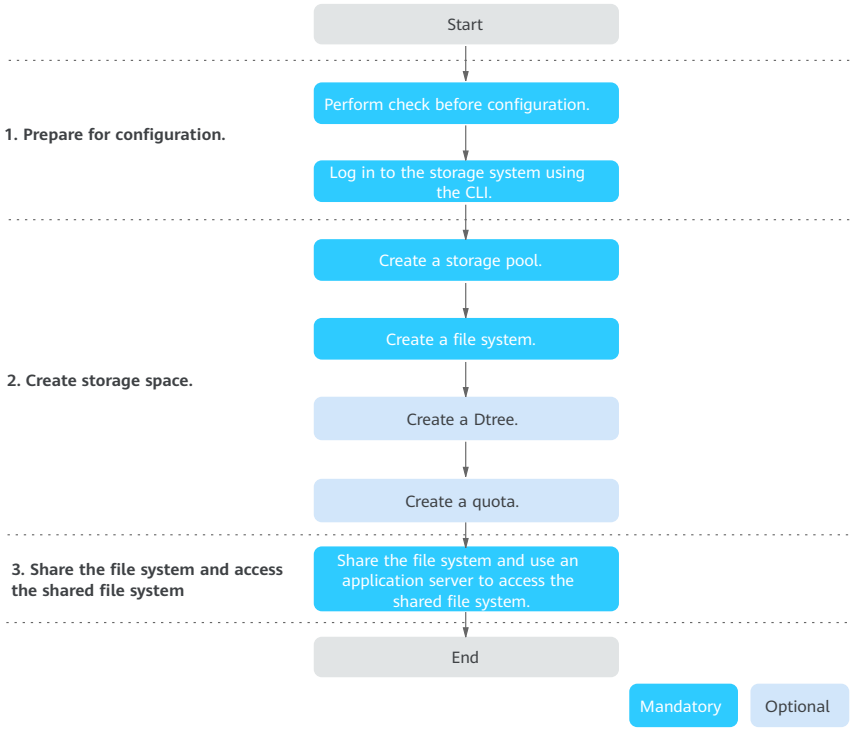
NOTE

- The CLI commands supported by different models may vary.
- For more CLI commands and their description, see the Command Reference specific to your product model and version.

Configuration Process

The following flowchart shows the common configuration process.

Figure C-1 Process for configuring the file storage service



Preparing for the Configuration

Table C-1 Preparations

Item	Reference
Pre-check (network connection status check and compatibility check)	For details, see **3.2 Check Before Configuration**.
Logging in to the storage system using the CLI	For details, see "Logging In to the CLI" in the *Initialization Guide*.

Creating Storage Space

Table C-2 Commands for creating storage space

Procedure	Command
Creating a storage pool	create storage_pool **NOTE** • When you run the **create storage_pool** command to create a storage pool, the system automatically creates a disk domain in the background. • You can also run the **create disk_domain** and **create storage_pool** commands to create a disk domain and a storage pool, respectively. If you run the **create disk_domain** command to create a disk domain separately, the default redundancy policy is disk redundancy. If you want to create a storage pool with enclosure redundancy, add **redundancy_strategy=enclosure** in the command to create a disk domain.
Creating a file system	create file_system general
Creating a dtree	create dtree general
Creating a quota	create quota file_system create quota dtree

Sharing a File System and Accessing the Shared File System

Table C-3 Some commands related to network configurations

Operation	Command
Creating a bond port	create bond_port
Creating a VLAN	create vlan general
Creating a DNS zone	create dns_zone general
Creating a logical port	• Creating a logical port based on a bond port: create logical_port bond • Creating a VLAN-based logical port: create logical_port vlan • Creating a logical port based on an Ethernet port: create logical_port eth
Setting DNS load balancing	change system dns_load_balance

Operation	Command
Adding a route for a logical port	• IPv4 network: add logical_port ipv4_route • IPv6 network: add logical_port ipv6_route

Table C-4 Commands for domain configurations

Operation	Command
Modifying the LDAP domain authentication configurations	change domain ldap_config
Modifying the advanced LDAP domain authentication configurations	change domain ldap_schema
Modifying the NIS domain authentication configurations	change domain nis_config
Modifying the AD domain authentication configurations	change domain ad_config
Configuring the IP address of the service DNS server within a vStore	change domain dns_config

Table C-5 Commands for NFS shares

Operation	Command
Creating an NFS share	create share nfs
Creating NFS share permissions	create share_permission nfs
Accessing a share	For details, see **3.8.1.11 Accessing an NFS Share**.

Table C-6 Commands for CIFS shares

Operation	Command
Creating a local Windows authentication user group	create windows_group general
Creating a local Windows authentication user	create windows_user general
Creating a CIFS share	create share cifs
Creating CIFS share permissions	create share_permission cifs

Operation	Command
Accessing a share	For details, see **3.8.3.9 Accessing a CIFS Share**.

Table C-7 Commands for CIFS Homedir shares

Operation	Command
Creating a local Windows authentication user group	create windows_group general
Creating a local Windows authentication user	create windows_user general
Creating a CIFS Homedir share	create share cifs
Creating a mapping rule for a CIFS Homedir share	create share_homedir_rule cifs
Accessing a share	For details, see **3.8.4.9 Accessing a CIFS Homedir Share**.

Table C-8 Commands related to cross-protocol share access

Operation	Command
Modifying user mapping configurations	change identity_mapping config
Adding a user mapping rule	add identity_mapping rule

D Managing Basic Storage Services Using the CLI

This section provides some CLI commands for managing file storage services.

NOTE

- The CLI commands supported by different models may vary.
- For more CLI commands and their description, see the Command Reference specific to your product model and version.

Managing Storage Pools

Table D-1 Commands for managing storage pools

Operation	Command
Creating a storage pool	create storage_pool
Querying storage pools	show storage_pool general
Modifying a storage pool	change storage_pool general
Deleting a storage pool	delete storage_pool

Managing File Systems

Table D-2 Commands for managing file systems

Operation	Command
Creating a file system	create file_system general
Querying file systems	show file_system general
Modifying a file system	change file_system general
Deleting a file system	delete file_system general

Operation	Command
Enabling or disabling file system functions	change file_system enabled

Managing Dtrees

Table D-3 Commands for managing dtrees

Operation	Command
Creating a dtree	create dtree general
Querying dtrees	show dtree general
Modifying a dtree	change dtree
Deleting a dtree	delete dtree general
Querying the number of dtrees	show dtree count

Managing Quotas

Table D-4 Commands for managing quotas

Operation	Command
Creating a quota	create quota file_system create quota dtree
Querying quotas	show quota general
Modifying a quota	change quota general
Deleting a quota	delete quota general

Managing the Service Network

Table D-5 Commands for managing bond ports

Operation	Command
Creating a bond port	create bond_port
Querying bond ports	show bond_port
Modifying a bond port	change bond_port general
Deleting a bond port	delete bond_port

Table D-6 Commands for managing VLANs

Operation	Command
Creating a VLAN	create vlan general
Querying VLANs	show vlan general
Modifying a VLAN	change vlan general
Deleting a VLAN	delete vlan general

Table D-7 Commands for managing logical ports

Operation	Command
Creating a logical port	• Creating a logical port based on a bond port: create logical_port bond • Creating a VLAN-based logical port: create logical_port vlan • Creating a logical port based on an Ethernet port: create logical_port eth
Querying logical ports	show logical_port general
Modifying a logical port	change logical_port general
Deleting a logical port	delete logical_port general
Adding a route for a logical port	• IPv4 network: add logical_port ipv4_route • IPv6 network: add logical_port ipv6_route
Querying routes of a logical port	show logical_port route
Deleting routes of a logical port	• IPv4 network: remove logical_port ipv4_route • IPv6 network: remove logical_port ipv6_route
Failing over to a logical port	change logical_port failback
Configuring the failover group for a logical port	change logical_port failover_group

Table D-8 Commands for managing built-in DNS load balancing

Operation	Command
Enabling or disabling the DNS load balancing function and configuring the load balancing policy	change system dns_load_balance
Querying information about DNS load balancing	show system dns_load_balance
Creating a zone for the built-in DNS server	create dns_zone general
Querying zones of the built-in DNS server	show dns_zone general
Changing the name of a DNS zone	change dns_zone general
Deleting a specified DNS zone	delete dns_zone general

Managing Local Authentication Users

Table D-9 Commands for managing local Windows authentication users

Operation	Command
Creating a local Windows authentication user	create windows_user general
Querying local Windows authentication users	show windows_user general
Modifying a local Windows authentication user	change windows_user general
Deleting a local Windows authentication user	delete windows_user
Querying the password and login policies of a Windows user	show windows_user safe_strategy
Changing the password and login policies of a Windows user	change windows_user safe_strategy
Changing the password of a Windows user	change windows_user password

Table D-10 Commands for managing local Windows authentication user groups

Operation	Command
Creating a local Windows authentication user group	create windows_group general
Querying local Windows authentication user groups	show windows_group general
Querying Windows users in a Windows user group	show windows_group windows_user
Querying AD domain users in a Windows user group	show windows_group ad_user
Querying AD domain user groups in a Windows user group	show windows_group ad_group
Modifying a local Windows authentication user group	change windows_group general
Deleting a local Windows authentication user group	delete windows_group
Adding a Windows user to a Windows user group	add windows_group windows_user
Adding a domain user to a Windows user group	add windows_group ad_user
Adding a domain user group to a Windows user group	add windows_group ad_group
Removing a Windows user from a Windows user group	remove windows_group windows_user
Removing an AD domain user from a Windows user group	remove windows_group ad_user
Removing an AD domain user group from a Windows user group	remove windows_group ad_group

Table D-11 Commands for managing local UNIX authentication users

Operation	Command
Creating a local UNIX authentication user	create unix_user general
Querying local UNIX authentication users	show unix_user general
Modifying a local UNIX authentication user	change unix_user general

Operation	Command
Deleting a local UNIX authentication user	delete unix_user

Table D-12 Commands for managing local UNIX authentication user groups

Operation	Command
Creating a local UNIX authentication user group	create unix_group
Querying local UNIX authentication user groups	show unix_group general
Modifying a local UNIX authentication user group	change unix_group general
Deleting a local UNIX authentication user group	delete unix_group
Adding a UNIX user to a UNIX user group	add unix_group_member
Removing a UNIX user from a UNIX user group	remove unix_group_member

Table D-13 Commands for managing user mappings

Operation	Command
Adding a user mapping rule	add identity_mapping rule
Querying user mapping rules	show identity_mapping rule
Querying user mapping configurations	show identity_mapping config
Checking whether a user can be queried after being mapped	show identity_mapping mapped_user
Modifying user mapping configurations	change identity_mapping config
Modifying a user mapping rule	change identity_mapping rule
Clearing the user mapping cache	clear identity_mapping cache
Clearing user mapping configurations	clear identity_mapping config

Managing Domain Configurations

Table D-14 Commands for LDAP domain configurations

Operation	Command
Modifying the LDAP domain authentication configurations	change domain ldap_config
Modifying the advanced LDAP domain authentication configurations	change domain ldap_schema
Querying the LDAP domain authentication configurations	show domain ldap
Querying the advanced LDAP domain authentication configurations	show domain ldap_schema
Testing the connectivity of the LDAP server	test domain ldap
Deleting LDAP domain configurations	delete domain ldap
Deleting advanced LDAP domain configurations	delete domain ldap_schema

Table D-15 Commands for NIS domain configurations

Operation	Command
Modifying the NIS domain authentication configurations	change domain nis_config
Querying the NIS domain authentication configurations	show domain nis
Testing the connectivity of the NIS server	test domain nis
Deleting NIS domain configurations	delete domain nis

Table D-16 Commands for AD domain configurations

Operation	Command
Modifying the AD domain authentication configurations	change domain ad_config

Operation	Command
Configuring and modifying the preferred domain controller	change domain ad_prefdc
Viewing AD domain controller configurations	show domain ad
Querying the preferred domain controller	show domain ad_prefdc
Testing the connectivity of the AD domain server	test domain ad
Querying the domain controller list	show domain controller
Querying sessions between a storage system and an AD domain	show domain session

Table D-17 Commanding for DNS servers

Operation	Command	Reference
Configuring the IP address of the file DNS server for a vStore	change domain dns_config	For details, see **change domain dns_config** in the *Command Reference*.
Querying the IP address of the DNS server for a vStore	show domain dns	For details, see **show domain dns** in the *Command Reference*.
Testing the connectivity of the DNS server	test domain dns	For details, see **test domain dns** in the *Command Reference*.
Deleting a DNS server	delete domain dns	For details, see **delete domain dns** in the *Command Reference*.

Managing Shares

Table D-18 Commands for managing NFS shares

Operation	Command
Creating an NFS share	create share nfs
Querying NFS shares	show share nfs

Operation	Command
Modifying NFS share configurations	change share nfs
Deleting an NFS share	delete share nfs
Creating NFS share permissions	create share_permission nfs
Querying NFS share permissions	show share_permission nfs
Modifying NFS share permissions	change share_permission nfs
Deleting NFS share permissions	delete share_permission nfs
Querying public NFS configurations	show service nfs_config
Modifying public NFS configurations	change service nfs_config

Table D-19 Commands for managing CIFS shares

Operation	Command
Creating a CIFS share	create share cifs
Querying CIFS shares	show share cifs
Modifying CIFS share configurations	change share cifs
Deleting a CIFS share	delete share cifs
Creating CIFS share permissions	create share_permission cifs
Querying CIFS share permissions	show share_permission cifs
Modifying CIFS share permissions	change share_permission cifs
Deleting CIFS share permissions	delete share_permission cifs
Querying the CIFS share service	show service cifs
Querying the public CIFS configurations	show service cifs_config
Modifying CIFS share service configurations	change service cifs
Modifying the public CIFS configurations	change service cifs_config

Table D-20 Commands for managing CIFS Homedir shares

Operation	Command
Creating a CIFS Homedir share	create share cifs name=? local_path=? share_type=homedir
Querying CIFS Homedir shares	show share cifs share_type=homedir
Modifying CIFS Homedir share configurations	change share cifs
Deleting a CIFS Homedir share	delete share cifs
Creating a mapping rule for a CIFS Homedir share	create share_homedir_rule cifs
Querying mapping rules for a CIFS Homedir share	show share_homedir_rule cifs
Modifying the mapping rule of a CIFS Homedir share	change share_homedir_rule cifs
Deleting a mapping rule from a CIFS Homedir share	delete share_homedir_rule cifs

E How to Obtain Help

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

E.1 Preparations for Contacting Huawei

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

E.1.1 Collecting Troubleshooting Information

You need to collect troubleshooting information before troubleshooting.

You need to collect the following information:

- Name and address of the customer
- Contact person and telephone number
- Time when the fault occurred
- Description of the fault phenomena
- Device type and software version
- Measures taken after the fault occurs and the related results
- Troubleshooting level and required solution deadline

E.1.2 Making Debugging Preparations

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

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

E.2 How to Use the Document

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

To better solve the problems, use the documents before you contact Huawei for technical support.

E.3 How to Obtain Help from Website

Huawei provides users with timely and efficient technical support through the regional offices, secondary technical support system, telephone technical support, remote technical support, and onsite technical support.

Huawei technical support system includes:

- Huawei headquarters technical support department
- Regional office technical support center
- Customer service center
- Technical support website: **https://support.huawei.com/enterprise/**

You can query how to contact the regional offices at **https://support.huawei.com/enterprise/**.

E.4 Ways to Contact Huawei

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

Huawei Technologies Co., Ltd.

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

Website: **https://e.huawei.com/en/**

F 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) on the network. Application programs of data services run on the application server.

Asynchronous remote replication A kind of remote replication. When the data at the primary site is updated, the data does not need to be updated synchronously at the mirroring site to finish the update. In this way, performance is not reduced due to data mirroring.

Air baffle It optimizes the ventilation channels and improves the heat dissipation capability of the system.

Audit log guarantee mode A mode for recording audit logs. This mode preferentially ensures that the audit log function is normal and no audit log is missing.

Audit log non-guarantee mode A mode for recording audit logs. In this mode, services are running properly. Audit logs may be missing.

B

Backup A collection of data stored on (usually removable) non-volatile storage media for purposes of recovery in case the original copy of data is lost or becomes inaccessible; also called a backup copy. To be useful for recovery, a backup must be made by copying the source data image when it is in a consistent state. The act of creating a backup.

Backup window	An interval of time during which a set of data can be backed up without seriously affecting applications that use the data.
Bandwidth	The numerical difference between the upper and lower frequencies of a band of electromagnetic radiation. A deprecated synonym for data transfer capacity that is often incorrectly used to refer to throughput.
Baud rate	The maximum rate of signal state changes per second on a communications circuit. If each signal state change corresponds to a code bit, then the baud rate and the bit rate are the same. It is also possible for signal state changes to correspond to more than one code bit, so the baud rate may be lower than the code 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	The probability that a transmitted bit will be erroneously received. The bit error rate (BER) is measured by counting the number of bits in error at the output of a receiver and dividing by the total number of bits in the transmission. BER is typically expressed as a negative power of 10.
Bonding	Bonding of multiple independent physical network ports into a logical port, which ensures the high availability of server network connections and improves network performance.
Boundary scan	A test methodology that uses shift registers in the output connections of integrated circuits (ICs). One IC is often connected to the next IC. 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 known as Joint Test Action Group (JTAG).
Browser/Server	Architecture that defines the roles of the browser and server. The browser is the service request party and the server is the service provider.
Built-in FRU Alarm indicator	It indicates errors on the built-in FRUs of a controller, such as errors on fans or memory modules.

C

Cache hit ratio	The ratio of the number of cache hits to the number of all I/Os during a read task, usually expressed as a percentage.
Captive screw	Specially designed to lock into place on a parent board or motherboard, allowing for easy installation and removal of attached pieces without release of the screw.
Challenge Handshake Authentication Protocol	A password-based authentication protocol that uses a challenge to verify that a user has access rights to a system. A hash of the supplied password with the challenge is sent for comparison so the cleartext password is never sent over the connection.
Compliance mode	A protection mode of WORM. In compliance mode, files within their protection period cannot be changed or deleted by either the file user or by the system administrator. Files with expired protection periods can be deleted but not changed by the file user or the system administrator.
Controller	The control logic in a disk or tape that performs command decoding and execution, host data transfer, serialization and deserialization of data, error detection and correction, and overall management of device operations. The control logic in a storage subsystem that performs command transformation and routing, aggregation (RAID, mirroring, striping, or other), high-level error recovery, and performance optimization for multiple storage devices.
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.
Copying	A pair state. The state indicates that the source LUN data is being synchronized to the target LUN.
Container root directory	Space used to store the metadata for running container images and container instances.
Container image	An image is a special file system, which provides the programs, libraries, resources, and configuration files required for running containers. It also contains configuration parameters, for example, for anonymous disks, environment variables, and users. The image does not contain dynamic data, and its content will not be modified after construction.
Containerized application	An image can start multiple containers, and an application can contain one or a group of containers.

Container node	Controller that runs the container service.
Configuration item list	A series of modifiable configuration items defined in the Helm chart of the container.
Container service	Containerized application management service, which manages the lifecycle of containerized applications.

D

Data compression	The process of encoding data to reduce its size. Lossy compression (i.e., compression using a technique in which a portion of the original information is lost) is acceptable for some forms of data (e.g., digital images) in some applications, but for most IT applications, lossless compression (i.e., compression using a technique that preserves the entire content of the original data, and from which the original data can be reconstructed exactly) is required.
Data flow	A process that involves processing data extracted from the source system. These processes include: 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	A movement of data or information between information systems, formats, or media. Migration is performed for reasons such as possible decay of storage media, obsolete hardware or software (including obsolete data formats), changing performance requirements, the need for cost efficiencies etc.
Data source	A system, database (database user; database instance), or file that can make BOs persistent.
Dirty data	Data that is stored temporarily on the cache and has not been written onto disks.
Disaster recovery	The recovery of data, access to data and associated processing through a comprehensive process of setting up a redundant site (equipment and work space) with recovery of operational data to continue business operations after a loss of use of all or part of a data center. This involves not only an essential set of data but also an essential set of all the hardware and software to continue processing of that data and business. Any disaster recovery may involve some amount of down time.

Disk array	A set of disks from one or more commonly accessible disk subsystems, combined with a body of control software. The control software presents the disks' storage capacity to hosts as one or more virtual disks. Control software is often called firmware or microcode when it runs in a disk controller. Control software that runs in a host computer is usually called a volume manager.
Disk domain	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 enclosure	Consists of the following parts in redundancy: expansion module, disk, power module, and fan module. System capacity can be expanded by cascading multiple disk enclosures.
Disk location	The process of locating a disk in the storage system by determining the enclosure ID and slot ID of the disk.
Disk utilization	The percentage of used capacity in the total available capacity.

E

eDevLUN	Logical storage array space created by a third-party storage array.
Expansion module	A component used for expansion.
Expansion	Connects a storage system to more disk enclosures through connection cables, expanding the capacity of the storage system.

F

Field replaceable unit	A unit or component of a system that is designed to be replaced in the field, i.e., without returning the system to a factory or repair depot. Field replaceable units may either be customer-replaceable or their replacement may require trained service personnel.
Firmware	Low-level software for booting and operating an intelligent device. Firmware generally resides in read-only memory (ROM) on the device.

Flash Translation Layer	Flash Translation Layer (FTL) organizes and manages host data, enables host data to be allocated to NAND flash chips of SSDs in an orderly manner, maintains the mapping relationship between logical block addresses (LBAs) and physical block addresses (PBAs), and implements garbage collection, wear leveling, and bad block management.
Front-end port	The port that connects the controller enclosure to the service side and transfers service data. Front-end port types are Fibre Channel and iSCSI.
Front-end interconnect I/O module (FIM)	On a storage device, all controllers share the front-end interface modules.

G

Garbage collection	The process of reclaiming resources that are no longer in use. Garbage collection has uses in many aspects of computing and storage. For example, in flash storage, background garbage collection can improve write performance by reducing the need to perform whole block erasures prior to a write.
Gateway	A device that receives data via one protocol and transmits it via another.
Global garbage collection	With a view to defragmentation of storage arrays and garbage collection of disks, global garbage collection reduces garbage of disks by enabling storage arrays to inform disks of not implementing invalid data relocation and of controlling space release so that disks and controllers consume less space, reducing costs and prolonging the useful life of storage arrays.
Global system for mobile communications	The second-generation mobile networking standard defined by the European Telecommunications Standards Institute (ETSI). It is aimed at designing a standard for global mobile phone networks. GSM consists of three main parts: mobile switching subsystem (MSS), base station subsystem (BSS), and mobile station (MS).
Global wear leveling	With a view to individual characteristics of a single disk, global wear leveling uses space allocation and write algorithms to achieve wear leveling among disks, preventing a disk from losing efficacy due to excessive writes and prolonging the useful life of the disk.

H

Hard disk tray	The tray that bears the hard disk.
Heartbeat	Heartbeat supports node communication, fault diagnosis, and event triggering. Heartbeats are protocols that require no acknowledgement. They are transmitted between two devices. The device can judge the validity status of the peer device.
Hit ratio	The ratio of directly accessed I/Os from the cache to all I/Os.
Hot swap	The substitution of a replacement unit (RU) in a system for a defective unit, where the substitution can be performed while the system is performing its normal functioning normally. Hot swaps are physical operations typically performed by humans.
HyperMetro	A value-added service of storage systems. HyperMetro means 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 generally; made up of two storage arrays and one quorum server. HyperMetro services can be created on a HyperMetro domain.
HyperMetro vStore pair	A HyperMetro vStore pair consists of two vStores, that is, two tenants. After a HyperMetro relationship is set up for a pair of vStores, the datasets in the two vStores work in redundancy mode and provide storage services in one dataset view, achieving hitless service failover.
HyperMetro-Inner	On an eight-controller network, with HyperMetro-Inner, continuous mirroring, back-end global sharing, and three-copy technologies, a storage system can tolerate one-by-one failures of seven controllers among eight controllers, concurrent failures of two controllers, and failure of a controller enclosure.
HyperDetect	HyperDetect is a feature that provides ransomware detection.
Handle	A handle resides on the structural part of a module. It is used to insert or remove a module into or from a chassis, not helpful in saving efforts.
Helm chart	A Helm chart is in TAR format. It is similar to the deb package of APT or the rpm package of Yum. It contains a group of yaml files that define Kubernetes resources.

I

In-band management The management control information of the network and the carrier service information of the user network are transferred through the same logical channel. In-band management enables users to manage storage arrays through commands. Management commands are sent through service channels, such as I/O write and read channels. The advantages of in-band management include high speed, stable transfer, and no additional management network ports required.

Initiator The system component that originates an I/O command over an I/O interconnect. The endpoint that originates a SCSI I/O command sequence. I/O adapters, network interface cards, and intelligent I/O interconnect control ASICs are typical initiators.

I/O Shorthand for input/output. I/O is the process of moving data between a computer system's main memory and an external device or interface such as a storage device, display, printer, or network connected to other computer systems. This encompasses reading, or moving data into a computer system's memory, and writing, or moving data from a computer system's memory to another location.

Intelligent ransomware detection The system detects known ransomware features to identify whether the file systems are attacked by ransomware. If no ransomware attack is identified, the system analyzes and compares the changes in file system snapshots, and uses machine learning algorithms to further check whether the file systems are infected by ransomware.

Interface module A replaceable field 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/Os or computing requests to physical resources of the system.

Logical unit The addressable entity within a SCSI target that executes I/O commands.

Logical unit number The SCSI identifier of a logical unit within a target. Industry shorthand, when phrased as "LUN", for the logical unit indicated by the logical unit number.

LUN formatting	The process of writing 0 bits in the data area of the logical drive and generating related parity bits so that the logical drive can be in the ready state.
LUN mapping	A storage system maps LUNs to application servers so that application servers can access storage resources.
LUN migration	A method for the LUN data to migrate between different physical storage spaces while ensuring data integrity and uninterrupted operation of host services.
LUN snapshot	A type of snapshot created for a LUN. This snapshot is both readable and writable and is mainly used to provide a snapshot LUN from point-in-time LUN data.
Lever	A lever resides on the structural part of a module. It is used to insert or remove a module into or from a chassis, saving efforts.
Local image repository	A private repository used to store the container images and Helm charts imported by users. It is different from the standard image repository. The imported images and Helm charts must meet the compatibility requirements of the system.

M

Maintenance terminal	A computer connected through a serial port or management network port. It maintains the storage system.
Management interface module	The module that integrates one or more management network ports.
Management network	An entity that provides means to transmit and process network management information.
Management network port	The network port on the controller enclosure connected to the maintenance terminal. It is provided for the remote maintenance terminal. Its IP address can be modified with the change of the customer's environment.

N

NVM Express	A host controller interface with a register interface and command set designed for PCI Express-based SSDs.

NVMe SSD	A solid state disk (SSD) with a non-volatile memory express (NVMe) interface. Compared with other SSDs, such SSDs can deliver higher performance and shorter latency.

O

Out-of-band management	A management mode used during out-of-band networking. The management and control information of the network and the bearer service information of the user network are transmitted through different logical channels.

P

Power failure protection	When an external power failure occurs, the AC PEM depends on the battery for power supply. This ensures the integrity of the dirty data in the cache.
Pre-copy	When the system monitors a failing member disk in a RAID group, the system copies the data from the disk to a hot spare disk in advance.
Palm-sized NVMe SSD	A palm-sized NVMe SSD is a type of NVMe SSD of which the dimensions (H x W x D) are 160 mm x 79.8 mm x 9.5 mm (neither 3.5-inch nor 2.5-inch).

Q

Quorum server	A server that can provide arbitration services for clusters or HyperMetro to prevent the resource access conflicts of 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 redundancy 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.

Ransomware file interception	When launching attacks, ransomware usually generates encrypted files with special file name extensions. In light of this, the system intercepts the write to files with specific file name extensions to block the extortion from known ransomware and protect file systems in the storage system.
Real-time ransomware detection	Ransomware has similar I/O behavior characteristics. By analyzing file I/O behavior characteristics, the system quickly filters out abnormal files and performs deep content analysis on the abnormal files to detect files attacked by ransomware. Then, secure snapshots are created for file systems where files have been attacked, and alarms are reported to notify the data protection administrator, limiting the impact of ransomware and reducing losses.
Reconstruction	The regeneration and writing onto one or more replacement disks of all of the user data and check data from a failed disk in a mirrored or RAID array. In most arrays, a rebuild can occur while applications are accessing data on the array's virtual disks.
Redundancy	The inclusion of extra components of a given type in a system (beyond those required by the system to carry out its function) for the purpose of enabling continued operation in the event of a component failure.
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 mirrors 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.
Reverse synchronization	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. On a TCP/IP network, each IP packet is routed independently. Routes can change dynamically.

S

Script	A parameterized list of primitive I/O interconnect operations intended to be executed in sequence. Often used with respect to ports, most of which are able to execute scripts of I/O commands autonomously (without policy processor assistance). A sequence of instructions intended to be parsed and carried out by a command line interpreter or other scripting language. Perl, VBScript, JavaScript and Tcl are all scripting languages.
Serial port	An input/output location (channel) that sends and receives data (one bit at a time) to and from the CPU of a computer or a communications device. Serial ports are used for serial data communication and as interfaces for some peripheral devices, such as mouse devices 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.
Simple network management protocol	An IETF protocol for monitoring and managing systems and devices in a network. The data being monitored and managed is defined by an MIB. The functions supported by the protocol are the request and retrieval of data, the setting or writing of data, and traps that signal the occurrence of events.
Single point of failure	One component or path in a system, the failure of which would make the system inoperable.
Slot	A position defined by an upper guide rail and the corresponding lower guide rail in a frame. A slot houses a board.
Small computer system interface	A collection of ANSI standards and proposed standards that define I/O interconnects primarily intended for connecting storage subsystems or devices to hosts through host bus adapters. Originally intended primarily for use with small (desktop and desk-side workstation) computers, SCSI has been extended to serve most computing needs, and is arguably the most widely implemented I/O interconnect in use today.
Snapshot	A point in time copy of a defined collection of data. Clones and snapshots are full copies. Depending on the system, snapshots may be of files, LUNs, file systems, or any other type of container supported by the system.
Snapshot copy	A copy of a snapshot LUN.

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 system	An integrated system that 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 to the actual storage media used to back up data.
Streaming media	Streaming media is media continuously streamed over the network. Combining technologies concerning streaming media data collection, compression, encoding, storage, transmission, playback, and network communications, streaming media can provide high-quality playback effects in real time at low bandwidth.
Subnet	A type of smaller network that forms a larger network according to a rule, such as, forming a network according to different districts. This facilitates the management of a large network.
Smart disk enclosure	Being compared with traditional disk enclosures, the smart disk enclosures are equipped with Arm chips and DDR memories or other computing modules to achieve powerful computing capabilities. With such capabilities, the smart disk enclosures can help controllers to share some computing loads, accelerating data processing.
Share authentication	During vStore configuration synchronization, the share authentication information (including the share information and domain controller configuration) is synchronized to the secondary end.

T

Target	The endpoint that receives a SCSI I/O command sequence.
Target LUN	The LUN on which target data resides.
Thin LUN	A logic disk that can be accessed by hosts. It dynamically allocates storage resources from the thin pool according to the actual capacity requirements of users.

Topology	The logical layout of the components of a computer system or network and their interconnections. Topology deals with questions of what components are directly connected to other components from the standpoint of being able to communicate. It does not deal with questions of physical location of components or interconnecting cables. The communication infrastructure that provides Fibre Channel communication among a set of PN_Ports (e.g., a Fabric, an Arbitrated Loop, or a combination of the two).
Trim	A method by which the host operating system may inform a storage device of data blocks that are no longer in use and can be reclaimed. Many storage protocols support this functionality via various names, e.g., ATA TRIM and SCSI UNMAP.

U

User interface	The space where users interact with a machine.
U-shaped bracket	It is an optional structural part like letter "U". It is located between the mounting ear of a chassis and the mounting bar of a cabinet or bay and is used to adjust the locations of the chassis and mounting bar of the cabinet or bay.

W

Wear leveling	A set of algorithms utilized by a flash controller to distribute writes and erases across the cells in a flash device. Cells in flash devices have a limited ability to survive write cycles. The purpose of wear leveling is to delay cell wear out and prolong the useful life of the overall flash device.
Write amplification	Increase in the number of write operations by the device beyond the number of write operations requested by hosts.
Write amplification factor	The ratio of the number of write operations on the device to the number of write operations requested by the host.

Write back	A caching technology in which the completion of a write request is signaled as soon as the data is in the cache. Actual writing to non-volatile media occurs at a later time. Write back includes inherent risks: an application will take 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 these reasons, sufficient write back implementations include mechanisms to preserve cache contents across system failures (including power failures) and a flushed cache at system restart time.
Write Once Read Many	A type of storage, designed for fixed content, that preserves what is written to it in an immutable fashion. Optical disks are an example of WORM storage.
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 equipped with the write through technology is approximately that of a non-cached system. However, if the written data is also held in a cache, subsequent read performance may be dramatically improved.

Z

Zone	A collection of Fibre Channel N_Ports and/or NL_Ports (i.e., device ports) that are permitted to communicate with each other via the fabric. Any two N_Ports and/or NL_Ports that are not members of at least one common zone are not permitted to communicate via the fabric. Zone membership may be specified by: 1) port location on a switch, (i.e., Domain_ID and port number); or, 2) the device's N_Port_Name; or, 3) the device's address identifier; or, 4) the device's Node_Name. Well-known addresses are implicitly included in every zone.

G Acronyms and Abbreviations

A	
AD	Active Directory
C	
CLI	Command Line Interface
D	
DNS	Domain Name Server
G	
GUI	Graphical User Interface
I	
IP	Internet Protocol
L	
LDAP	Lightweight Directory Access Protocol
M	
MMC	Microsoft Management Console
N	
NAS	Network Attached Storage
NFS	Network File System
NTFS	New Technology File System
NTLM	NT LAN Manager

NTP	Network Time Protocol
S	
SSH	Secure Shell

OceanStor
6.1.x

HyperMetro Feature Guide for Block

Issue	02
Date	2022-08-25

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: https://e.huawei.com

Contents

1 About This Document

Purpose

This document describes HyperMetro and provides an overview of its configuration, management, and usage scenarios.

The following table lists the product models that support HyperMetro.

Product Model	Product Version
OceanStor 5310	6.1.3 6.1.5
OceanStor 5510	
OceanStor 5610	
OceanStor 6810	
OceanStor 18510	
OceanStor 18810	

NOTICE

This document is updated periodically with the software version. The operations described in this document use the latest version as an example. Note that the supported functions and features vary according to the software version. The content in this document is for reference only.

Intended Audience

This document is intended for:

- Technical support engineers
- Maintenance engineers

Symbol Conventions

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

Symbol	Description
DANGER	Indicates a hazard with a high level of risk which, if not avoided, will result in death or serious injury.
WARNING	Indicates a hazard with a medium level of risk which, if not avoided, could result in death or serious injury.
CAUTION	Indicates a hazard with a low level of risk which, if not avoided, could result in minor or moderate injury.
NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
NOTE	Supplements the important information in the main text. 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 previous issues.

Issue 02 (2022-08-25)

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

- Added the description about IPsec supported by replication links.
- Optimized descriptions.

Issue 01 (2022-01-25)

This issue is the first official release.

2 Overview

This chapter describes the architecture, highlights, and working principles of the active-active storage solution for SAN, also known as HyperMetro.

2.1 About HyperMetro

This section describes the logical architecture and highlights of the active-active DC solution.

HyperMetro is Huawei's active-active storage solution that enables two storage systems to process services simultaneously, establishing a mutual backup relationship between them. In the event of a device fault or DC failure, the other functioning DC automatically takes over services. This ensures robust reliability, enhanced service continuity, and high storage resource utilization.

Huawei provides the active-active storage architecture based on OceanStor storage systems to ensure uninterrupted service running for customers. This architecture supports both single-data center (DC) and cross-DC deployment modes.

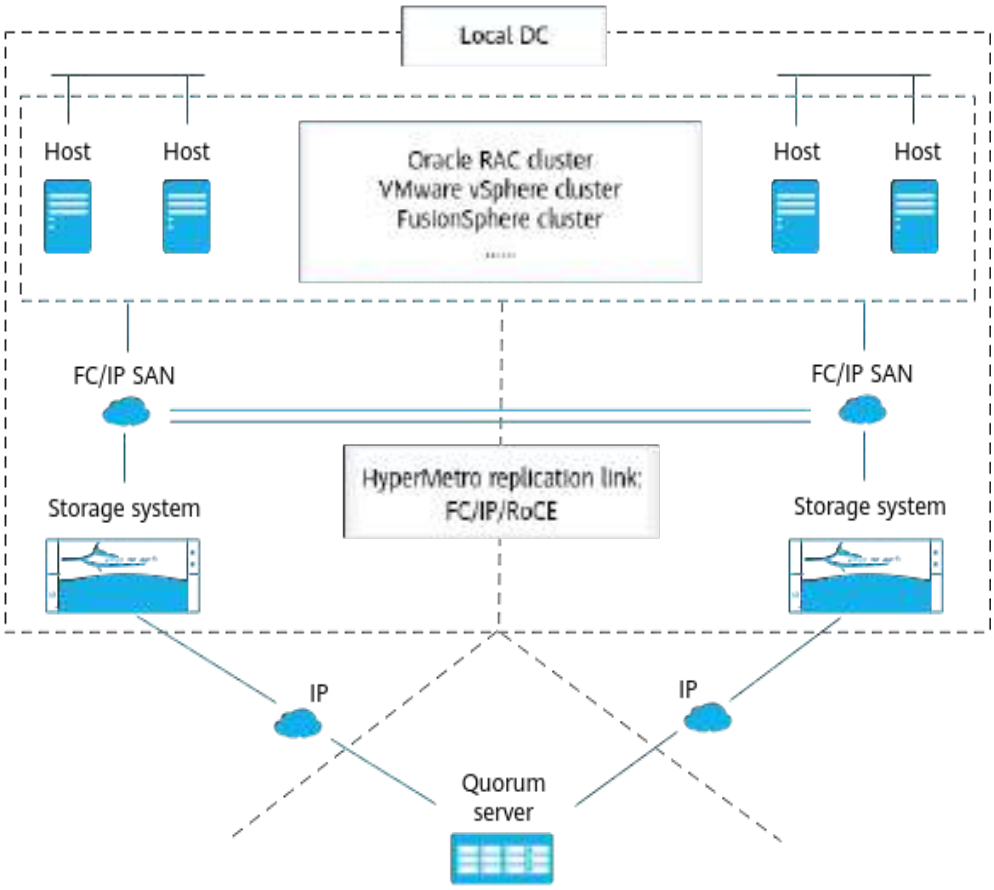
- Single-DC deployment

  In this mode, the active-active storage systems are deployed in two equipment rooms in the same campus.

  Hosts are deployed in a cluster. Hosts communicate with storage systems through a switched fabric (Fibre Channel or IP). Dual-write mirroring channels are deployed on the storage systems to ensure continuous operation of active-active services.

  Figure 2-1 shows the logical diagram of the solution.

Figure 2-1 Single-DC deployment



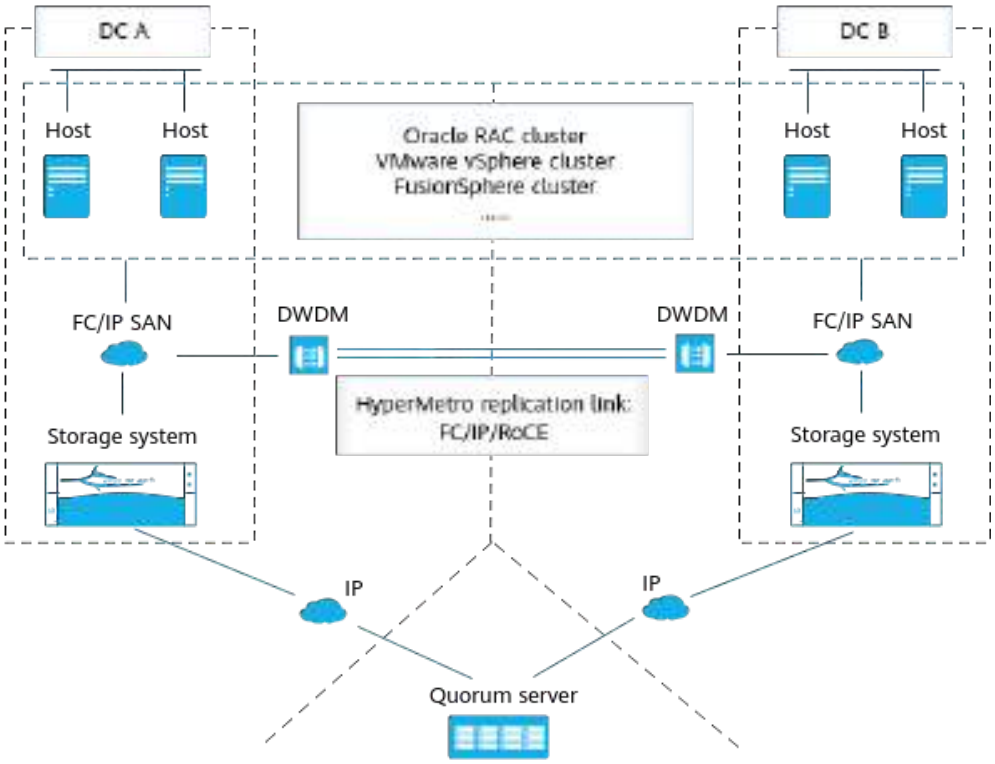
- Cross-DC deployment

  In this mode, the active-active storage systems are deployed in two DCs in the same city or in two cities located in close proximity. The distance between the two DCs is within 300 km. Both of the DCs can handle service requests concurrently, thereby accelerating service response and improving resource utilization. If one DC fails, its services are automatically switched to the other DC.

  In cross-DC deployment scenarios involving long-distance transmission, dense wavelength division multiplexing (DWDM) devices must be used to ensure a short transmission latency. In addition, mirroring channels must be deployed between the active-active storage systems for data synchronization.

  Figure 2-2 shows an example of the cross-DC deployment mode.

Figure 2-2 Cross-DC deployment



The active-active DC solution for SAN has the following highlights:

- Dual-write ensures data redundancy on the storage systems. In the event of a storage system or DC failure, services are switched over to the other DC at zero RTO and RPO, ensuring service continuity without any data loss.

  NOTE

  In typical clusters, HyperMetro achieves zero RTO. In virtual clusters, the RTO is approximately equal to zero because VMs will be automatically restored on other hosts if a host in the cluster becomes faulty.

- Both DCs provide services simultaneously, fully utilizing DR resources.
- The active-active solution ensures 24/7 service continuity. The gateway-free design reduces potential fault points, further enhancing system reliability.
- HyperMetro can work with HyperReplication to form a geo-redundant layout comprising three DCs.

With these highlights, HyperMetro is well suitable to various industries such as health care, finance, and social insurance.

2.2 Basic Concepts

This section provides the key concepts associated with HyperMetro.

Protected Object

For customers, the protected objects are LUNs or protection groups. That is, HyperMetro is configured for LUNs or protection groups for data backup and disaster recovery.

- Data protection can be implemented for each individual LUN.
- Data protection can be implemented for a protection group, which consists of multiple independent LUNs or a LUN group.

Protection Group (PG) and LUN Group

A LUN group can be directly mapped to a host for the host to use storage resources. You can group LUNs for different hosts or applications.

A protection group (PG) applies to data protection with consistency groups. You can plan data protection policies for different applications and components in the applications. In addition, you can enable unified protection for LUNs used by multiple applications in the same protection scenario. For example, you can group the LUNs to form a LUN group, map the LUN group to a host or host group, and create a protection group for the LUN group to implement unified data protection of the LUNs used by multiple applications in the same protection scenario.

HyperMetro Domain

A HyperMetro domain allows application servers to access data across DCs. It consists of a quorum server and the local and remote storage systems.

HyperMetro Pair

A HyperMetro pair is created between a local and a remote LUN within a HyperMetro domain. The two LUNs in a HyperMetro pair have an active-active relationship. You can examine the state of the HyperMetro pair to determine whether operations such as synchronization, suspension, or priority switchover are required by its LUNs and whether such an operation is performed successfully.

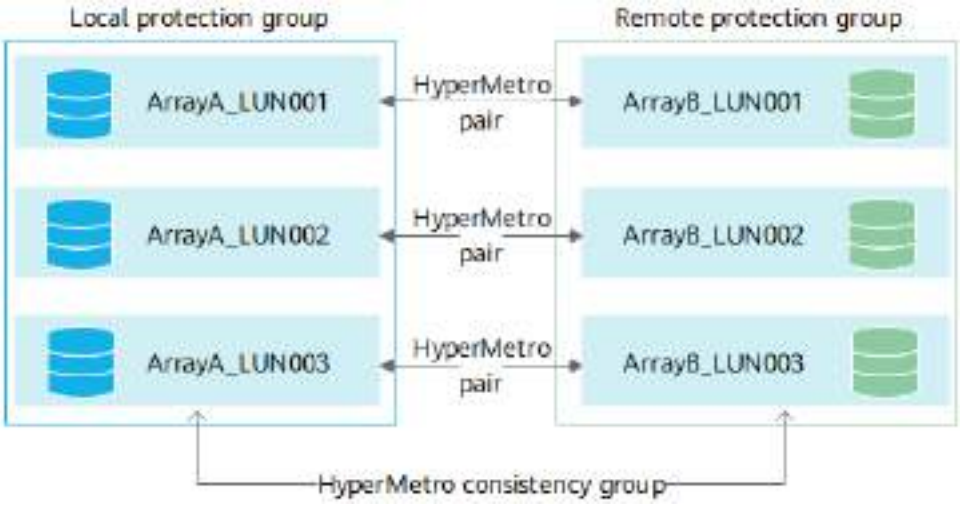
HyperMetro Consistency Group (CG)

A HyperMetro consistency group (CG) is created based on a protection group. It is a collection of HyperMetro pairs that have a service relationship with each other. For example, the service data, logs, and change tracking information of a medium- or large-size database are stored on different LUNs of a storage system. Placing these LUNs in a protection group and then creating a HyperMetro consistency group for that protection group can preserve the integrity of their data and guarantee write-order fidelity.

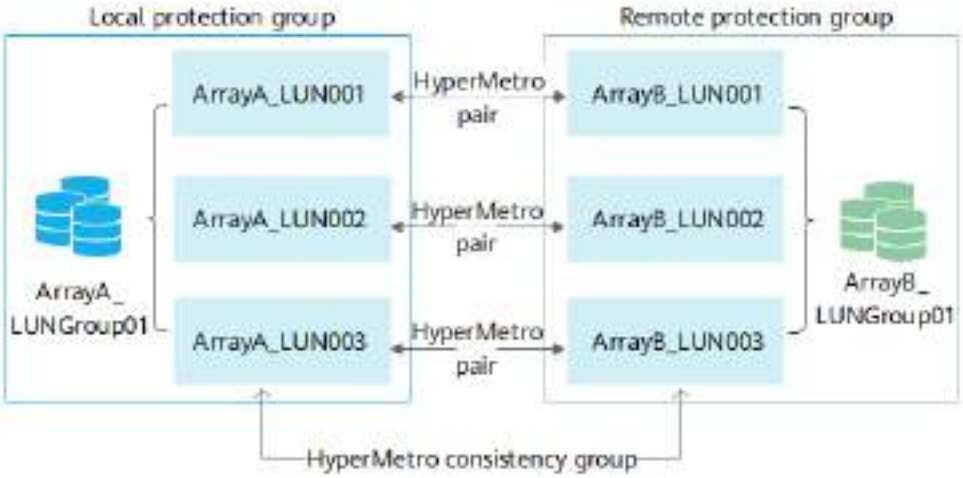
Relationships Between LUNs, Protection Groups, HyperMetro Pairs, and HyperMetro Consistency Groups

Creating a HyperMetro pair for an individual LUN:

Creating a HyperMetro consistency group for a protection group (formed by multiple independent LUNs)



Creating a HyperMetro consistency group for a protection group (formed by a LUN group)



Dual-Write

Dual-write enables the synchronization of application I/O requests with both local and remote LUNs.

DCL

Data change logs (DCLs) record changes to the data in the storage systems.

Synchronization

HyperMetro synchronizes differential data between the local and remote LUNs in a HyperMetro pair. You can also synchronize data among multiple HyperMetro pairs in a consistency group.

Pause

Pause is a state indicating the suspension of a HyperMetro pair.

Force Start

To ensure data consistency in the event that multiple elements in the HyperMetro deployment malfunction simultaneously, HyperMetro stops hosts from accessing both storage systems. You can forcibly start the local or remote storage system (depending on which one is normal) to restore services quickly.

Preferred Site Switchover

Preferred site switchover indicates that during arbitration, precedence is given to the storage system which has been set as the preferred site (by default, this is the local storage system). If the HyperMetro replication network is down, the storage system that wins arbitration continues providing services to hosts.

FastWrite

FastWrite uses the First Burst Enabled function of the SCSI protocol to optimize data transmission between storage devices, reducing the number of interactions in a data write process by half.

2.3 Functions of a HyperMetro Consistency Group

A consistency group ensures that the read/write control policies of the multiple LUNs on a storage system are consistent.

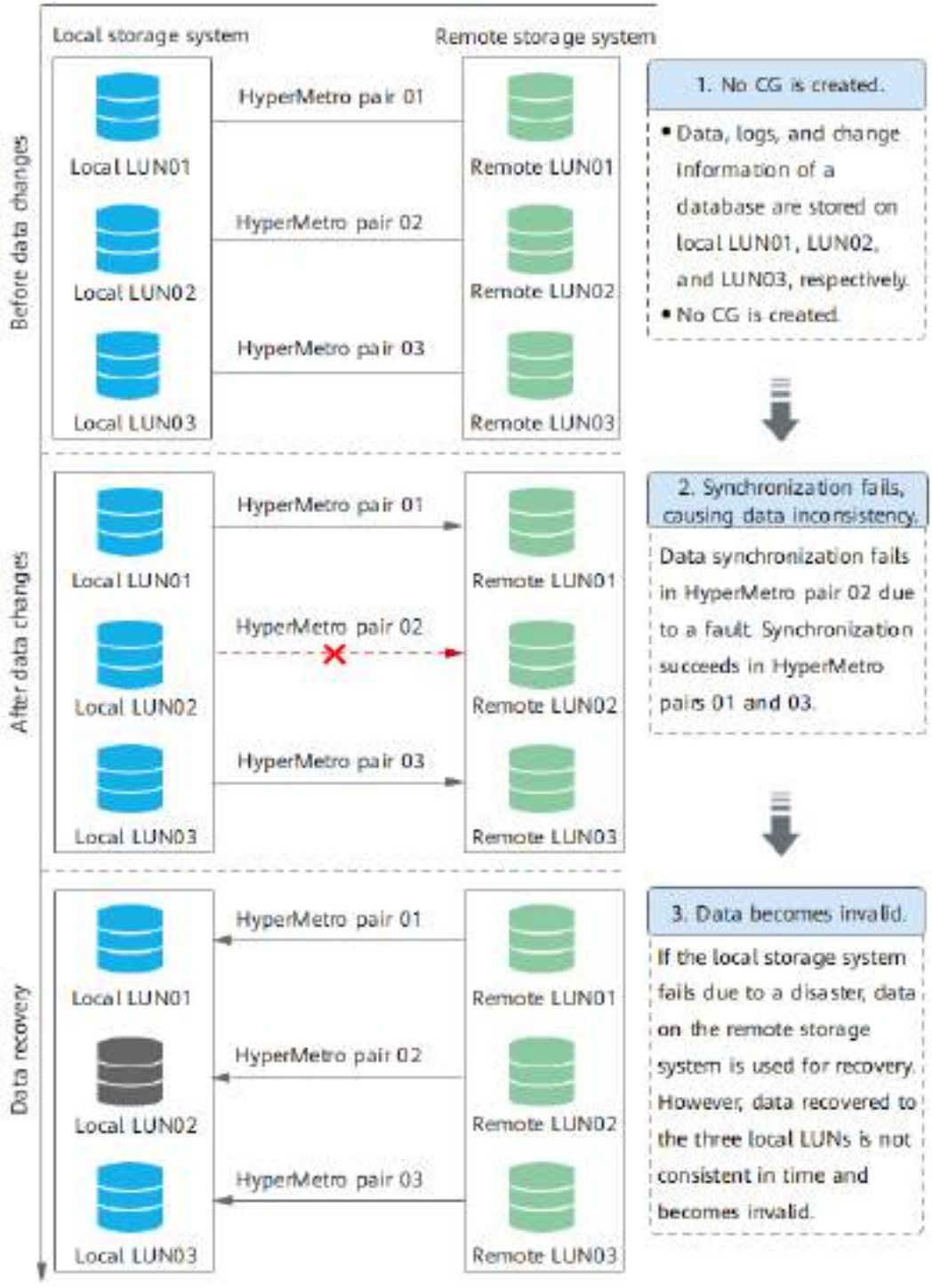
In medium- and large-size databases, the user data and logs are stored on different LUNs. If data on any LUN is lost or becomes inconsistent in time with the data on other LUNs, data on all of the LUNs becomes invalid. Creating a HyperMetro consistency group for these LUNs can preserve the integrity of their data and guarantee write-order fidelity.

The following compares data synchronizations with and without a consistency group.

Without a HyperMetro Consistency Group

If LUNs are not added to a HyperMetro consistency group, there is a high probability of data loss on these LUNs, as shown in **Figure 2-3**.

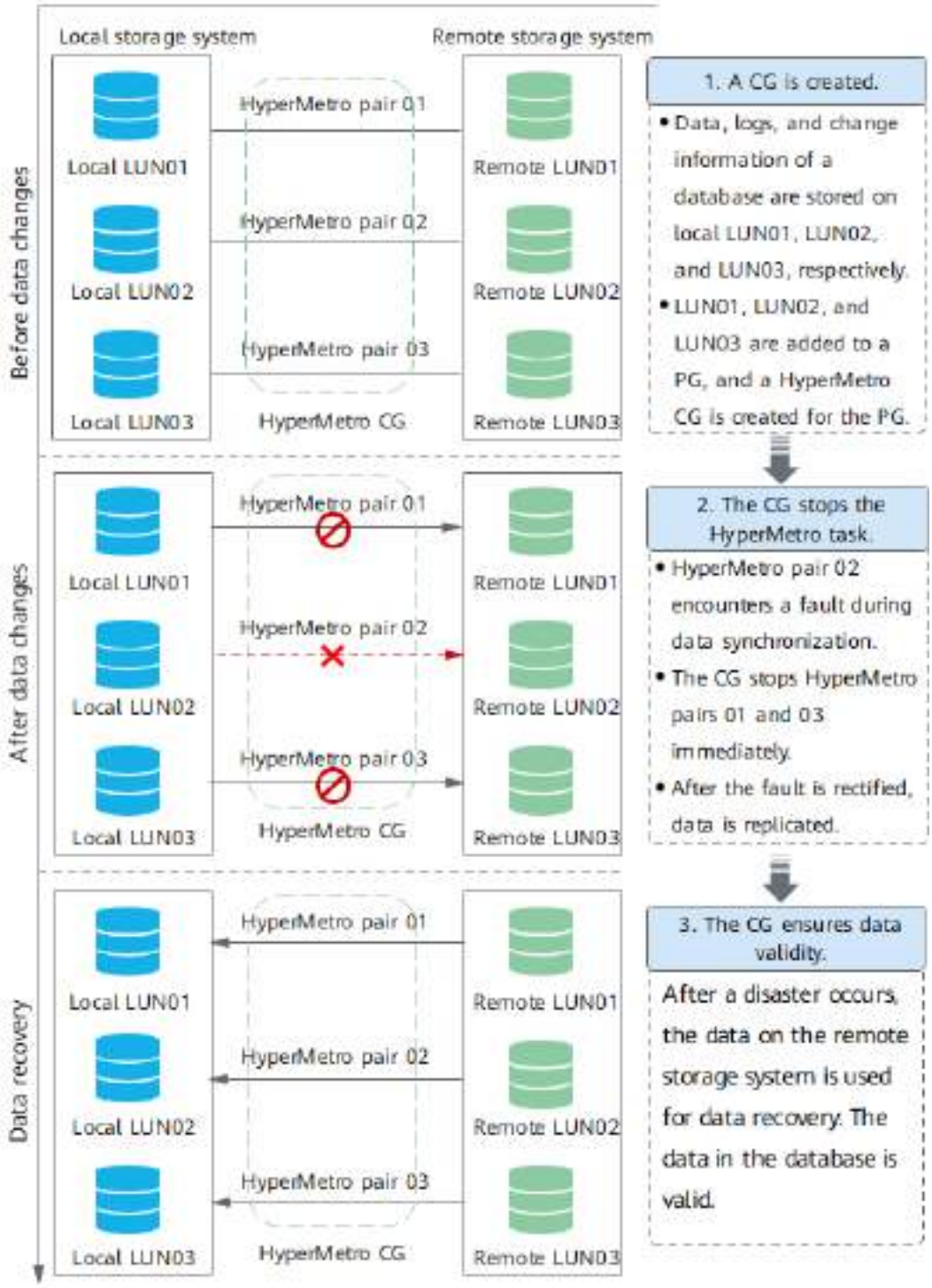
Figure 2-3 Without a HyperMetro consistency group



With a HyperMetro Consistency Group

If LUNs are added to a HyperMetro consistency group, no data is lost, as shown in **Figure 2-4**.

Figure 2-4 With a HyperMetro consistency group



2.4 HyperMetro I/O Processing Mechanism

HyperMetro uses dual-write and data change log (DCL) to synchronize data changes between the storage systems in two DCs, ensuring data consistency. The storage systems in both DCs provide services for hosts concurrently.

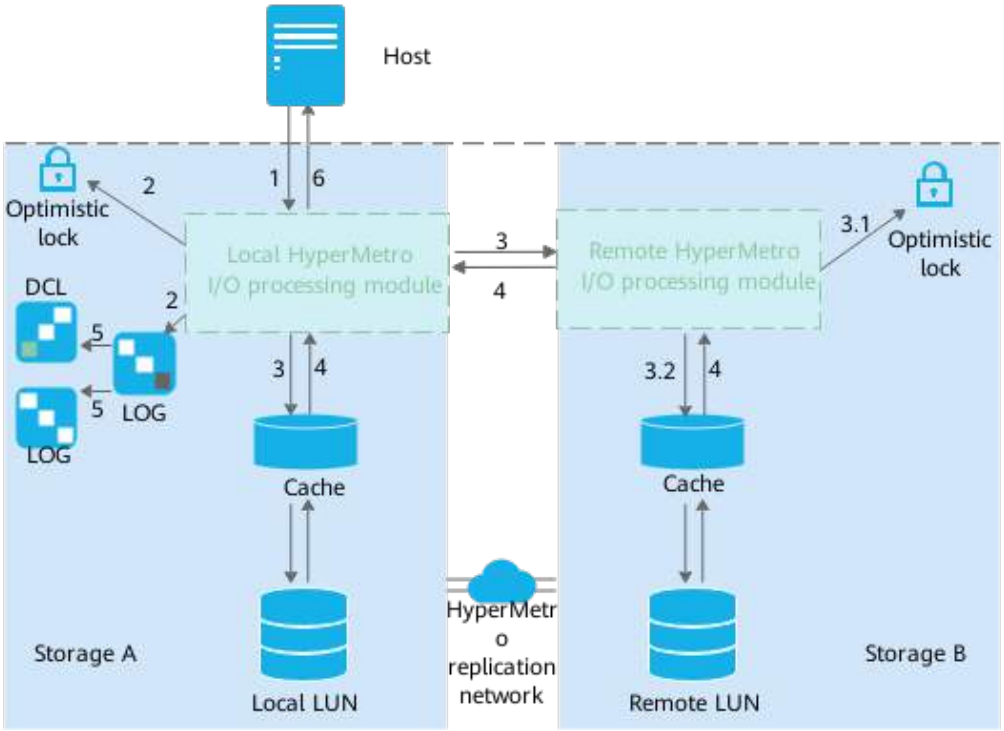
Write I/O Process

Dual-write and locking mechanisms are essential for data consistency between storage systems.

- Dual-write and DCL technologies synchronize data changes while services are running. Dual-write enables hosts' I/O requests to be delivered to both local and remote caches, ensuring data consistency between the caches. If the storage system in one DC malfunctions, the DCL records data changes. After the storage system recovers, the data changes are synchronized to the storage system, ensuring data consistency across DCs.
- Two HyperMetro storage systems can process hosts' I/O requests concurrently. To prevent conflicts when different hosts access the same data on a storage system simultaneously, a locking mechanism is used to allow only one storage system to write data. The storage system denied by the locking mechanism must wait until the lock is released and then obtain the write permission.

Figure 2-5 shows an example of the write I/O process in which a host delivers an I/O request to the local storage system and dual-write is used to write the data to the remote storage system.

Figure 2-5 Write I/O process



1. A host delivers a write I/O to the HyperMetro I/O processing module.
2. The write I/O applies for write permission from the optimistic lock on the local storage system. After write permission is obtained, the system records the address information in the log but does not record the data content.
3. The HyperMetro I/O processing module writes the data to the caches of both the local and remote LUNs concurrently. When data is written to the remote storage system, the write I/O applies for write permission from the optimistic lock before the data can be written to the cache.

4. The local and remote caches return the write result to the HyperMetro I/O processing module.
5. The system determines whether dual-write is successful.
   - If writing to both caches is successful, the log is deleted.
   - If writing to either cache fails, the system:
     i. Converts the log into a DCL that records the differential data between the local and remote LUNs. After conversion, the original log is deleted.
     ii. Suspends the HyperMetro pair. The status of the HyperMetro pair becomes **To be synchronized**. I/Os are only written to the storage system on which writing to its cache succeeded. The storage system on which writing to its cache failed stops providing services for the host.

   NOTE

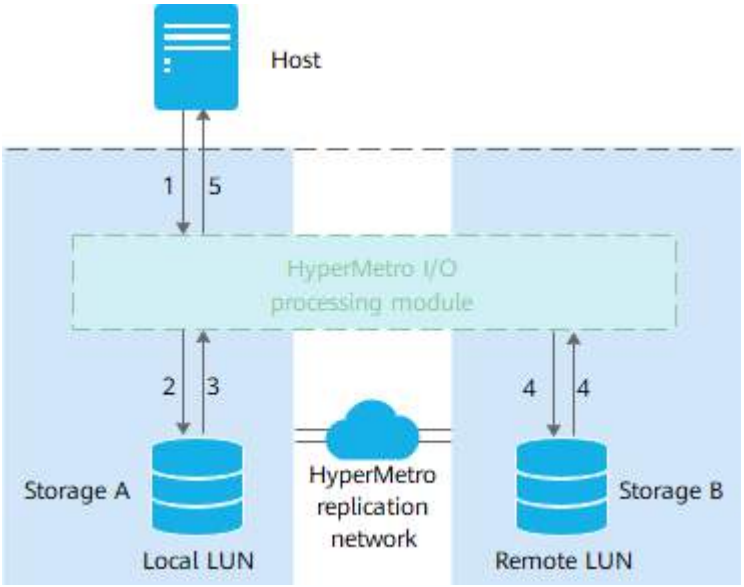
   In the background, the storage systems use the DCL to synchronize data between them. Once the data on the local and remote LUNs is identical, HyperMetro services are restored.
6. The HyperMetro I/O processing module returns the write result to the host.

Read I/O Process

The data of LUNs on both storage systems is synchronized in real time. Both storage systems are accessible to hosts. If one storage system malfunctions, the other one continues providing services for hosts.

Figure 2-6 shows an example of the read I/O process.

Figure 2-6 Read I/O process



1. A host delivers a read I/O to the HyperMetro I/O processing module.
2. The HyperMetro I/O processing module enables the local storage system to respond to the read request of the host.

3. If the local storage system is operating properly, it returns data to the HyperMetro I/O processing module.
4. If the local storage system is not operating properly, the HyperMetro I/O processing module enables the host to read data from the remote storage system. Then the remote storage system returns data to the HyperMetro I/O processing module.
5. The HyperMetro I/O processing module returns the requested data to the host.

2.5 Arbitration Mechanism

If links between two HyperMetro storage systems are disconnected or either storage system breaks down, real-time data synchronization will be unavailable to the storage systems and only one storage system of the HyperMetro relationship can continue providing services. To ensure data consistency, HyperMetro uses the arbitration mechanism to determine which storage system continues providing services.

NOTE

HyperMetro supports arbitration by pair or consistency group.

HyperMetro provides two arbitration modes:

- Static priority mode

  Applies when no quorum server is deployed.
- Quorum server mode (recommended)

  Applies when quorum servers are deployed.

2.5.1 Static Priority Mode

If no quorum server is configured or the quorum server is inaccessible, HyperMetro works in static priority mode. When an arbitration occurs, the preferred site wins the arbitration and provides services.

- If links between the two storage systems are down or the non-preferred site of a HyperMetro pair breaks down, LUNs of the storage system at the preferred site continue providing HyperMetro services and LUNs of the storage system at the non-preferred site stop.
- If the preferred site of a HyperMetro pair breaks down, the non-preferred site does not take over HyperMetro services automatically. As a result, the services stop. You must forcibly start the services at the non-preferred site.

NOTE

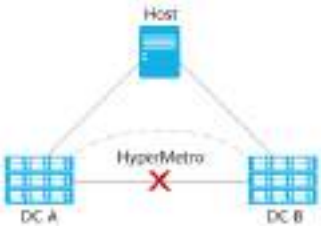
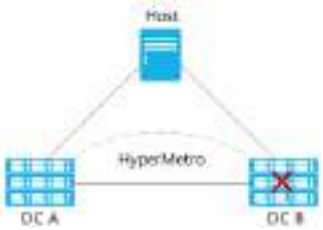
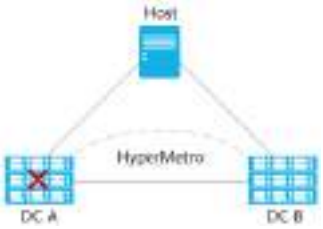
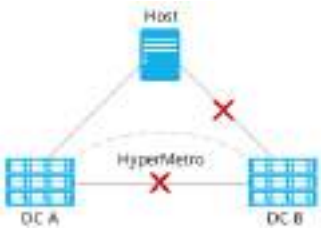
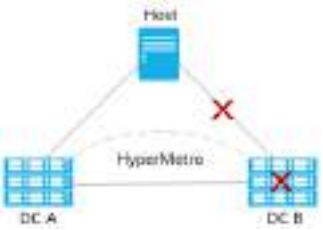
If you power off the storage system at the preferred site for maintenance (by choosing ■ > **Power Off Device** on DeviceManager), the storage system at the non-preferred site takes over all HyperMetro services without interruption.

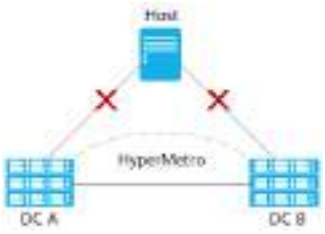
The following example uses DC A as the preferred site and DC B as the non-preferred site. **Table 2-1** describes the arbitration mechanism in static priority mode.

NOTE

In the following table, if two faults occur in the system, the interval between the faults is less than or equal to 60 seconds.

Table 2-1 Arbitration mechanism in static priority mode

Fault Diagram	Fault Description	Arbitration Result
	The link between two storage systems is down.	The HyperMetro pair is in the **To be synchronized** state. The LUN in DC A continues providing services while the LUN in DC B stops.
	The storage system in DC B malfunctions.	The HyperMetro pair is in the **To be synchronized** state. The LUN in DC A continues providing services while the LUN in DC B stops.
	The storage system in DC A malfunctions.	The HyperMetro pair is in the **To be synchronized** state. The LUN in DC A is inaccessible while the LUN in DC B stops. **NOTE** You must forcibly start the HyperMetro pair to enable the LUN in DC B to provide services.
	The HyperMetro replication link and the link between the host and DC B are down.	The HyperMetro pair is in the **To be synchronized** state. The LUN in DC A continues providing services while the LUN in DC B stops.
	The storage system in DC B malfunctions and the link between the host and DC B is down.	The HyperMetro pair is in the **To be synchronized** state. The LUN in DC A continues providing services while the LUN in DC B stops.

Fault Diagram	Fault Description	Arbitration Result
	The links between the host and DCs A and B are down.	The HyperMetro pair is in the **Normal** state. The host cannot access the LUNs in DCs A and B.

2.5.2 Single-Quorum-Server Mode

In this mode, an independent physical server or VM is used as the quorum server. You are advised to deploy the quorum server at a dedicated quorum site that is in a different fault domain from the two DCs.

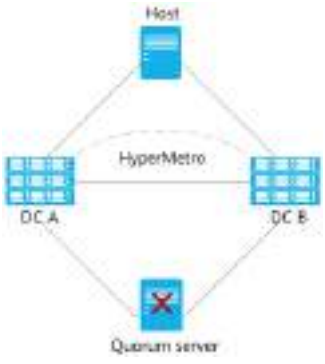
In the event of a DC failure or disconnection between the storage systems, each storage system sends an arbitration request to the quorum server, and only the winner continues providing services. The preferred site takes precedence in arbitration.

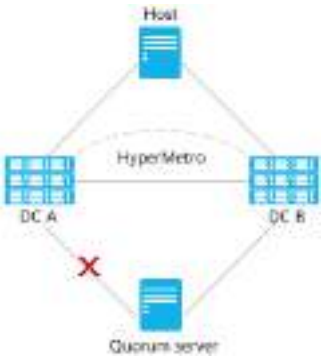
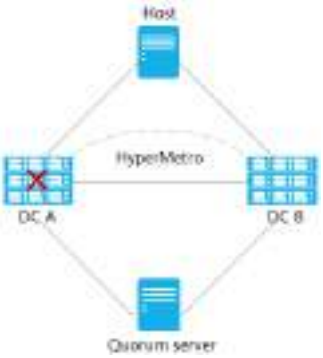
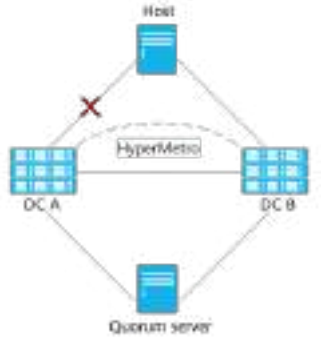
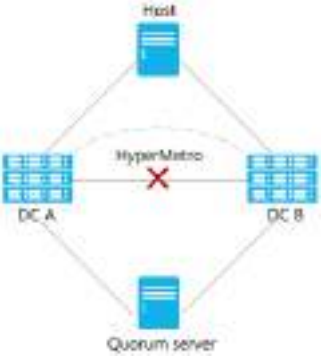
The following example uses DC A as the preferred site and DC B as the non-preferred site. **Table 2-2** describes the arbitration mechanism in quorum server mode.

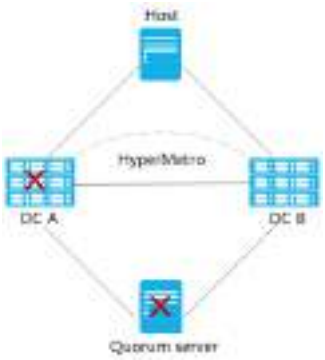
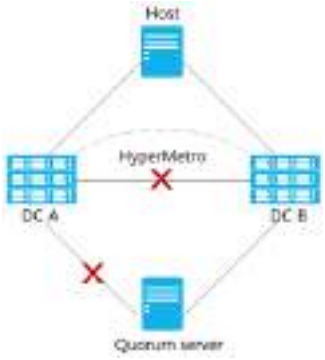
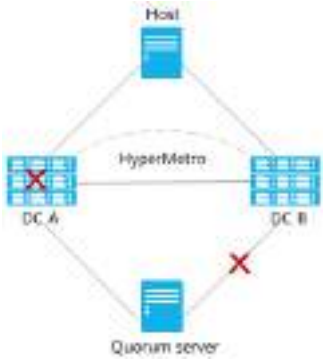
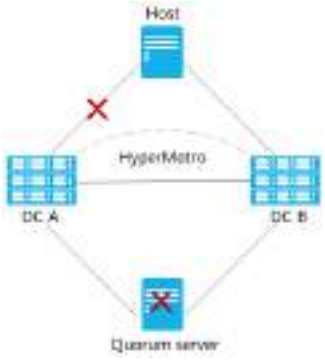
NOTE

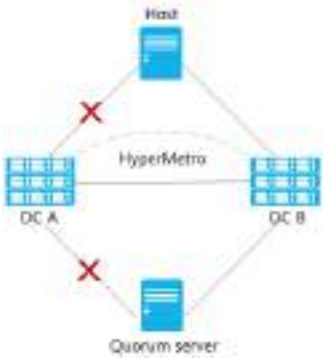
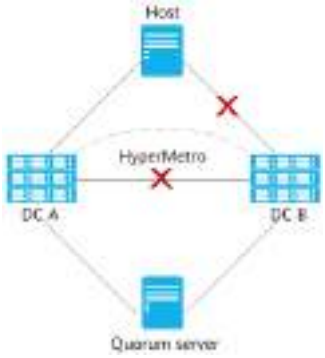
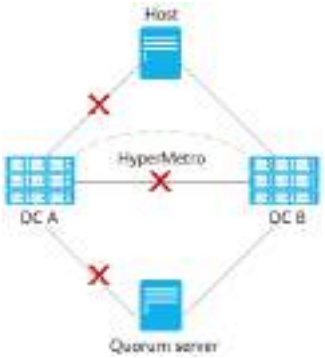
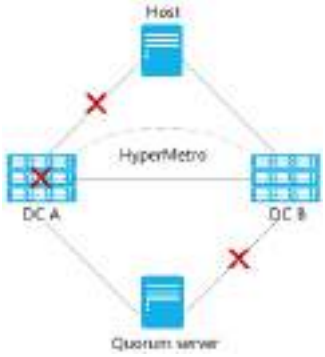
In the following table, if two or more faults occur in the system, the interval between the faults is less than or equal to 60 seconds.

Table 2-2 Arbitration mechanism in quorum server mode

Fault Diagram	Fault Description	Arbitration Result
	The quorum server malfunctions.	The HyperMetro pair is in the **Normal** state. The LUNs in both DCs A and B continue providing services. **NOTE** HyperMetro automatically switches to static priority mode.

Fault Diagram	Fault Description	Arbitration Result
	The link between one storage system (for example, storage system in DC A) and the quorum server is down.	The HyperMetro pair is in the **Normal** state. The LUNs in both DCs A and B continue providing services.
	A storage system (for example, storage system in DC A) malfunctions.	The HyperMetro pair is in the **To be synchronized** state. The LUN in DC A stops while the LUN in DC B continues providing services.
	The link between one storage system (for example, storage system in DC A) and the host is down.	The HyperMetro pair is in the **Normal** state. The LUN in DC B provides services.
	The link between two storage systems is down.	The HyperMetro pair is in the **To be synchronized** state. The LUN in DC A continues providing services while the LUN in DC B stops.

Fault Diagram	Fault Description	Arbitration Result
	A storage system (for example, storage system in DC A) and the quorum server malfunction.	The HyperMetro pair is in the **To be synchronized** state. The LUN in DC A is inaccessible while the LUN in DC B stops. **NOTE** You must forcibly start the HyperMetro pair to enable the LUN in DC B to provide services.
	The link between the two storage systems and the link between a storage system (for example, storage system in DC A) and the quorum server are down.	The HyperMetro pair is in the **To be synchronized** state. The LUN in DC A stops while the LUN in DC B continues providing services.
	A storage system malfunctions (for example, storage system in DC A) and the link between the other storage system and the quorum server is down.	The HyperMetro pair is in the **To be synchronized** state. The LUN in DC A is inaccessible while the LUN in DC B stops. **NOTE** You must forcibly start the HyperMetro pair to enable the LUN in DC B to provide services.
	The quorum server malfunctions and the link between the host and one storage system (for example, storage system in DC A) is down.	The HyperMetro pair is in the **Normal** state. The LUN in DC B provides services. **NOTE** HyperMetro automatically switches to static priority mode.

Fault Diagram	Fault Description	Arbitration Result
	The link between a storage system (for example, storage system in DC A) and the quorum server is down and the link between the storage system and the host is down.	The HyperMetro pair is in the **Normal** state. The LUN in DC B provides services.
	The link between the storage systems is down and the link between the non-preferred site (for example, DC B) and the host is down.	The HyperMetro pair is in the **To be synchronized** state. The LUN in DC A continues providing services while the LUN in DC B stops.
	The link between the storage systems is down. Then the links between a storage system (for example, storage system in DC A) and the quorum server as well as the host are down.	The HyperMetro pair is in the **To be synchronized** state. The HyperMetro services are interrupted. **NOTE** To avoid misoperation or data loss, contact Huawei technical support for service recovery.
	One storage system (for example, storage system in DC A) malfunctions and the links between the storage system and the host as well as between the other storage system and the quorum server are down.	The HyperMetro pair is in the **To be synchronized** state. The LUN in DC A is inaccessible while the LUN in DC B stops. **NOTE** You must forcibly start the HyperMetro pair to enable the LUN in DC B to provide services.

Fault Diagram	Fault Description	Arbitration Result
	The link between the host and the non-preferred storage system, the replication link, and the link between the quorum server and the non-preferred storage system are down.	The LUN in DC A continues providing services while the LUN in DC B stops.

2.5.3 Dual-Quorum-Server Mode

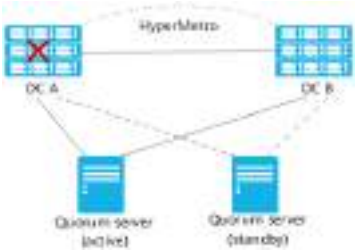
In the active-active SAN solution, two quorum servers in active/standby mode can be deployed at the quorum site for device-level failover.

When the quorum site has two quorum servers, the two quorum servers work in active/standby mode. If all links between the active quorum server and both storage systems are down while both storage systems are properly connected to the standby quorum server and to each other, the standby quorum server will automatically take over arbitration services 1 minute after the fault occurs.

The following example uses DC A as the preferred site and DC B as the non-preferred site. **Table 2-3** describes the arbitration mechanism in dual-quorum-server mode.

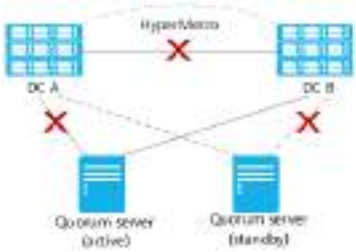
Table 2-3 Arbitration mechanism in dual-quorum-server mode

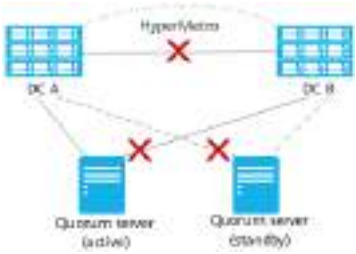
Fault Diagram	Fault Description	Arbitration Result
	The active quorum server malfunctions.	The HyperMetro pair is in the **Normal** state. The standby quorum server takes over the arbitration services from the active quorum server. The LUNs in both DCs A and B continue providing services. After the quorum server recovers, it works as the standby.

Fault Diagram	Fault Description	Arbitration Result
	The link between one storage system (for example, storage system in DC A) and the active quorum server is down.	The HyperMetro pair is in the **Normal** state. The active quorum server runs properly. The LUNs in both DCs A and B continue providing services.
	The links between the active quorum server and both storage systems are down.	The HyperMetro pair is in the **Normal** state. The standby quorum server takes over the arbitration services from the active quorum server. The LUNs in both DCs A and B continue providing services.
	A storage system (for example, storage system in DC A) malfunctions.	The HyperMetro pair is in the **To be synchronized** state. The active quorum server runs properly. The LUN in DC A is inaccessible while the LUN in DC B continues providing services.
	The link between two storage systems is down.	The HyperMetro pair is in the **To be synchronized** state. The active quorum server runs properly. Result 1: The LUN in DC A continues providing services while the LUN in DC B stops. Result 2: The LUN in DC B continues providing services while the LUN in DC A stops. **NOTE** Serving as the preferred site, DC A takes precedence in arbitration. Generally, the arbitration result is Result 1.

Fault Diagram	Fault Description	Arbitration Result
	The active quorum server malfunctions and then the storage system at the preferred site (for example, DC A) malfunctions. The interval between the two faults is less than 60 seconds.	The HyperMetro pair is in the **To be synchronized** state. No quorum server is working. The LUN in DC A is inaccessible while the LUN in DC B stops.
	The link between the two storage systems and the link between a storage system (for example, storage system in DC A) and the active quorum server are down. **NOTE** The interval between the two faults is less than or equal to 60 seconds.	The HyperMetro pair is in the **To be synchronized** state. The active quorum server runs properly. The LUN in DC B continues providing services while the LUN in DC A stops.

Fault Diagram	Fault Description	Arbitration Result
	One storage system (for example, storage system in DC A) malfunctions and the link between the other storage system and the active quorum server is down.	The HyperMetro pair is in the **To be synchronized** state. • If the storage system malfunctions before the quorum link is down: – If the interval between the two faults is less than or equal to 60 seconds, the active quorum server continues working. The LUN in DC A is inaccessible while the LUN in DC B may stop. – If the interval between the two faults is greater than 60 seconds, the active quorum server continues working. The LUN in DC A is inaccessible while the LUN in DC B continues providing services. • If the storage system malfunctions after the quorum link is down: The active quorum server continues working. The LUN in DC A is inaccessible while the LUN in DC B stops.

Fault Diagram	Fault Description	Arbitration Result
	The active quorum server malfunctions and then the link between two storage systems is down.	The HyperMetro pair is in the **To be synchronized** state. Result 1: If the interval between the two faults is greater than 60 seconds, the standby quorum server takes over the arbitration services from the active quorum server. DC A wins the arbitration. The LUN in DC A continues providing services while the LUN in DC B stops. Result 2: If the interval between the two faults is less than or equal to 60 seconds, the standby quorum server cannot take over the arbitration services. The LUNs in both DCs A and B stop.
	The following faults occur concurrently: • The link between the active quorum server and the preferred site is down. • The link between the standby quorum server and the non-preferred site is down. • The link between two storage systems is down. **NOTE** The interval between the faults is less than or equal to 60 seconds.	The HyperMetro pair is in the **To be synchronized** state. The active quorum server runs properly. The LUN in DC B continues providing services while the LUN in DC A stops.

Fault Diagram	Fault Description	Arbitration Result
	The following faults occur concurrently: • The link between the active quorum server and the non-preferred site is down. • The link between the standby quorum server and the preferred site is down. • The link between two storage systems is down. **NOTE** The interval between the faults is less than or equal to 60 seconds.	The HyperMetro pair is in the **To be synchronized** state. The active quorum server runs properly. The LUN in DC A continues providing services while the LUN in DC B stops.

3 Planning

Planning the network, storage layer, and host applications before deploying active-active SAN DCs helps ensure a smooth implementation.

You can plan the active-active solution according to the networking topologies provided in **3.2.1 Standard Networking**, or use the LLDesigner to plan and design the project based on actual requirements.

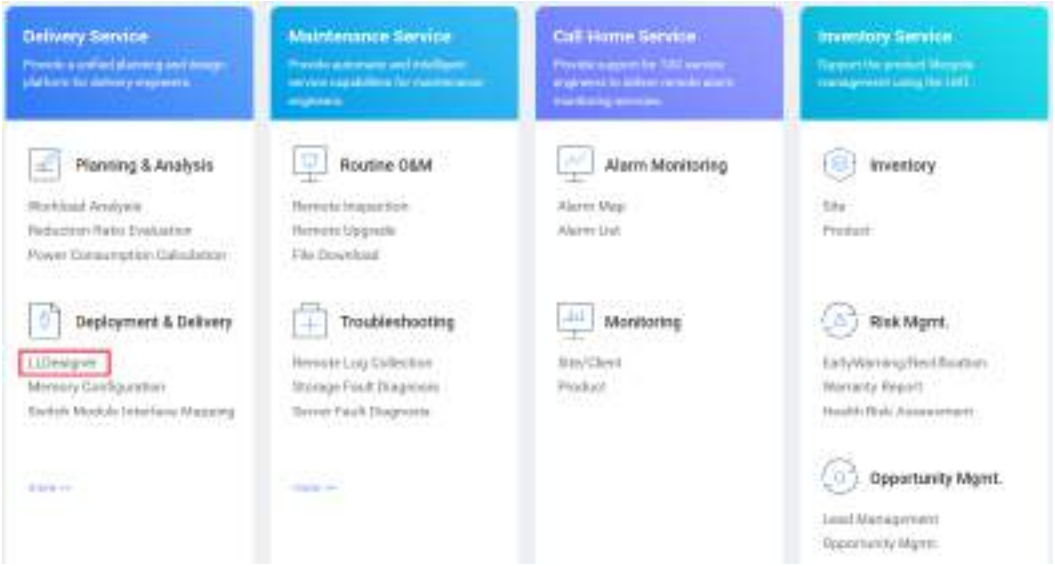
3.1 Using the LLDesigner to Plan and Design the Solution

You can use the LLDesigner to plan the hardware configuration, device networking, and resource allocation.

Step 1 Log in to **eService** with your Uniportal account and password.

Step 2 In the **Delivery Service** area, click **LLDesigner**, as shown in **Figure 3-1**.

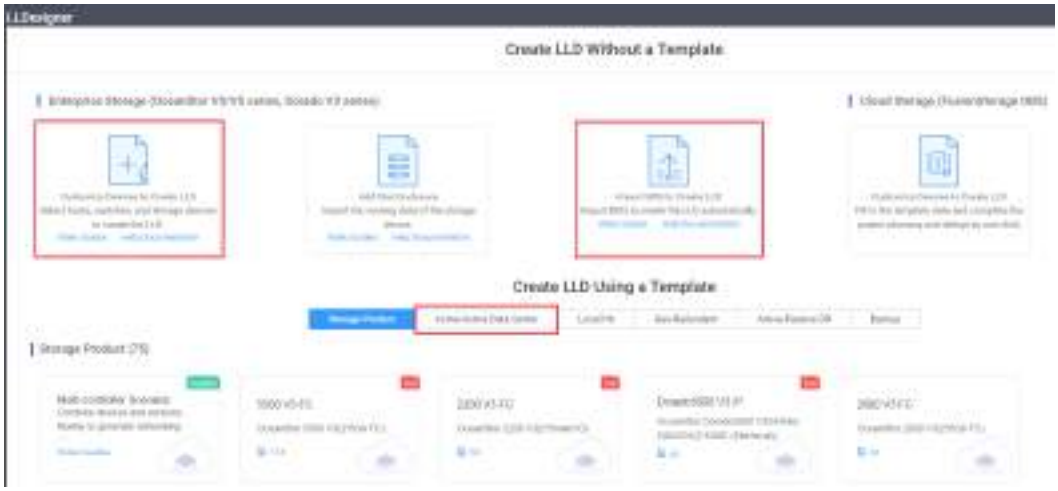
Figure 3-1 eService home page



Step 3 Click **Create LLD**. You can create an LLD by using one of the following methods:

- In **Create LLD Without a Template**, click **Customize Devices to Create LLD**.
- In **Create LLD Without a Template**, click **Import BOQ to Create LLD**.
- In **Create LLD Using a Template**, click **Active-Active Data Center** and customize a template or choose an existing template.

Figure 3-2 Creating LLD



----End

3.2 Network Planning for Single-Quorum-Server Mode

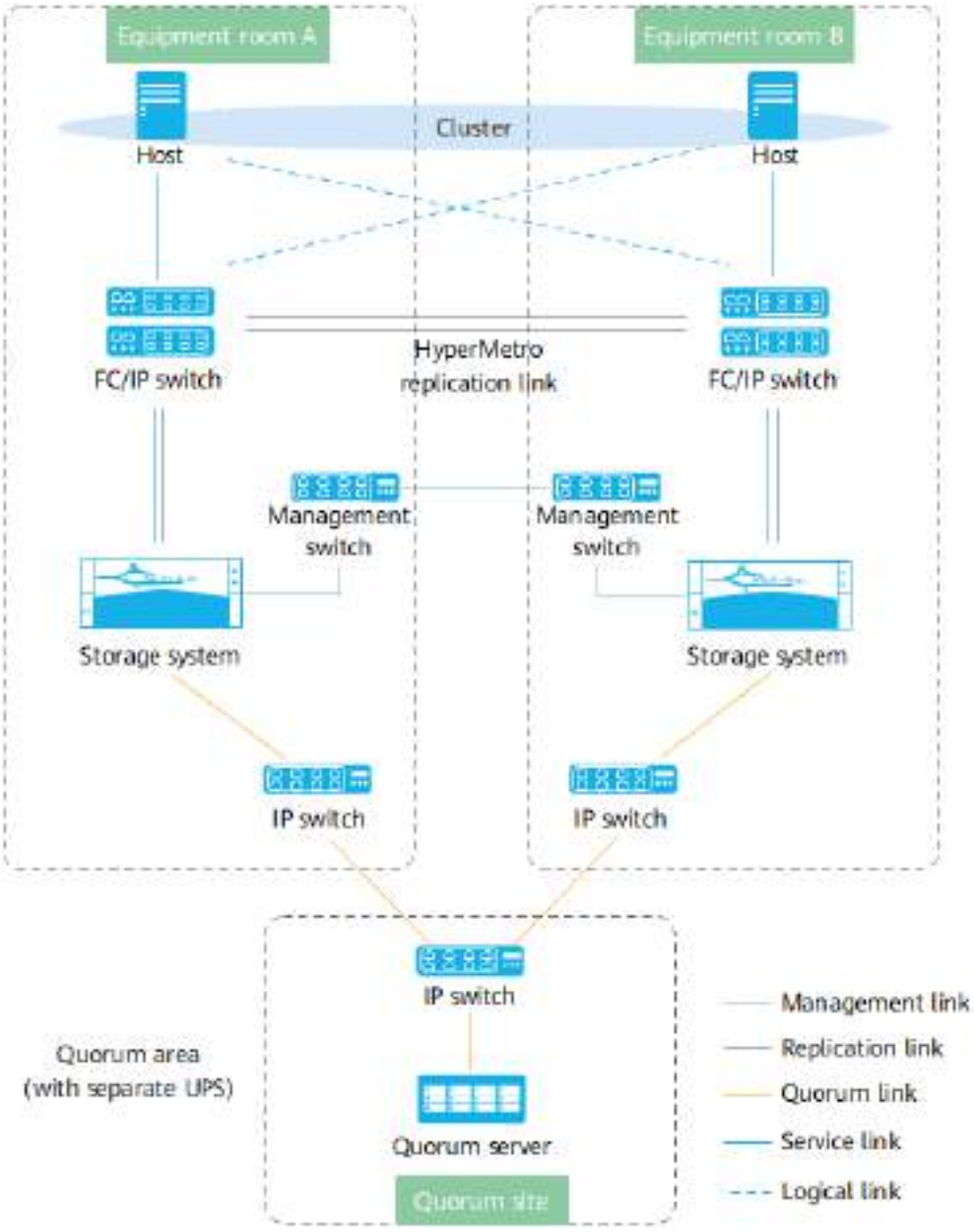
3.2.1 Standard Networking

This section describes the standard networking topologies for the active-active DC solution, including both single-DC and cross-DC deployment modes.

Single-DC Deployment

Figure 3-3 illustrates the standard networking for single-DC deployment.

Figure 3-3 Standard networking for single-DC deployment



- Scenario

  The storage systems are deployed in two equipment rooms in the same campus.

- Networking principle
  - The two equipment rooms are in different fault domains. Uninterruptible power supplies (UPSs) must be configured separately for the quorum server and network devices.
  - Hosts are deployed in a cluster.

  - Hosts are physically and logically connected to both storage systems.
  - Each equipment room uses two switches for HyperMetro replication. The switches are connected in pairs.

    NOTE

    If the storage systems are in the same equipment room, UPSs must be configured for the storage systems, quorum server, and quorum network devices separately.

- Network planning

  HyperMetro ensures the reliability of storage systems by using redundant links among all of its networks. For details, see **Table 3-1**.

  Table 3-1 Network planning

Network	Description	
Host-to-storage network All hosts can be interconnected to form a cluster.	Network type	The network can be an 8 Gbit/s Fibre Channel, 16 Gbit/s Fibre Channel, 32 Gbit/s Fibre Channel, GE, 10GE, 25GE, 40GE, or 100GE network.
	Networking mode	• Use full-mesh networking between hosts and storage systems. For OceanStor 5310, 5510, and 5610, each host is physically and logically connected to every controller on both storage systems. For OceanStor 6810, 18510, and 18810, each host is physically and logically connected to each quadrant on both storage systems. • A host must connect to both storage systems using the same type of network. • Dual-switch networking must be used. • The HyperMetro replication network, host-to-storage network, and quorum network must be physically isolated and use different ports. • The host-to-storage network can be an NVMe over RoCE network. When the NVMe over RoCE network is used, install Huawei UltraPath on the hosts. OS native or third-party multipathing software is not supported.

Network	Description	
HyperMetro replication network A network between the storage systems to synchronize heartbeat information and data. **NOTE** Storage systems set link priorities for transferring different types of data. Heartbeat information has a higher priority than data synchronization.	Network type	• The network type can be 8 Gbit/s Fibre Channel, 16 Gbit/s Fibre Channel, 32 Gbit/s Fibre Channel, 10GE, 25GE, 40GE, 100GE, 25 Gbit/s RoCE, or 100 Gbit/s RoCE. **NOTE** If you use an IP network, you can use an L2 or L3 network. For better synchronization performance, you are advised to use an L2 network. • Bandwidth: ≥ peak service bandwidth (total read and write bandwidth on both storage systems). At least 2 Gbit/s is required.

Network	Description	
	Networking mode	• On OceanStor 5310, 5510, and 5610, each controller on every storage system must have at least two redundant physical links. On OceanStor 6810, 18510 and 18810, each quadrant must have at least two redundant physical links. • A full-mesh network is recommended for the connections between two storage systems. For OceanStor 5310, 5510, and 5610, physical or logical links are established between every controller on each local controller enclosure and every controller on each remote controller enclosure. For example, controller A on the local controller enclosure 0 must have links to every controller on each remote controller enclosure. For OceanStor 6810, 18510 and 18810, physical or logical links are established between every quadrant on each local controller enclosure and the same quadrant on each remote controller enclosure. For example, quadrant A on the local controller enclosure 0 must have links to quadrant A on every remote controller enclosure. • The HyperMetro replication network, host-to-storage network, and quorum network must be physically isolated and use different ports. The ports used to establish replication links between both storage systems cannot be bond ports. • If a local device establishes replication or HyperMetro relationships with multiple remote devices, it is not recommended that you use the same port on the local device to connect to the remote devices. If the same port is used, remote devices will contend for resources and the replication or HyperMetro services may be interrupted. • The HyperMetro replication network and quorum network must not share switches.

Network	Description	
		• The storage systems do not support network address translation (NAT). If a NAT device is deployed on the network, you must configure bidirectional NAT on the NAT device to translate both the source and destination addresses of the HyperMetro replication network. • FastWrite – It is recommended that you enable FastWrite on both storage systems when the Fibre Channel network between the two sites spans over 10 km. To enable FastWrite, run the **change port fc fc_port_id**=*XXX* **fast_write_enable=yes** command. Then run the **show port general port_id=***XXX* command. If **Fast Write Enable** in the command output is **Yes**, FastWrite has been enabled successfully. (On DeviceManager, choose **Services** > **Network** > **FC Network** and click a port. In the dialog box displayed on the right, click **Modify** and then enable **Immediate Data**.) – On an IP or RoCE replication network, FastWrite has been enabled by default. – FastWrite on the storage system and FastWrite on the switch cannot be used together. (The function name for Brocade switches is Fast Write, while for Cisco switches is Write Acceleration.) • The TCP offload engine (TOE) is supported to reduce the use of storage system resources when the TCP/IP protocol processes network traffic. – TOE is enabled by default. – Run the **show port eth_toe_switch eth_port_id=***XXX* command at the end where the remote device is added to query

Network	Description	
		the TOE status. If the status in the command output is **Yes**, TOE is enabled. If the status in the command output is **No**, TOE is disabled. – To enable TOE, first run the **chang port eth_toe_switch eth_port_id=*XXX* toe_enable=yes** command in developer mode at the local and remote ends to enable TOE for ports. (If the command output contains **This function is not supported by the product**, the Ethernet port does not support TOE.) Then run the **change remote_device general remote_device_id=*XXX* toe_switch=on** command at the local end to enable TOE for replication links.
Quorum network If communication between the storage systems is interrupted or a storage system malfunctions, the quorum server determines which storage system is accessible. **NOTE** The quorum server resides on a dedicated network that is linked to both storage systems.	Network type	• Quorum links must be established on GE and 10GE networks, but not a Fibre Channel network. • Quorum links support IPv4 and IPv6 addresses. • Network quality and bandwidth requirements – Latency: RTT ≤ 50 ms – Bandwidth: ≥ 10 Mbit/s

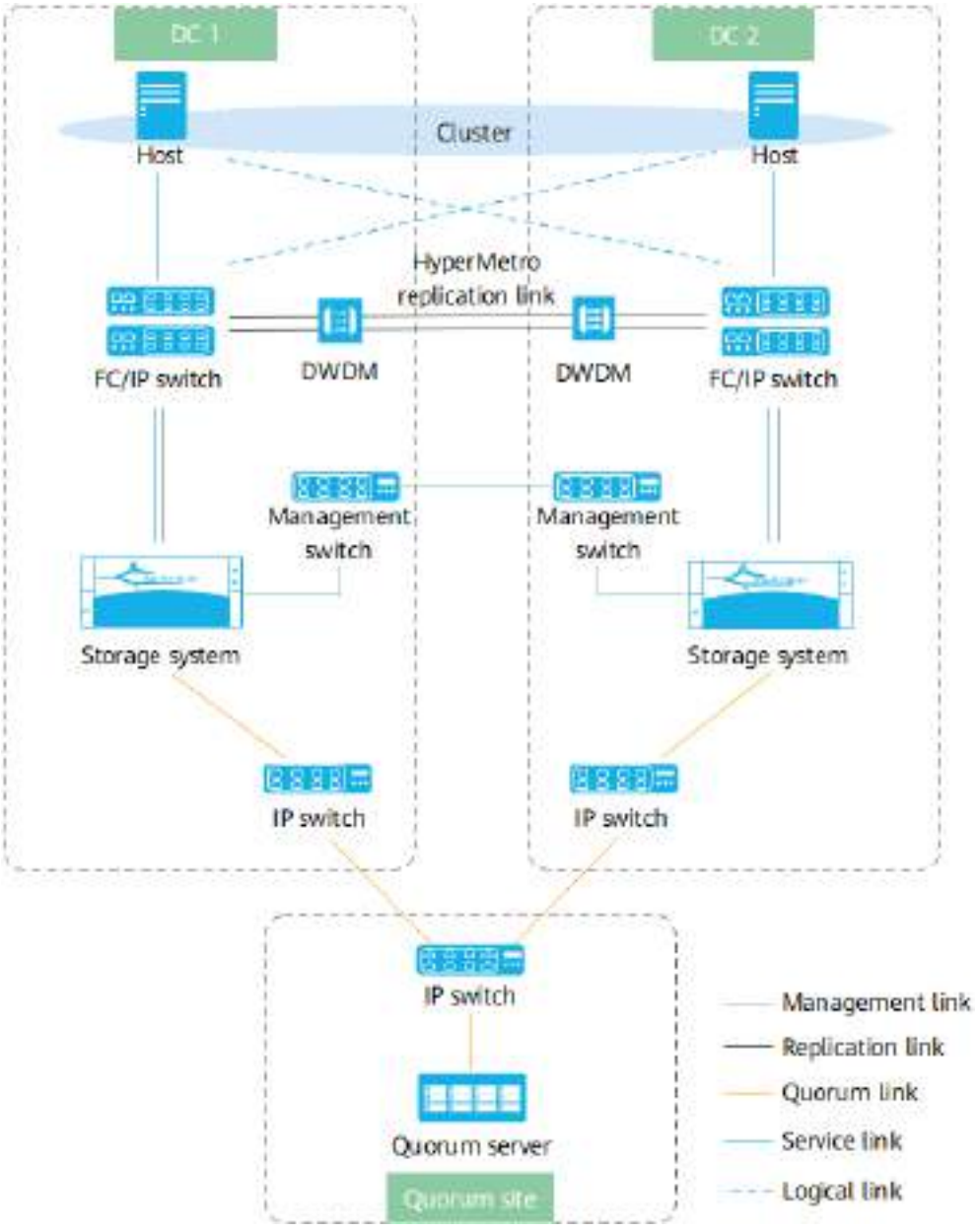
Network	Description	
	Networking mode	• Independent front-end or management ports can be used as quorum ports, but maintenance ports cannot. **NOTE** • You are advised to use independent front-end ports as quorum ports. • If you use independent GE ports as quorum ports, you must install dedicated GE interface modules if your product model is one of the following: OceanStor 5510, 5610, 6810, 18510, and 18810. • An independent quorum server must be deployed. • For OceanStor 5310, 5510, and 5610, each controller of the storage systems must have quorum links. For OceanStor 6810, 18510, and 18810, each quadrant must have quorum links. • It is recommended that you configure the quorum ports on the storage systems on different network segments to prevent arbitration failures caused by network segment faults. • The quorum server and storage systems can be connected by L2 or L3 networks, but do not support Virtual Router Redundancy Protocol (VRRP). • The networks between both storage systems and the quorum server, and the active and standby ports on the quorum server must be on different network segments. • The HyperMetro replication network, host-to-storage network, and quorum network must be physically isolated and use different ports. In addition, the HyperMetro replication network and quorum network must not share switches. • The storage systems do not support network address translation (NAT). If a NAT device is deployed on the network, you must configure bidirectional NAT on the NAT device

Network	Description	
		to translate both the source and destination addresses of the HyperMetro replication network.

Cross-DC Deployment

Figure 3-4 illustrates the standard networking for cross-DC deployment.

Figure 3-4 Standard networking for cross-DC deployment



- Scenario

The storage systems are deployed in two different DCs up to 300 km apart.

- Networking principle
  - The two DCs and the quorum site must be in different fault domains.

    NOTE

    A fault domain is a set of devices that share a possible point of failure, such as the power system, cooling system, network, and impact from natural disasters.
  - Hosts are deployed in a cluster.
  - Hosts are physically and logically connected to both storage systems.
  - Each DC uses two switches for HyperMetro replication. The switches are connected in pairs.
- Network planning

  HyperMetro ensures the reliability of storage systems by using redundant links among all of its networks. For details, see **Table 3-2**.

Table 3-2 Network planning

Network	Description	
Host-to-storage network All hosts can be interconnected across DCs to form a cluster.	Network type	The network can be an 8 Gbit/s Fibre Channel, 16 Gbit/s Fibre Channel, 32 Gbit/s Fibre Channel, GE, 10GE, 25GE, 40GE, or 100GE network.
	Networking mode	• Use full-mesh networking between hosts and storage systems. For OceanStor 5310, 5510, and 5610, each host is physically and logically connected to every controller on both storage systems. For OceanStor 6810, 18510, and 18810, each host is physically and logically connected to each quadrant on both storage systems. • A host must connect to both storage systems using the same type of network. • Dual-switch networking must be used. • The HyperMetro replication network, host-to-storage network, and quorum network must be physically isolated and use different ports.

Network	Description	
HyperMetro replication network A network between the storage systems to synchronize heartbeat information and data. **NOTE** Storage systems set link priorities for transferring different types of data. Heartbeat information has a higher priority than data synchronization.	Network type	• The network type can be 8 Gbit/s Fibre Channel, 16 Gbit/s Fibre Channel, 32 Gbit/s Fibre Channel, 10GE, 25GE, 40GE, 100GE, 25 Gbit/s RoCE, or 100 Gbit/s RoCE. • Network quality and bandwidth requirements – Bandwidth: ≥ peak service bandwidth (total read and write bandwidth on both storage systems). At least 2 Gbit/s is required. – Latency: RTT < 10 ms (distance < 300 km) **NOTE** In practice, the latency is determined by the requirements of the application layer. The active-active DC solution must meet the minimum latency requirement. For the Oracle RAC, SQL Server, and DB2 applications, the RTT must be less than 1 ms (with a distance of less than 100 km). For the VMware vSphere applications, the RTT must be less than 10 ms. – No jitter or packet loss – BER: ≤ 10^{-12} • FastWrite – It is recommended that you enable FastWrite on both storage systems when the Fibre Channel network between the two sites spans over 10 km. To enable FastWrite, run the **change port fc fc_port_id**=*XXX* **fast_write_enable=yes** command. Then run the **show port general port_id=***XXX* command. If **Fast Write Enable** in the command output is **Yes**, FastWrite has been enabled successfully. (On DeviceManager, choose **Services** > **Network** > **FC Network** and click a port. In the dialog box displayed on the right, click **Modify** and then enable **Immediate Data**.)

Network	Description	
		– On an IP or RoCE replication network, FastWrite has been enabled by default. – FastWrite on the storage system and FastWrite on the switch cannot be used together. (The function name for Brocade switches is Fast Write, while for Cisco switches is Write Acceleration.) ● The TCP offload engine (TOE) is supported to reduce the use of storage system resources when the TCP/IP protocol processes network traffic. – TOE is enabled by default. – Run the **show port eth_toe_switch eth_port_id=***XXX* command at the end where the remote device is added to query the TOE status. If the status in the command output is **Yes**, TOE is enabled. If the status in the command output is **No**, TOE is disabled. – To enable TOE, first run the **chang port eth_toe_switch eth_port_id=***XXX* **toe_enable=yes** command in developer mode at the local and remote ends to enable TOE for ports. (If the command output contains **This function is not supported by the product**, the Ethernet port does not support TOE.) Then run the **change remote_device general remote_device_id=***XXX* **toe_switch=on** command at the local end to enable TOE for replication links.

Network	Description	
	Networking mode	• On OceanStor 5310, 5510, and 5610, each controller on every storage system must have at least two redundant physical links. On OceanStor 6810, 18510 and 18810, each quadrant must have at least two redundant physical links. • A full-mesh network is recommended for the connections between two storage systems. For OceanStor 5310, 5510, and 5610, physical or logical links are established between every controller on each local controller enclosure and every controller on each remote controller enclosure. For example, controller A on the local controller enclosure 0 must have links to every controller on each remote controller enclosure. For OceanStor 6810, 18510 and 18810, physical or logical links are established between every quadrant on each local controller enclosure and the same quadrant on each remote controller enclosure. For example, quadrant A on the local controller enclosure 0 must have links to quadrant A on every remote controller enclosure. • The HyperMetro replication network, host-to-storage network, and quorum network must be physically isolated and use different ports. The ports used to establish replication links between both storage systems cannot be bond ports. • If a local device establishes replication or HyperMetro relationships with multiple remote devices, it is not recommended that you use the same port on the local device to connect to the remote devices. If the same port is used, remote devices will contend for resources and the replication or HyperMetro services may be interrupted. • The HyperMetro replication network and quorum network must not share switches.

Network	Description	
		• The storage systems do not support network address translation (NAT). If a NAT device is deployed on the network, you must configure bidirectional NAT on the NAT device to translate both the source and destination addresses of the HyperMetro replication network.
Network between DCs Both data centers A and B can provide services for hosts and carry the same services. The two data centers back up each other. If one data center is faulty, its services are automatically switched to the other data center without data loss or service interruption.	Network type	The network must use switches and bare fibers.
	Networking mode	For Fibre Channel and RoCE networks: • The two DCs can be connected using switches and bare fibers if their distance is within 25 km. Ensure that the storage and application layers each have at least two pairs (four wires) of bare fibers for heartbeat interconnection in the cluster. • If the two DCs are greater than or equal to 25 km apart, use DWDM devices to interconnect them. **NOTE** The direct transmission distance of the Fibre Channel switches depends on the optical modules. You can query the value from the label on your optical module or in the documentation specific to your optical module. For RoCE, the direct transmission distance depends on the switch specifications. • For IP networks: – The two DCs can be connected using switches and bare fibers if their distance is within 80 km. If core switches are used, ensure that at least two pairs (four wires) of fibers are connected to the core switches for HyperMetro replication between the storage systems and heartbeat interconnection at the application layer. – If the two DCs are greater than or equal to 80 km apart, use DWDM devices to interconnect them.

Network	Description	
Quorum network If communication between the storage systems is interrupted or a storage system malfunctions, the quorum server determines which storage system is accessible. **NOTE** The quorum server resides on a dedicated network that is linked to both storage systems.	Network type	• Quorum links must be established on GE and 10GE networks, but not a Fibre Channel network. • The requirements for the quorum ports on the storage systems are the same as those for the deployment in a single DC. • Quorum links support IPv4 and IPv6 addresses. • Network quality and bandwidth requirements – Latency: RTT ≤ 50 ms – Bandwidth: ≥ 10 Mbit/s

Network	Description	
	Networking mode	• An independent quorum server must be deployed. • You are advised to deploy the quorum server at a dedicated quorum site. **NOTE** • If there is no dedicated quorum site, you are advised to deploy the quorum server at the preferred site and configure UPS protection for the quorum server and quorum network devices. • If the quorum server is deployed at the preferred site, the preferred site wins the arbitration and continues providing services in the event of a failure on the network between the DCs. If the quorum server is deployed at the non-preferred site, services will be provided by the non-preferred site if the network between the DCs fails, and the expectations of setting the preferred site cannot be met. • For OceanStor 5310, 5510, and 5610, each controller of the storage systems must have quorum links. For OceanStor 6810, 18510, and 18810, each quadrant must have quorum links. **NOTE** The requirements for the management ports that can connect to the quorum server are the same as those for the single-DC deployment. • You are advised to connect the quorum ports on each storage system to different switches and configure different network segments to prevent arbitration failures caused by network segment faults. • The quorum server can be a physical or a virtual server. If a virtual server is used, you are advised to deploy VMware vSphere/FusionSphere FT or HA to achieve high availability. • The quorum server can be deployed on Huawei Enterprise Cloud (HEC). When the HEC is used, apply for a VM with the same specifications that you require on the quorum server (including the CPU, memory, disk,

Network	Description	
		and OS). In addition, apply for 2 Mbit/s exclusive bandwidth and one elastic IP address for each storage system. • The quorum server and storage systems can be connected by Layer 2 or Layer 3 networks, but the quorum network between the two DCs does not support Virtual Router Redundancy Protocol (VRRP). • The networks between both storage systems and the quorum server, and the active and standby ports on the quorum server must be on different network segments. • The HyperMetro replication network, host-to-storage network, and quorum network must be physically isolated and use different ports. In addition, the HyperMetro replication network and quorum network must not share switches. • The storage systems do not support network address translation (NAT). If a NAT device is deployed on the network, you must configure bidirectional NAT on the NAT device to translate both the source and destination addresses of the HyperMetro replication network.

3.2.2 Non-Recommended Networking

This section describes some non-recommended networking topologies for the active-active DC solution.

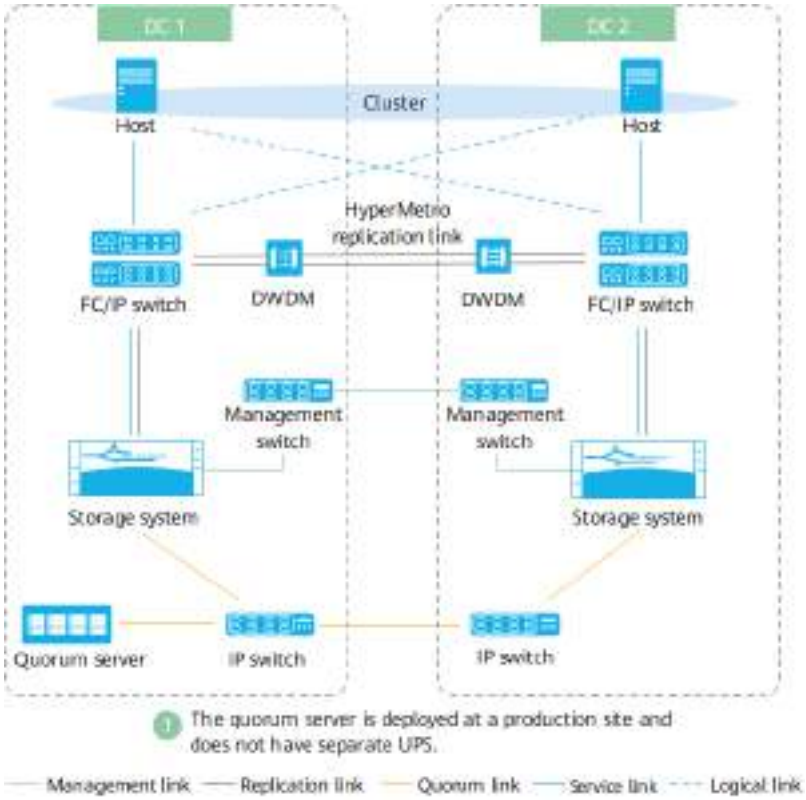
NOTE

If your network does not use the standard or any of the following network topologies, contact Huawei technical support to help you assess risks.

Quorum Server Deployed in Either Active-Active DC

In the following example, the quorum server is deployed in DC 1.

Figure 3-5 Deployment example (quorum server deployed in DC 1)



- Scenario

  The quorum server is deployed in DC 1 or DC 2. No UPS is configured for the quorum server and quorum network devices.

- Risk

  Services will be interrupted if the DC where the quorum server is deployed goes down due to a power failure or disaster.

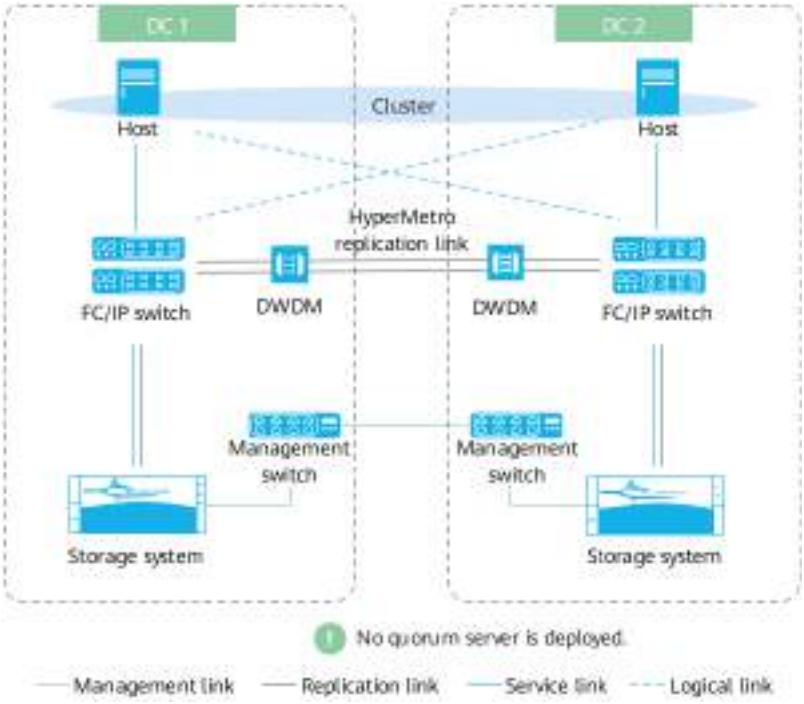
No Quorum Server

The following uses cross-DC deployment as an example. DC 1 is the preferred site and DC 2 is the non-preferred site. **Figure 3-6** shows a network on which no quorum server is deployed.

NOTE

This example is also applicable to single-DC deployment.

Figure 3-6 Deployment example (no quorum server)



- Scenario

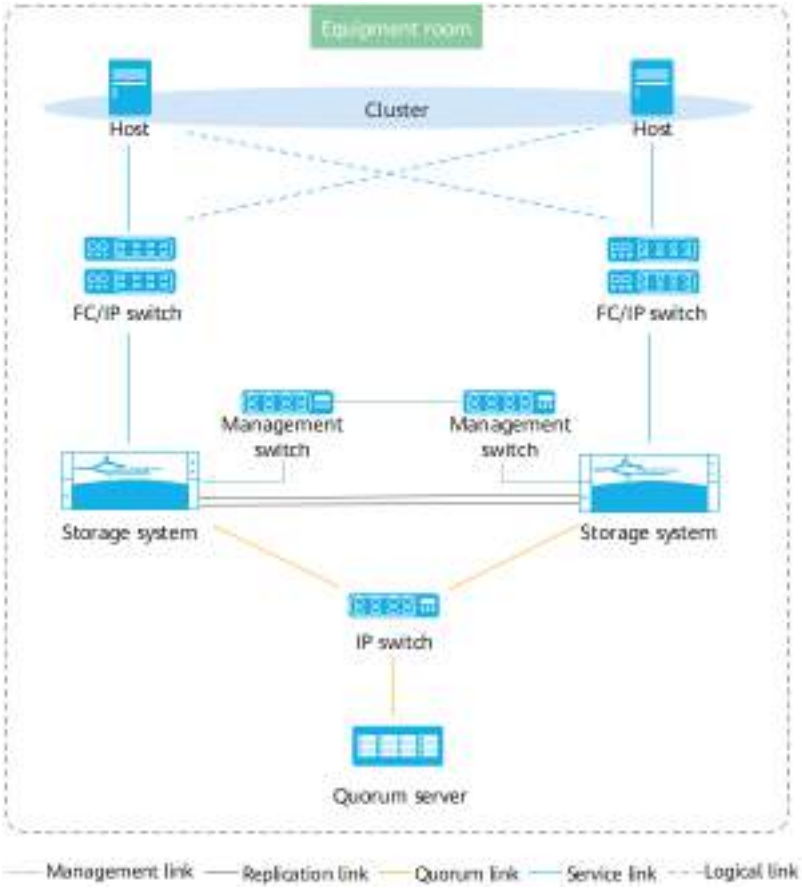
  No quorum server is deployed and the storage systems use static priorities.
- Risk

  Services will be interrupted if the preferred site fails.

Both Storage Systems Deployed in the Same Equipment Room

Figure 3-7 shows a network on which both storage systems are deployed in the same equipment room.

Figure 3-7 Deployment example (both storage systems in the same equipment room)



- Scenario

  Both storage systems are deployed in the same equipment room.

- Risk

  Services will be interrupted if the equipment room goes down due to a power failure or disaster.

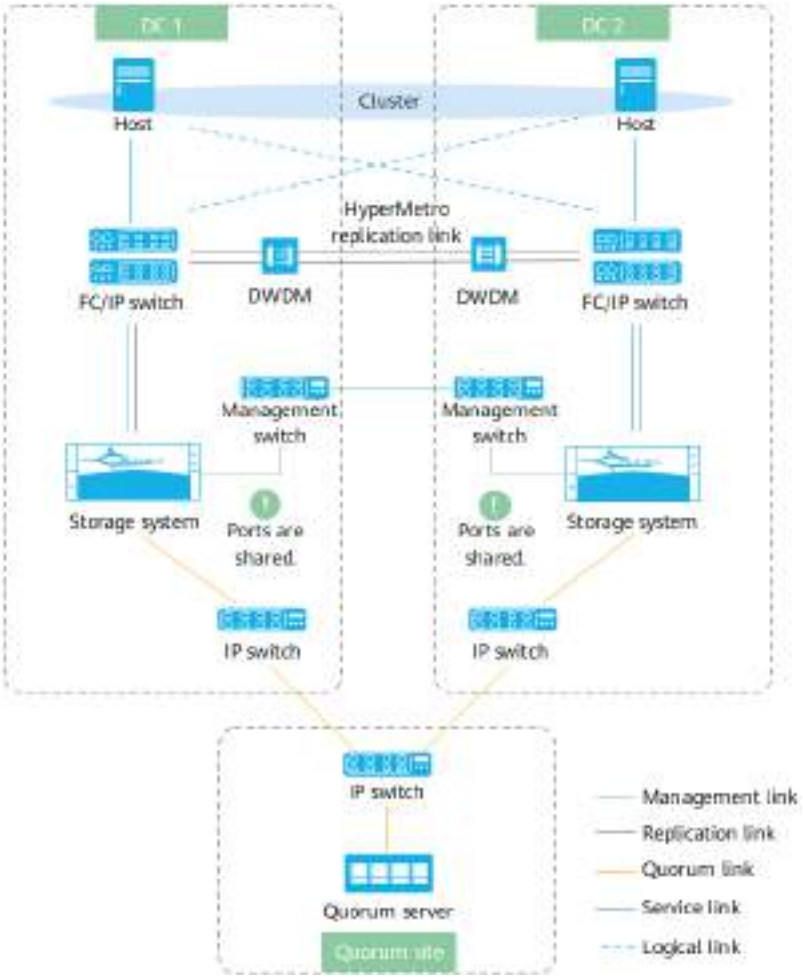
Port Sharing

The following uses cross-DC deployment as an example. **Figure 3-8** illustrates the networking mode.

NOTE

This example is also applicable to single-DC deployment.

Figure 3-8 Port sharing



- Scenario

  The host-to-storage service network, HyperMetro replication network between the DCs, and quorum network share ports on the storage systems.

- Risk
  - The service and replication networks must be physically isolated and must not share ports.
  - If the service and quorum networks share a port, the quorum link will be down if this port fails.
  - If the replication and quorum networks share a port, both the replication and quorum links will be down if this port fails. Services may be interrupted.

3.2.3 Unsupported Networking

This section describes the networking topologies that are not supported by the active-active DC solution. Do not use the networking topologies in this section when deploying the active-active DC solution.

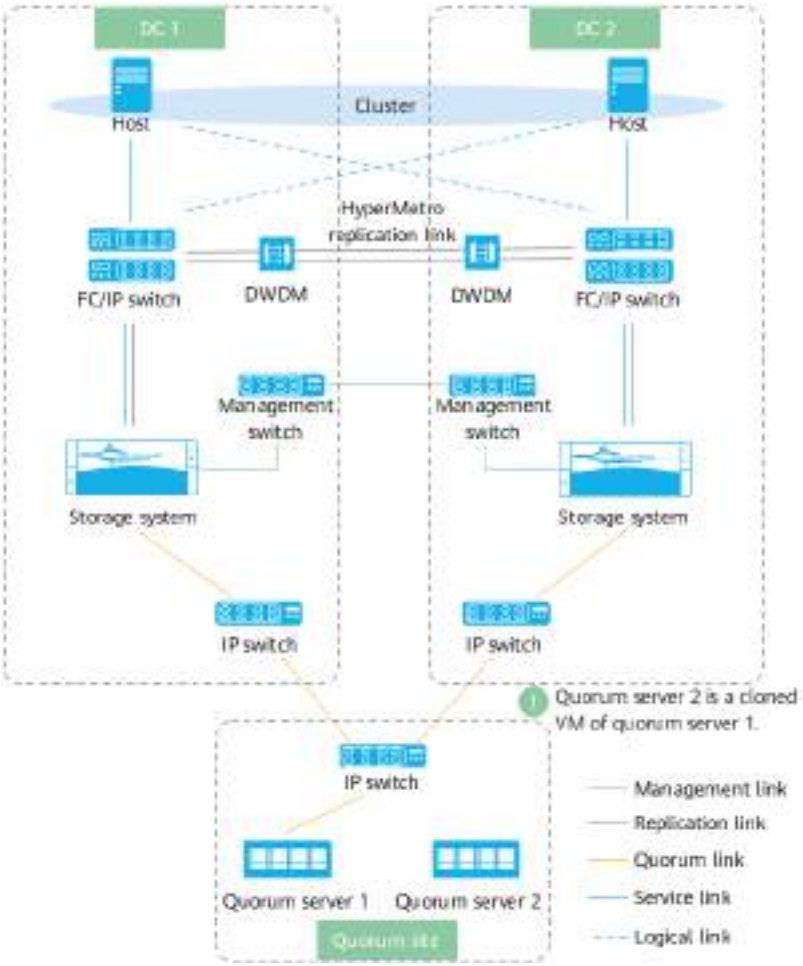
Cloned VM Used as the Other Quorum Server

In this networking mode, a VM is used as the quorum server and the VM is cloned as the other quorum server. **Figure 3-9** shows the networking mode.

NOTICE

When a VM is used as the quorum server, the VM's system and data disks must not be created on the HyperMetro LUNs.

Figure 3-9 Cloned VM as the other quorum server



- Scenario

  The quorum server is a cloned VM of the other existing quorum server VM.

- Risk

  The cloned VM has the same information as the source VM, which will cause a quorum server conflict.

3.3 Network Planning for Dual-Quorum-Server Mode

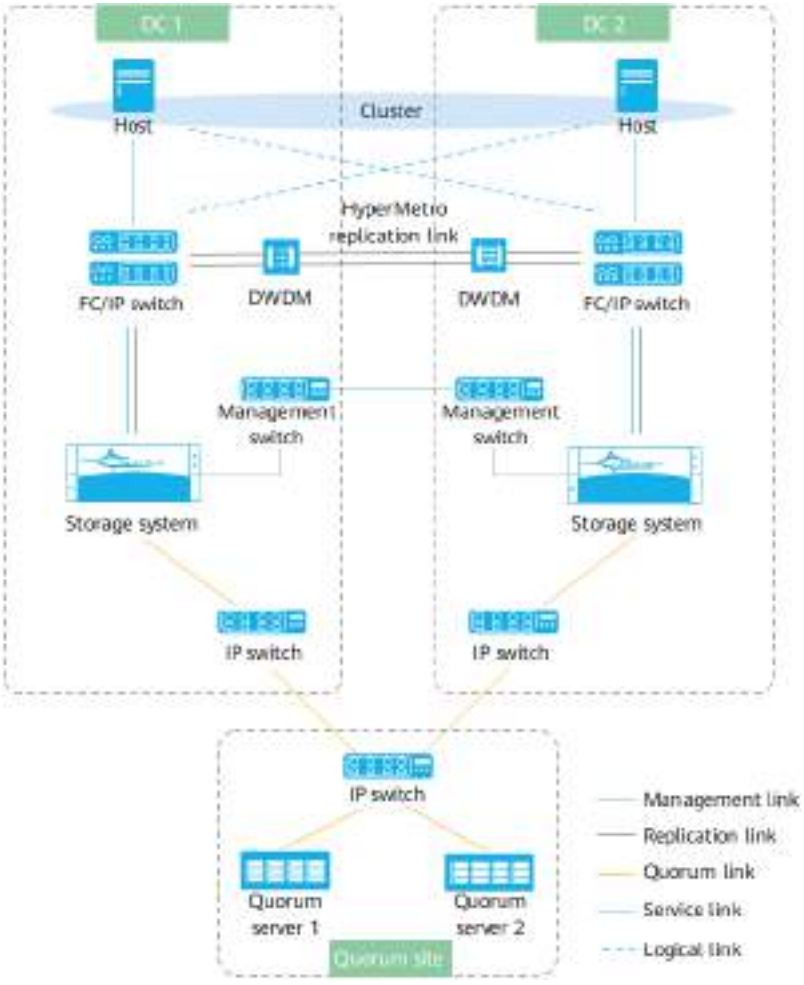
This section describes the network planning when two quorum servers are deployed for the active-active DC solution, including the standard, non-recommended, and unsupported networking modes.

3.3.1 Standard Networking

You can add two quorum servers to the HyperMetro domain for higher availability.

Figure 3-10 illustrates the recommended networking diagram when two quorum servers are deployed.

Figure 3-10 Recommended networking diagram for dual-quorum-server deployment



Plan the storage systems and quorum servers based on **Table 3-3**.

Table 3-3 Network planning

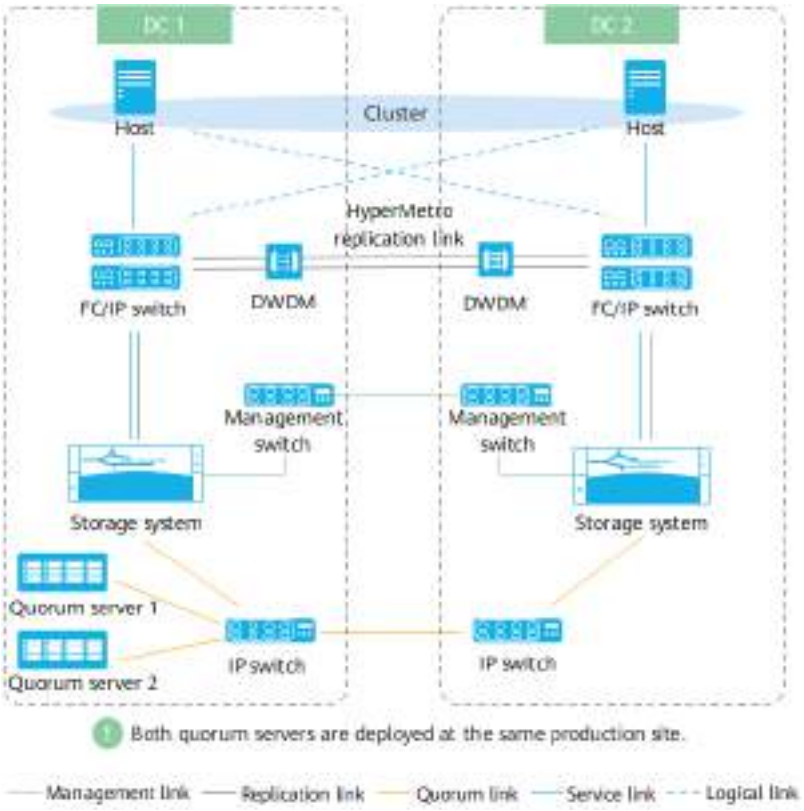
Device	Description
Storage system	Each controller of every storage system provides a GE or 10GE port for the quorum network. These ports must use different IP addresses.
Quorum server	Each quorum server provides two independent ports.

3.3.2 Non-Recommended Networking

Both Quorum Servers Deployed in the Same Active-Active DC

Figure 3-11 is an example of deploying the quorum servers in DC 1.

Figure 3-11 Networking diagram



- Scenario

  The quorum servers are deployed in DC 1 or DC 2.

- Risk

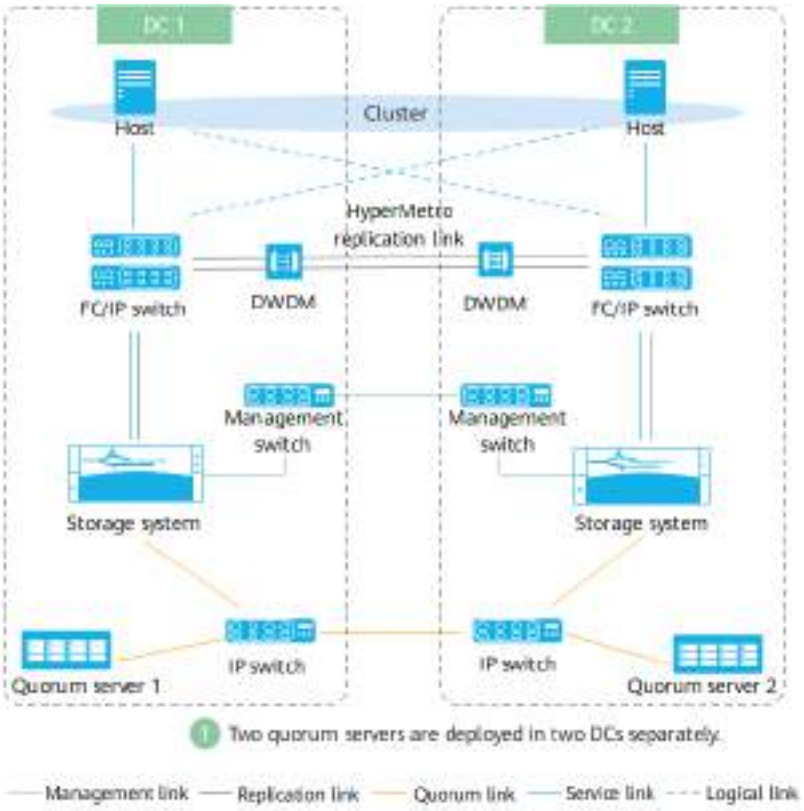
  Services will be interrupted if the DC where the quorum servers are deployed is down due to a power failure or an unexpected disaster.

3.3.3 Unsupported Networking

Two Quorum Servers Deployed in Different DCs Separately

Figure 3-12 is an example of deploying the two quorum servers in different DCs separately.

Figure 3-12 Networking diagram



- Scenario

  The two quorum servers are deployed in DC 1 and DC 2 separately.

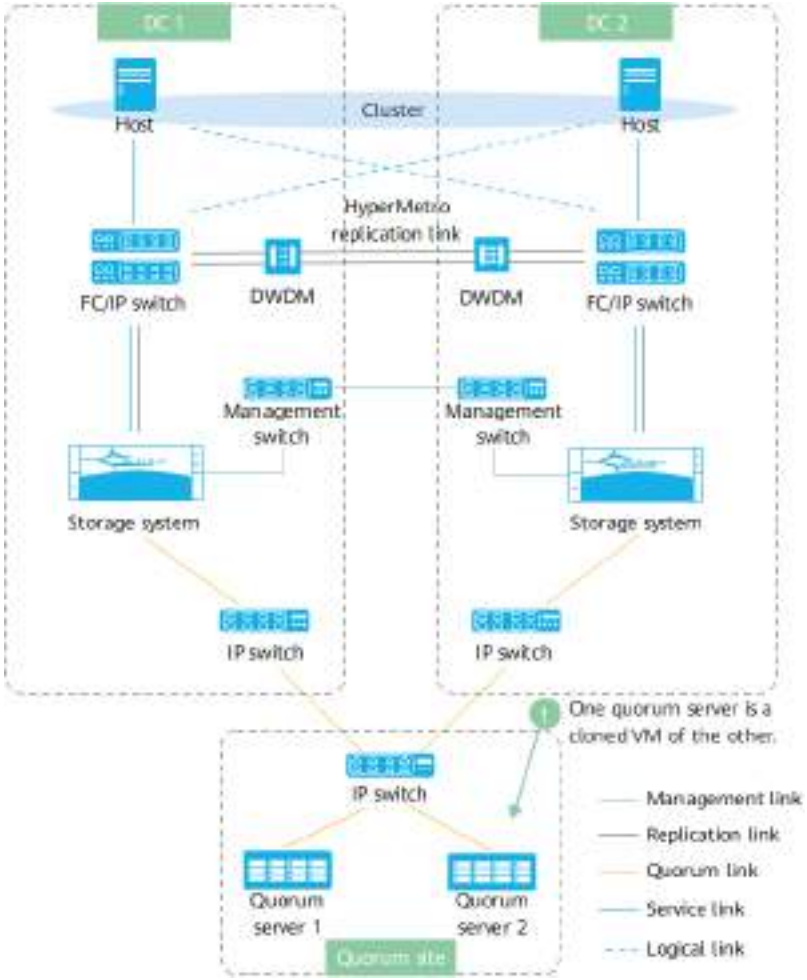
- Risk

  The active and standby quorum servers are far away from each other, so switchover between them may be impacted by network delay. In this case, services may be interrupted in the event of a site failure.

Cloned VM Used as the Other Quorum Server

In this networking mode, a VM is used as the quorum server and the VM is cloned as the other quorum server. Figure 3-13 shows the networking mode.

Figure 3-13 Networking diagram



- Scenario

  The quorum server is a cloned VM of the other existing quorum server VM.

- Risk

  The cloned VM has the same information as the source VM, which will cause a quorum server conflict.

3.4 Storage Interconnection Rules

This section describes how to plan a HyperMetro storage layout.

Both HyperMetro storage systems must comply with the following principles.

Storage Devices

For OceanStor storage systems, the local and remote storage systems of HyperMetro can use the same or different product models. To be specific, HyperMetro can be configured between:

- OceanStor 5510 and OceanStor 5610

- OceanStor 6810, OceanStor 18510, and OceanStor 18810

The OceanStor 6.x storage systems provide different performance from OceanStor V3, OceanStor V5, OceanStor Dorado 6.x, and OceanStor Dorado V3 storage systems. Therefore, HyperMetro cannot be configured between OceanStor 6.x and OceanStor V3, OceanStor V5, OceanStor Dorado 6.x, or OceanStor Dorado V3.

Storage Pools

- The storage pools where the HyperMetro LUNs reside must use the same storage media and configurations (such as RAID policies).

LUN

- The local and remote LUNs in a HyperMetro pair must have the same capacity.
- The LUNs in a HyperMetro pair must be mapped to all hosts.
- The LUNs used by a database or VM must be added to the same consistency group. The snapshots of LUNs used by the same application must be protected by a consistency group.
- If either of the two storage systems has taken over a heterogeneous storage system, eDevLUNs that are taken over in online mode and have the **Third-party** or **Basic masquerading** properties can be used to create HyperMetro pairs. Before creating HyperMetro pairs, use SmartMigration to migrate data to the local storage system. After data migration is complete, cancel the migration relationship and use the eDevLUNs as internal LUNs. The remote LUN of the HyperMetro pair is an internal LUN whose masquerading property is **No Masquerading**.

3.5 Application Planning

This section provides suggestions on how to plan the application layer.

3.5.1 Planning the Oracle Database

Proper partitioning of applications and distribution of data storage resources reduce the data traffic generated when Oracle RAC Cache Fusion reads and writes data in both DCs. Use **Huawei Storage Interoperability Navigator** to query the supported Oracle versions.

Application Partitioning

Application partitioning is applicable to scenarios where core service data is loosely related and upper-layer services can be isolated according to different applications. To prevent Cache Fusion from frequently transmitting data blocks among instances, the most effective solution is to store applications in different partitions, namely, to run different applications on different RAC instances for application isolation.

Data Partitioning

Data partitioning is applicable to scenarios where some applications' accesses to the data concentrate on a few tables. In this situation, it is difficult to isolate applications, and more refined optimization is required.

- Partition tables according to application characteristics.

  Store the tables in different partitions to prevent a certain instance from using a certain partition or to achieve physically distributed data storage. For RAC applications, partitioning tables are effective in reducing the possibility of hot data block contention.

- Place the data of certain read-only access or the data generated by read-only access in a certain period in a read-only table space.

  When Cache Fusion is enabled, if a certain table space is read-only, accesses to the data in this table space can be performed locally and do not require coordination between RAC instances.

ASM Disk Groups

- To improve file management efficiency and database performance, you are advised to store different types of files in different automatic storage management (ASM) disk groups.
- Oracle temporary table space is used to query and save buffer data and sort queried intermediate results. If there are a large number of "group by" query systems, you are advised to create an independent ASM disk group for the temporary table space to ensure that sufficient disk space is available and to improve query efficiency.
- In Oracle RAC OLTP environments, to reduce the possibility of resource contention due to the storage of user data and system data on the same disk group, you are advised to dedicate two ASM groups respectively to the file where system table space and recovery table space reside and the file where user data resides.
- When creating ASM disk groups, you must set redundancy levels as required. Two redundant ASM disks are configured at the storage layer. Unless there are special requirements for high availability, you are advised to set EXTERNAL redundancy for all disk groups except the disk group where Oracle RAC files are stored and use Huawei storage RAID 2.0+ technology and HyperMetro for data protection.

3.5.2 Planning the VMware Application

This section describes the principles for planning virtualization services.

HyperMetro Consistency Group

If the space for a VM is allocated across datastores, all HyperMetro LUNs mapped to the host cluster must be added to the same HyperMetro consistency group. If cross-datastore space allocation is not involved, you do not need to create a consistency group.

vMotion Network

The vMotion network is a migration network defined by a virtual cluster. When VMs are migrated in online mode between hosts, fast memory synchronization is required between hosts to achieve fast online migration. The latency must be less than 5 ms (the latency varies with versions and 5 ms is the recommended value). The 10GE network is recommended.

Host Layer Configuration

When the VMware ESXi cluster works with HyperMetro, host layer parameters must be configured for the Permanent Device Loss (PDL) and All Paths Down (APD) scenarios.

When the Hyper-V cluster works with HyperMetro, you must configure a proper cluster timeout period.

Use **Huawei Storage Interoperability Navigator** to query the supported VMware and Hyper-V versions.

4 Check Before Delivery

Check the items described in this section before delivering the HyperMetro solution and components.

Table 4-1 lists the check items.

Table 4-1 Check items before delivery

Category	Item	Criteria	Method
Device list	Hardware models and configurations of the HyperMetro storage systems	• The hardware models meet the requirements described in **3.4 Storage Interconnection Rules**. • (Recommended) The hardware configurations (such as the number of controllers and interface modules) are the same.	Verify that the hardware models, hardware configurations, and license files of the two DCs all match those listed in the Bill of Quotation (BOQ).
	HyperMetro license	Both storage systems must have the HyperMetro license.	

Category	Item	Criteria	Method
	Software version	The software versions of both storage systems must be identical.	On the storage systems, run the **show version all** command to query the version. admin:/>show version all Product Version : XXX
	Switch license **NOTE** Applies to HyperMetro deployment across DCs.	The switch has the long-distance transmission license and cascading license. **NOTE** The long-distance transmission license is required if the distance between the DCs is over 10 km.	Check the switch based on the BOQ.
	DWDM device **NOTE** Applies to HyperMetro deployment across DCs.	The DWDM device is deployed.	Check the device based on the BOQ or on the live network at the field.
Compatibility	Multipathing software	Meets the HyperMetro compatibility requirements.	Check the compatibility using the **Huawei Storage Interoperability Navigator**.
	Operating system and application version of the application server	Meets the HyperMetro compatibility requirements.	
	Switch	Meets the HyperMetro compatibility requirements.	

Category	Item	Criteria	Method
Network quality	Distance between the active-active DCs, latency, and packet loss rate	• The requirements for database services are as follows: – Distance < 100 km – Round-trip time (RTT) ≤ 1 ms – No jitter or packet loss – Bit error rate (BER) ≤ 10^{-12} • The requirements for non-database services (such as the virtualization platform and file system cluster) are as follows: – Distance < 300 km – RTT ≤ 10 ms – No jitter or packet loss – BER ≤ 10^{-12}	• Check the RTT and packet loss rate. On the storage systems, run the **ping -I** command to check the RTT and packet loss rate of network. For example, you can send three 1024-bit packets from the local eth2 port. Storage: minisystem> ping -I eth2 -c 3 -s 1024 9.41.51.60 PING 9.41.51.60 (9.41.51.60) from 9.41.51.22 eth2: 1024(1052) bytes of data. 1032 bytes from 9.41.51.60: icmp_seq=1 ttl=64 time=4.07 ms 1032 bytes from 9.41.51.60: icmp_seq=2 ttl=64 time=0.239 ms 1032 bytes from 9.41.51.60: icmp_seq=3 ttl=64 time=0.233 ms --- 9.41.51.60 ping statistics --- 3 packets transmitted, 3 received, 0% packet loss, time 2000ms rtt min/avg/max/mdev = 0.233/1.515/4.075/1.810 ms **NOTE** In this example, 9.41.51.60 is the IP address of the management network port on the peer storage system. • Check the BER. Log in to the switch and run the relevant commands to collect statistics. For details about the commands, see the switch user guide.

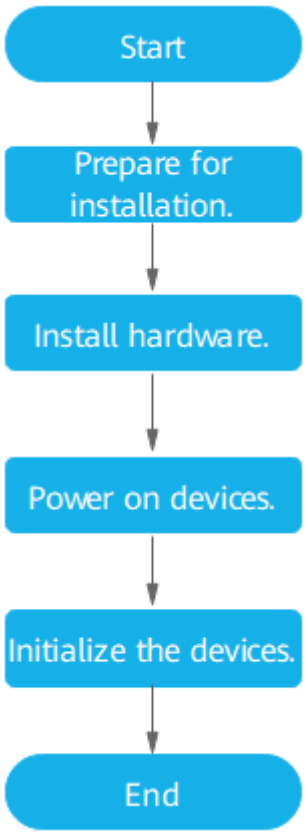
5 Installing Hardware

This chapter describes how to install the hardware required by this solution and initialize the configurations.

5.1 Installation Process

Figure 5-1 shows the installation process.

Figure 5-1 Installation process



5.2 Preparing for Installation

This section describes the tools, meters, software, and documentation that you must prepare before installation.

Tools and Meters

Marker, Phillips screwdriver, flat-head screwdriver, diagonal pliers, crimp pliers, and multimeter.

Hardware

Prepare the following hardware before deploying HyperMetro:

- Storage systems

  The storage system models and versions meet the requirements in **3.4 Storage Interconnection Rules**.
- Switches

  The switches meet the compatibility requirements. For details, see **Huawei Storage Interoperability Navigator**.
- Quorum server

NOTE

For the quorum server specifications, see the *Product Description* specific to your storage system.

- Huawei dedicated quorum server

  These servers include 1288H V5 and the 2280 balanced model (2280 for short) of TaiShan 200. EulerOS has been installed and customized security policies have been configured on these servers. For details about the components of the 2280 server, see the *TaiShan 200 Server User Guide (Model 2280)*.

- Other quorum servers must meet the following requirements:

  - CPU: 2-core 1.6 GHz CPU (minimum configuration).
  - Memory: 4 GB DDR memory (minimum configuration)
  - The operating system must meet compatibility requirements. Use **Huawei Storage Interoperability Navigator** to check compatibility.

    For details, see **15.4 How Can I Query Compatibility of the Quorum Server on Huawei Storage Interoperability Navigator?**
  - Storage capacity for installing the quorum server software: ≥ 10 GB
  - Number of network ports: ≥ 3. One network port is used for operating system management and the other two are used as quorum ports that connect to the storage systems.
  - The quorum server software can be deployed on either a physical machine or a virtual machine (VM). If a VM is used, its system and data disks can be created only on local disks of the servers or LUNs independent of the HyperMetro storage systems.

Documentation

You must prepare the following materials before installing any devices: the contract or agreement, a device configuration table, the equipment room design schema, a construction drawing paper (provided by the customer), and product documents listed in **Table 5-1**.

Table 5-1 Documentation list

Document	How to Obtain
Installation guide, initialization guide, and basic storage service configuration guide specific to your product model	Log in to **https://support.huawei.com/enterprise/**. In the search field, enter the product name and download the documents of the corresponding version. For example, if you want to obtain the installation guide, log in to **https://support.huawei.com/enterprise/**, enter your storage model in the search box, and select the associated path to the product documentation page. Then specify the product version, and find and download the desired document.

5.3 Installing Hardware and Connecting Cables

Install and connect devices in DC A, DC B, and the quorum site in sequence.

Table 5-2 describes the hardware installation process.

Table 5-2 Hardware installation process

Site	Step	Remarks
DCs A and B	1. Install the storage systems and connect the cables inside the systems. 2. Install the switches. 3. Connect the storage systems to the switches.	• For details about how to install the storage systems, see the installation guide specific to your product model. • For details about how to install switches, see the user guide of your switches.
Quorum site	1. Install the quorum server. 2. Install the switches. 3. Connect the quorum server to the switches.	• For details about how to install the quorum server, see its user guide. • For details about how to install the switches, see their user guide.

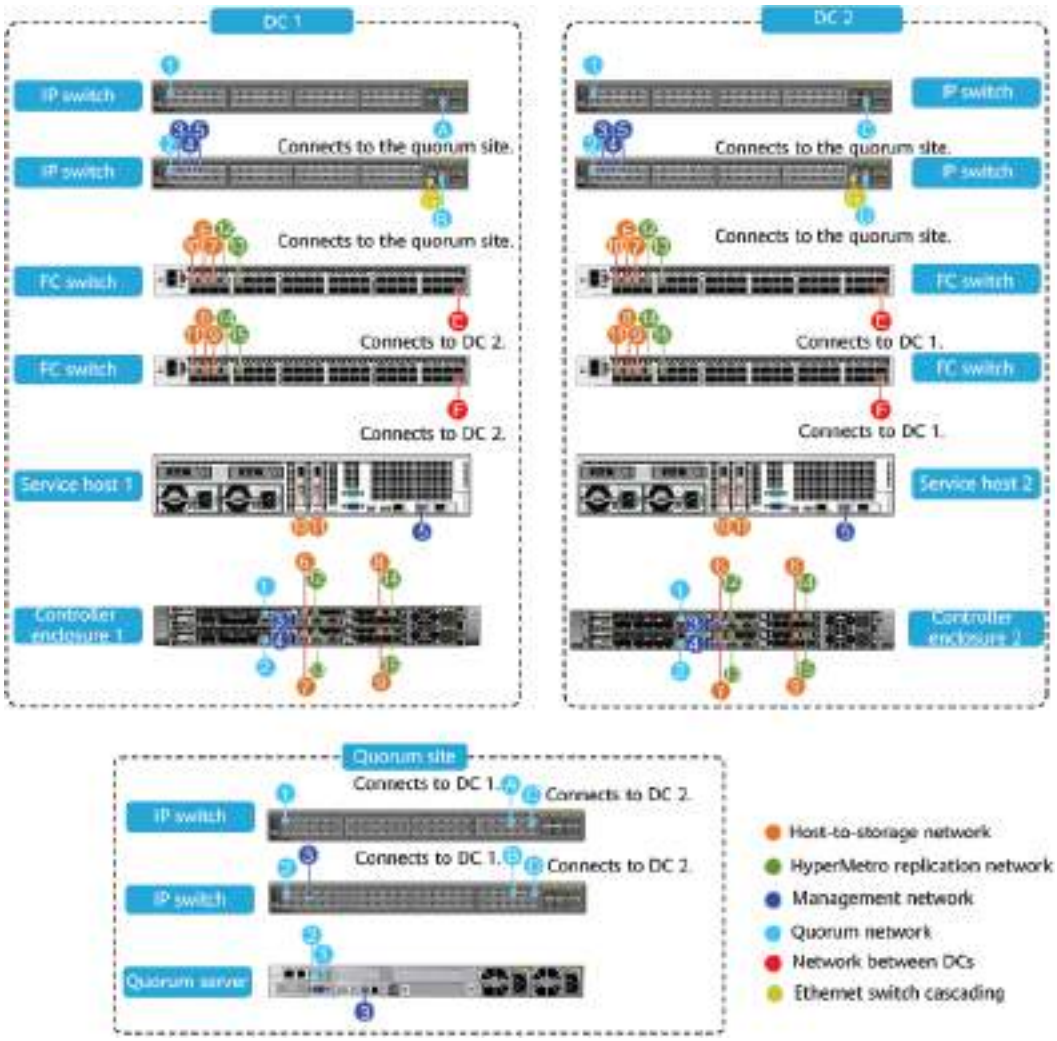
5.3.1 Cable Connection When One Controller Enclosure Is Deployed

Connect the cables for the host-to-storage network, HyperMetro replication network, quorum network, and management network.

Dual-Controller Connection

Figure 5-2 uses OceanStor 5310 as an example.

Figure 5-2 Cable connections in and across DCs (2 U storage device)



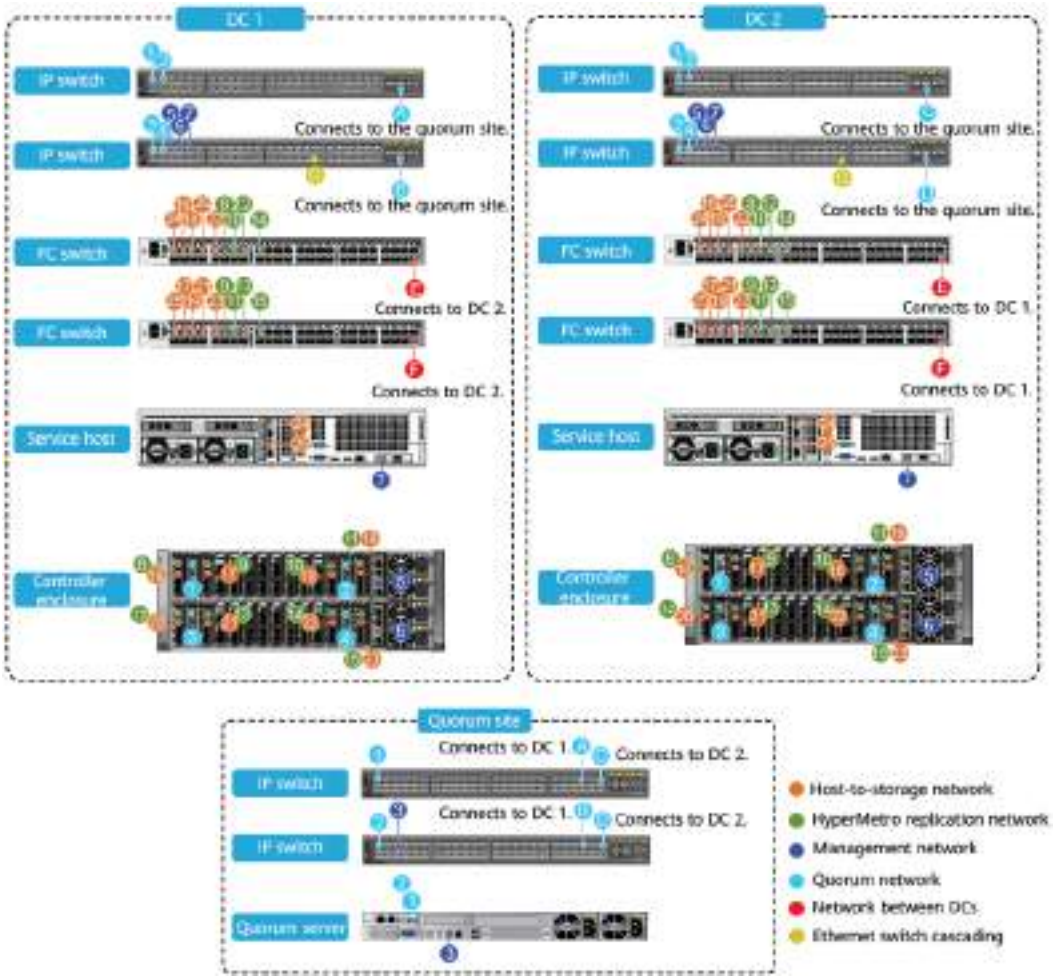
NOTE

- The numbered ports are connections within a DC and the lettered ports are connections across DCs.
- For connections within a DC, connect the ports with the same numbers; for connections across DCs, connect the ports with the same letters.
- For details about cable connections between disk enclosures and controller enclosures, see "Connecting Disk Enclosures" in the installation guide corresponding to your product model.

Four-Controller Connection

Figure 5-3 uses OceanStor 6810 as an example.

Figure 5-3 Cable connections in and across DCs (4 U storage device)



NOTE

- The numbered ports are connections within a DC and the lettered ports are connections across DCs.
- For connections within a DC, connect the ports with the same numbers; for connections across DCs, connect the ports with the same letters.
- For details about cable connections between disk enclosures and controller enclosures, see "Connecting Disk Enclosures" in the installation guide corresponding to your product model.

Table 5-3 explains the cable connection principles (using the Fibre Channel replication network as an example).

Table 5-3 Cable connection principles

Network Type	Cable Connection Principle
Host-to-storage network	• Each host has a logical connection to every controller on both storage systems. • Hosts and storage systems are connected by Fibre Channel switches. Each DC has two Fibre Channel switches. • Each Fibre Channel switch has at least *N* ports to connect hosts and storage systems (*N* = 1 x Number of servers + 2 x Number of storage systems). • Host-to-switch connection: Each host has at least two Fibre Channel ports to connect to the two Fibre Channel switches in the local DC. It is recommended that the two ports be on different HBAs. • Storage-to-switch connection: Each controller has at least two ports to connect to the two Fibre Channel switches in the local DC. It is recommended that the two ports be on different Fibre Channel interface modules.
HyperMetro replication network	• The HyperMetro replication network between storage systems is connected by Fibre Channel switches. Each DC has two Fibre Channel switches. • Storage-to-switch connection: Each controller has two Fibre Channel ports to connect to the two Fibre Channel switches in the local DC. It is recommended that the two ports be on different Fibre Channel interface modules. • DWDM devices are recommended for DC interconnection. • The Fibre Channel switches are cascaded in one-to-one mode. (If the HyperMetro replication network is an IP network, Ethernet switches are cascaded in one-to-one mode.)
Quorum network	• The quorum server is connected to the storage systems by Ethernet switches. Each DC has two Ethernet switches. • Each controller of a storage system has one IP port to connect to one Ethernet switch in the local DC. • The quorum server has two IP ports to connect to two Ethernet switches at the quorum site. It is recommended that the two IP ports be on different network adapters.
Management network	An Ethernet switch is used for management. The management network ports of the hosts and storage controllers are connected to one Ethernet switch of the DC.

5.3.2 Cable Connection When Multiple Controller Enclosures Are Deployed

This section describes how to connect the networks if the storage systems are scaled out (controller expansion).

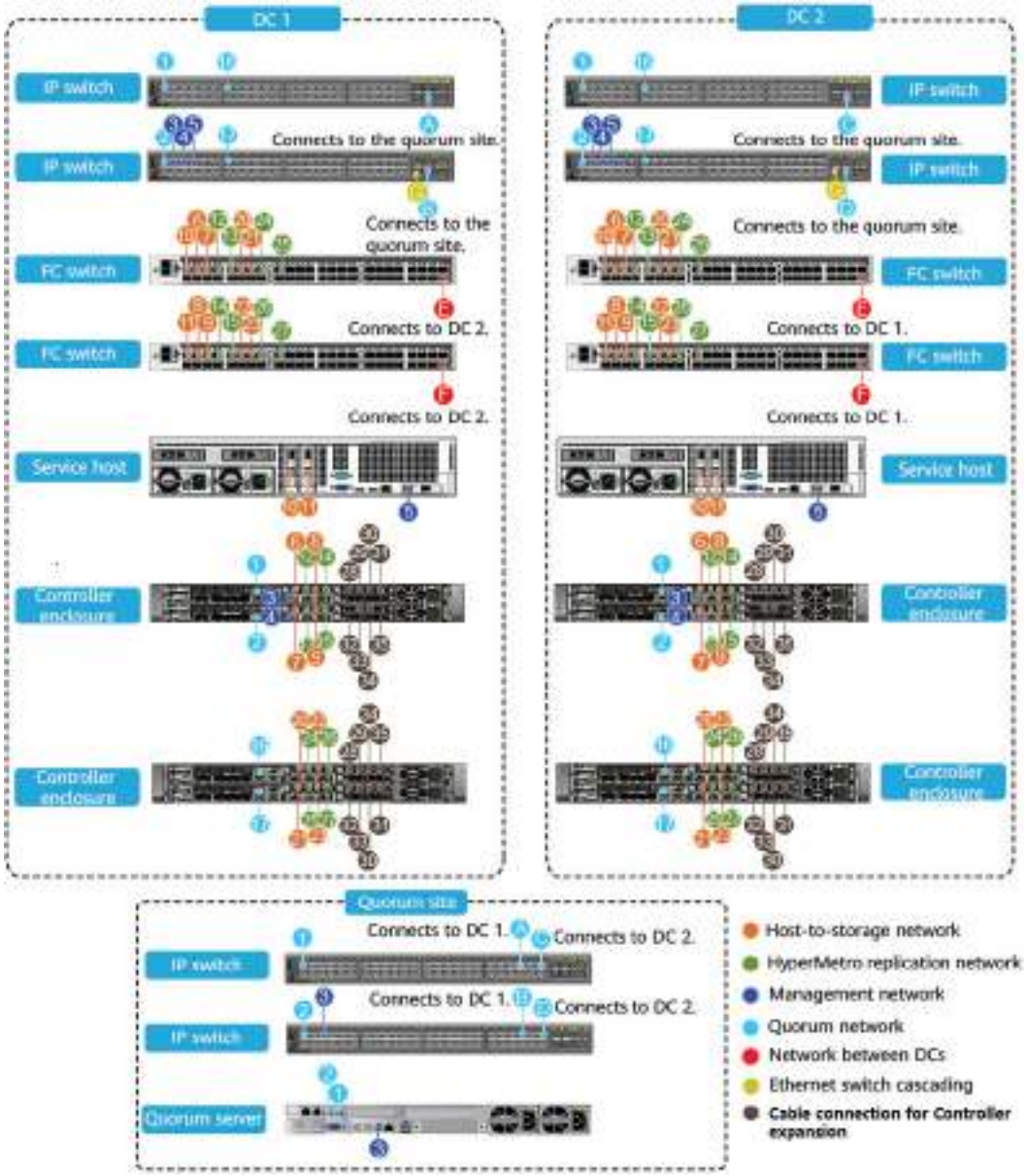
NOTE

For details on how to add controllers to a storage system, see the *Installation Guide* specific to your product model.

Four-Controller Connection

Figure 5-4 uses OceanStor 5310 four-controller deployment as an example.

Figure 5-4 Cable connections for four-controller deployment



NOTE

- The numbered ports are connections within a DC and the lettered ports are connections across DCs.
- For connections within a DC, connect the ports with the same numbers; for connections across DCs, connect the ports with the same letters.
- For details about cable connections between disk enclosures and controller enclosures, see "Connecting Disk Enclosures" in the installation guide corresponding to your product model.

Table 5-3 explains the cable connection principles (using Fibre Channel networking as an example).

Table 5-4 Cable connection principles

Network Type	Cable Connection Principle
Host-to-storage network	• Each controller has at least two ports to connect to the replication network. It is recommended that the ports be on different interface modules. • The ports that connect to the replication network must have the same speed. Other cabling principles are the same as those for the connection of a single controller enclosure. For details, see **5.3.1 Cable Connection When One Controller Enclosure Is Deployed**.
HyperMetro replication network	
Network between DCs	
Quorum network	
Management network	

5.4 Powering On Devices

After installing all devices, power on them and check their operating status. It is critical to ensure all devices and hardware have been properly installed before powering on them.

Context

- Devices can be powered on only when representatives from the customer and Huawei are onsite to confirm the operation.
- Use of power sourcing equipment (PSE), power distribution equipment (PDE), and powered devices (PDs) must comply with standards and regulations.
- After the customer's administrative unit has approved the power-on application, the devices can be powered on and operated under the supervision of the customer's technicians and engineers.
- PDs must be connected to the PSE and PDE at the positions specified on the units.
- You must use a measuring instrument to check whether the power supplies meet the following requirements before powering on a device:

- The device and its power supply are not short-circuited, the power cable is firmly connected, the output switch of the PSE is turned off, and the output voltage is within the normal range.
- All power switches of the PDs are turned off.

Procedure

Step 1 Connect ground cables.

1. Huawei personnel must connect all ground cables for cabinets and storage devices and check that the ground resistance connectors are firmly attached.
2. Huawei personnel must also test the ground resistance between the storage cabinets and the equipment room.

Step 2 Power on power distribution frames (PDFs) and cabinets.

1. Huawei is responsible for turning on miniature circuit breakers (MCBs) and switches of PDFs and cabinets.
2. The customer must check the output voltage of the PDFs and cabinets and ensure that it falls within the normal range. The customer must also verify that the PSE has sufficient redundant power supplies to meet the power requirements of all connected cabinets and storage devices.

Step 3 Power on devices.

1. Huawei is responsible for turning on switches of power distribution units (PDUs) and powering on devices in sequence under the customer's supervision.

   The power-on sequence is: storage devices > Fibre Channel switches > core switches > application servers.

   NOTE

   Verify that each device is operating properly before powering on the next. For details about how to power on storage devices, see "Powering On Devices" in the installation guide specific to your product model.
2. The customer must verify that the input power is stable while Huawei personnel are powering on the cabinets and storage devices.

----End

Follow-up Procedure

After powering on devices, you must verify that:

- Fans of the devices are working properly and air is being exhausted from the air vent.
- The device indicators are normal.

  NOTE

  For details about the indicator status, see the product description specific to your product model.
- Log in to each device and check its operating status.

5.5 Initializing Devices

Storage systems and switches must be initialized after they are powered on.

- Storage system initialization includes configuring IP addresses for the management network ports, applying for and importing licenses, initializing the system configurations, and configuring alarm handling policies.

  NOTE

  For details on how to initialize a storage system, see the initialization guide specific to your product model.

- Switch initialization includes configuring IP addresses for the management network ports.

  NOTE

  For details, see the user guide specific to your switch model.

6 Configuring Host Applications

The active-active SAN solution is applicable to databases (Oracle and SQL), operating system applications (Windows), and virtual clusters (VMware, FusionSphere, and Hyper-V).

6.1 Oracle RAC

Use **Huawei Storage Interoperability Navigator** to query the supported Oracle versions.

To reduce private network traffic and improve database performance, the following configurations are recommended.

- Application partition: Run different applications on different RAC instances for application isolation.
- Data partition:
  - Partition tables according to the application types.
  - Place the data that can be read only or the data that can be read only in a certain period into the read-only table space.
- Principles of planning Automatic Storage Management (ASM) disk groups:
  - Store different types of files in different ASM disk groups.
  - If there are a large number of systems using the **group by** query statement, create an independent ASM disk group for the temporary table space.
  - Dedicate two ASM groups respectively to the file where system table space and recovery table space reside and the file where user data resides.
  - If there are no special requirements on high availability, you are advised to apply **EXTERNAL** redundancy policy to all disk groups except the one where Oracle RAC files reside and use RAID2.0+ and active-active technologies of Huawei storage for data protection.

6.2 SQL Server

When SQL Server databases are used, to reduce the I/O latency and offer optimal performance, set **target_recovery_time** to **60** according to the SQL official suggestion. For details, see **https://docs.microsoft.com/en-us/sql/relational-databases/logs/database-checkpoints-sql-server#IndirectChkpt**.

NOTE

The preceding operation applies to SQL Server 2012 and later.

6.3 Windows Cluster

This section describes Windows cluster configuration requirements. Use **Huawei Storage Interoperability Navigator** to query the supported Windows versions.

- Set the timeout parameter of the cluster hosts' quorum disks to 60 seconds (20 seconds by default):
  a. Start **PowerShell** and run the **Get-Cluster | fl*** command.
  b. In the command output, check whether the value of **QuorumArbitrationTimemax** is **60**. If it is not, go to the next step.
  c. Run the **(Get-Cluster** *cluster_name***).QuorumArbitrationTimemax=60** command.

  NOTE

  cluster_name represents the Windows cluster name.
- Set the disk timeout period of the host operating system to 60 seconds.

7 Configuring Multipathing Software

7.1 Optimized I/O Access Policies

By working with UltraPath, HyperMetro provides two I/O access policies based on the distance between the active-active sites.

- Load balancing mode
- Local preferred mode

Load Balancing Mode

This mode is mainly used when HyperMetro storage systems are deployed in the same DC. In this scenario, both storage systems deliver almost the same access performance to a host. To maximize resource usage, host I/Os are evenly distributed to both storage systems.

Local Preferred Mode

This mode is mainly used when HyperMetro storage systems are deployed in different DCs. In this scenario, the two DCs may be far away from each other, and the round-trip time is longer than in a single DC. In this mode, you can assign a preferred storage system on UltraPath. Host I/Os are delivered only to the preferred storage system. This avoids I/O access across storage systems. I/Os are delivered to the non-preferred storage system only when the preferred storage system is faulty.

7.2 Configuring DC Connectivity

Perform the operations in **Table 7-1** in DCs A and B.

Table 7-1 Configuring connectivity in DCs A and B

Network Type	Operation
Fibre Channel	1. Log in to each of the hosts and query the WWNs of their Fibre Channel ports. 2. Log in to each of the Fibre Channel switches to query their models and versions and configure zones. 3. Log in to the storage systems to add initiators.
iSCSI	1. Log in to each of the hosts to configure service IP addresses and initiators. 2. Log in to each switch to configure VLANs. 3. Log in to the storage systems to configure IP addresses for Ethernet ports and add initiators.

7.3 Obtaining Software and Documentation

Table 7-2 lists the software packages and documents required for deploying HyperMetro.

Table 7-2 Software and document list

Software/Document Name	How to Obtain
Multipathing software **NOTE** • Huawei UltraPath and OS native multipathing software are supported. • For the multipathing software version supported by the storage system, refer to the version mapping table. • Use the OS installation CD-ROM to install the native multipathing software (if needed).	• Log in to **https://support.huawei.com/enterprise/** (you can register for an account at this website). Click **Centralized Storage** in **Enterprise Data Center** under **PRODUCT AND SOLUTION SUPPORT**. Then select **UltraPath** under **Others**. On the **Software Download** tab page, specify the version and click the desired software in the **Version and Patch** area. Then download the software. • For the version mapping information of UltraPath, download its *Version Configuration Information Form* from the **Documentation** area on the software download page.
• OceanStor UltraPath for XXX User Guide • Host Connectivity Guide	Log in to **https://support.huawei.com/enterprise/**. In the search field, enter the keywords and download the desired documents. For example: • If you want to obtain *OceanStor UltraPath for Linux 21.6.2 User Guide*, log in to **https://support.huawei.com/enterprise/**, enter **UltraPath Linux 21.6.2** in the search bar, and press **Enter** to view or download the relevant document. • If you want to obtain *Host Connectivity Guide for Windows*, enter **Host Connectivity Guide Windows** in the search bar, and press **Enter** to browse and download the document.

7.4 Installing Multipathing Software

7.4.1 Using SmartKit to Install UltraPath

SmartKit allows you to install UltraPath on multiple hosts in a batch. It significantly improves the installation efficiency with automatic software package

verification and uploading, pre-installation check, software installation, and post-installation check.

Prerequisites

- The UltraPath and SmartKit versions match the storage system version.

  NOTE

  You can query the version information in the version mapping table:

  1. Log in to **https://support.huawei.com/enterprise/**, enter your storage model in the search box, and select the associated path to the product documentation page.
  2. Find and download the version mapping table.
  3. Query the UltraPath and SmartKit versions in the version mapping table.

- You have used **PGP Verify** to check the integrity of the UltraPath software package. (If the check fails, ensure that you have obtained the correct UltraPath software package.)
- You have obtained the management IP address, and login username and password of the host and verified that the host hardware and software meet the software installation requirements. For details, see section "Environment Requirements" in the *OceanStor UltraPath for XXX User Guide*.

  NOTE

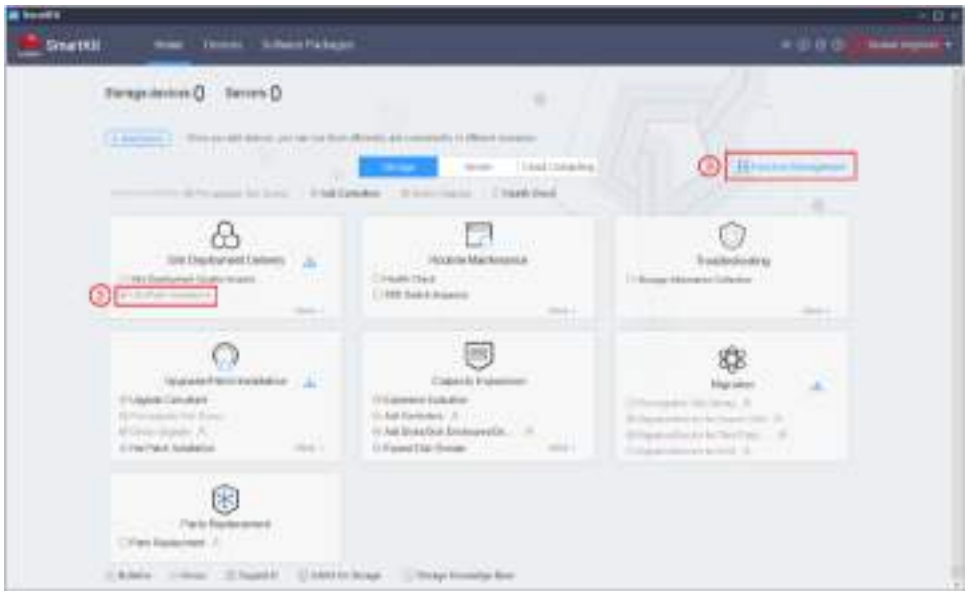
  To obtain the UltraPath user guide, log in to Huawei's technical support website (**https://support.huawei.com/enterprise/**), enter **UltraPath** in the search box, and select the associated path to the documentation page. Then find and download the desired document. To download software, click the **Software Download** tab and find the desired software.

Context

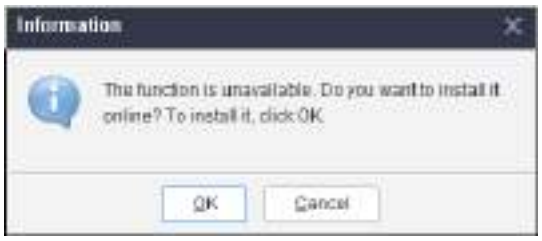
The GUI may vary slightly with the tool version.

Procedure

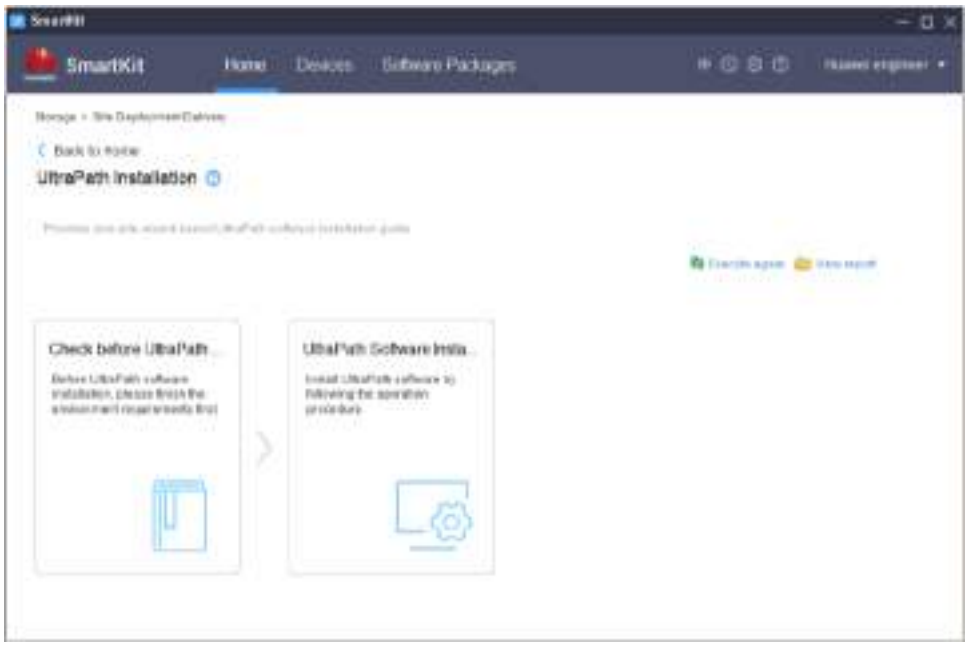
Step 1 Start and log in to SmartKit. Click the **Storage** tab. In the **Site Deployment Delivery** area, select **UltraPath Installation**.



If the following dialog box is displayed, click **OK**.

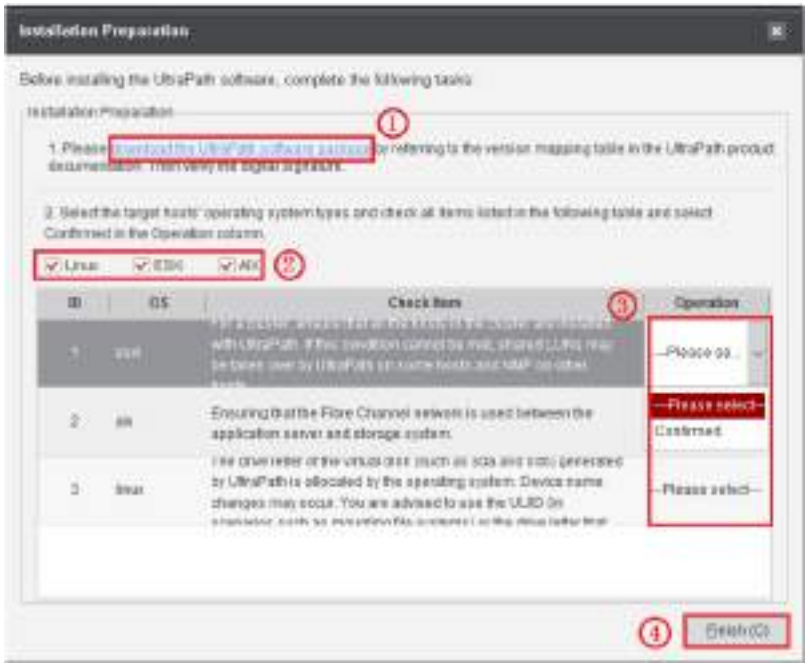


Step 2 In the UltraPath installation wizard, select **Check before UltraPath Installation.**

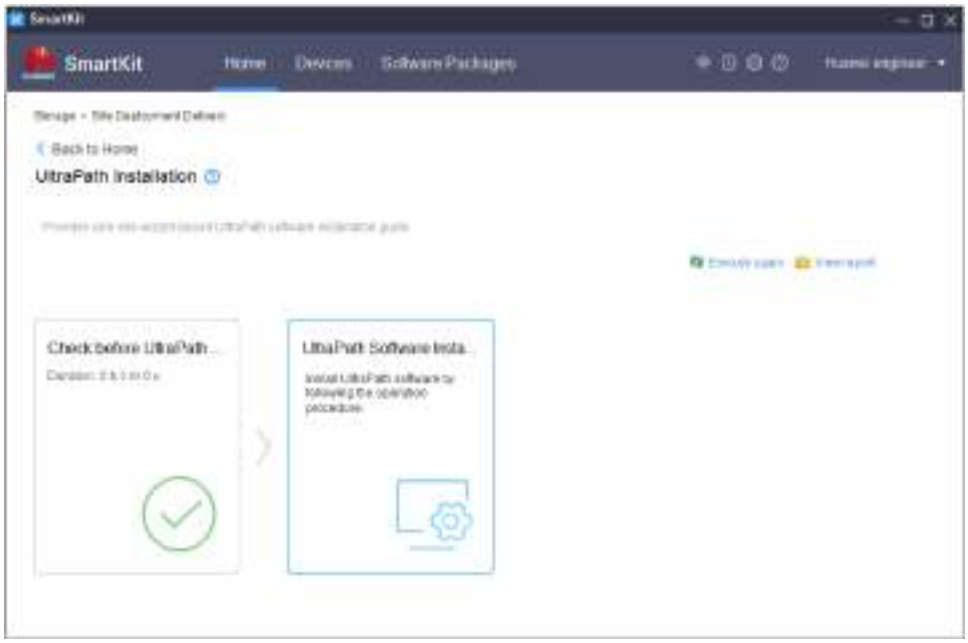


Step 3 In the displayed **Installation Preparation** dialog box, complete the following preparations as prompted:

1. Click **download the UltraPath software package**. On the support website, download the desired UltraPath software package. In addition, download the signature verification tool and verify the digital signature. If the UltraPath software package has been obtained, skip this step.
2. Select the operating systems of the hosts on which UltraPath is to be installed.
3. Manually complete a pre-installation check for all hosts and select **Confirmed** from the **Operation** drop-down list box on the right.
4. Click **Finish**.



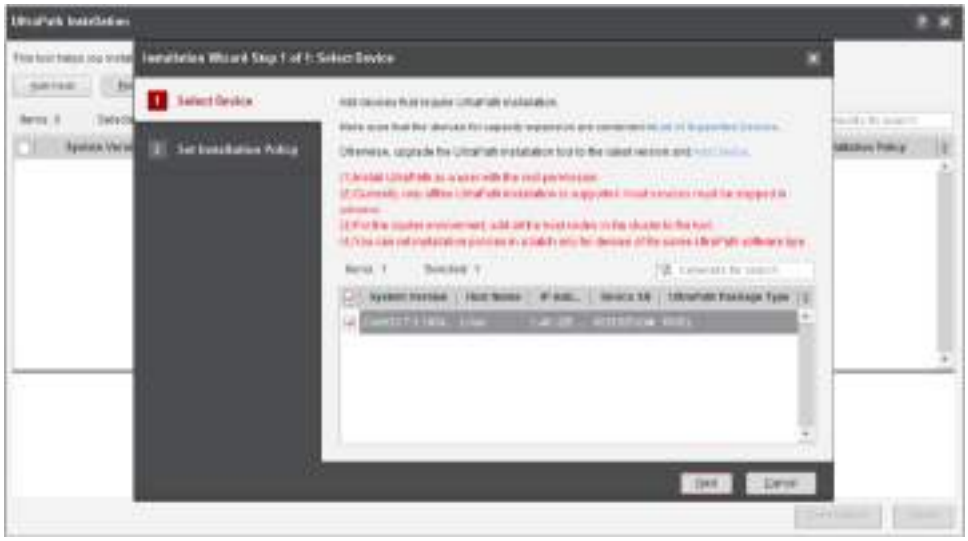
Step 4 In the UltraPath installation wizard, select **UltraPath Software Installation**.



Step 5 Add devices.

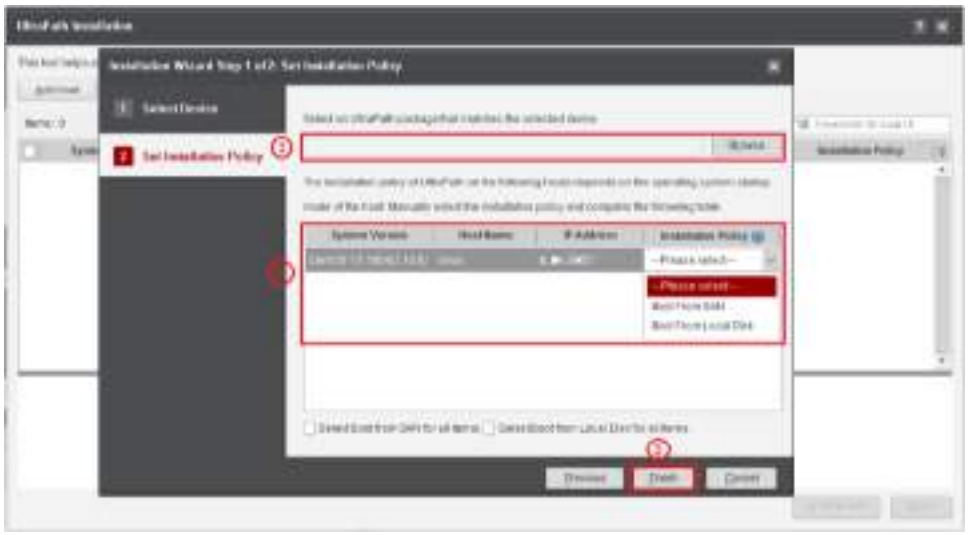
1. Click **Add Host**. The **Select Device** wizard is displayed.
2. Click **Add Device**. The **Add Device** dialog box is displayed.
3. To add one device, select **Device Type** and set **IP Address**.
4. To add devices in batches, click the **Template** link to obtain the corresponding template, fill in the device information, click **Path**, select the template file, and upload and parse the file. The system automatically adds the devices.

After the devices are added successfully, the tool displays the device information. Click **Next**.



Step 6 Set an installation policy.

1. Select an UltraPath software package for all the selected devices.
2. For Linux hosts, you must manually specify an installation policy.
   - **Boot From SAN**: If a host boots from the SAN storage, you must select this policy. Otherwise, the host may fail to restart. If the number of disks mounted to a host exceeds 500, you are advised to select this option.
   - **Boot From Local Disk**: If a host boots from a local disk, you are advised to select this option.
3. Click **Finish**. The configuration is complete and the main window is displayed.



Step 7 Click **Start**.

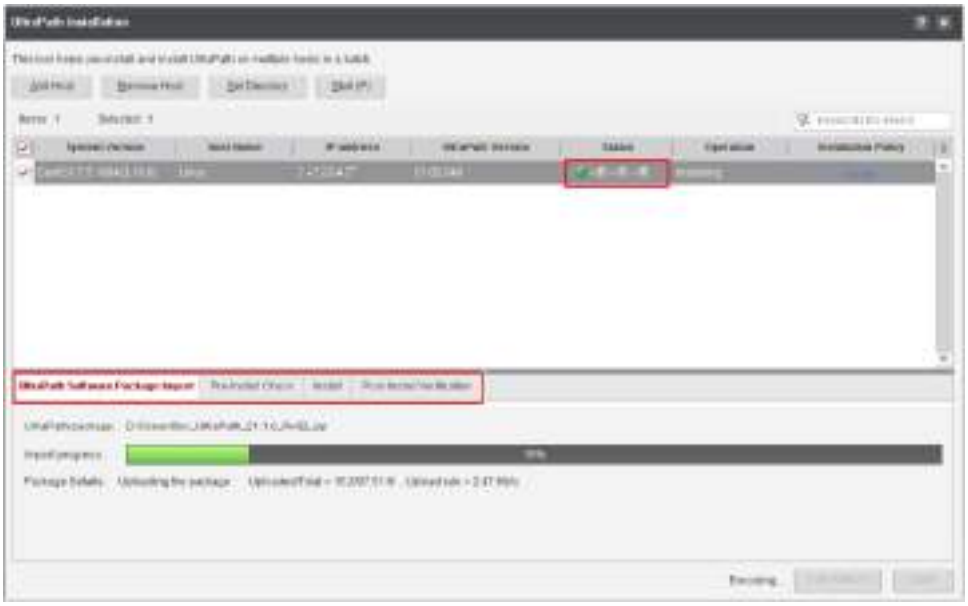
NOTE

- After hosts are added, they are displayed in the main window. If any host is incorrectly added, select it and click **Remove Host** to delete the host.
- After all the selected hosts have executed the installation policy, the system automatically generates a report. To specify a report directory, click **Set Directory**.
- To modify an installation policy, click **Modify** in the **Installation Policy** column.

Step 8 Confirm the precautions in the displayed dialog box, select **I have read the previous information and understood consequences of the operation**, and click **OK**.

Step 9 Start installing UltraPath.

1. The tool concurrently installs UltraPath on the selected hosts. You can select a host in the host list to view the current installation status.



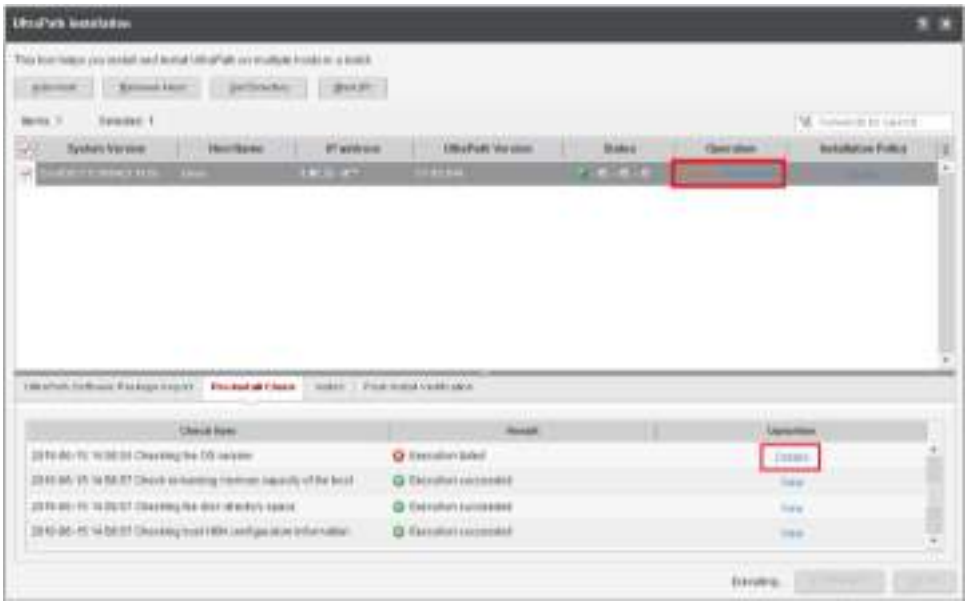
NOTE

The installation process consists of four steps. You can click each tab to view details about the corresponding step.

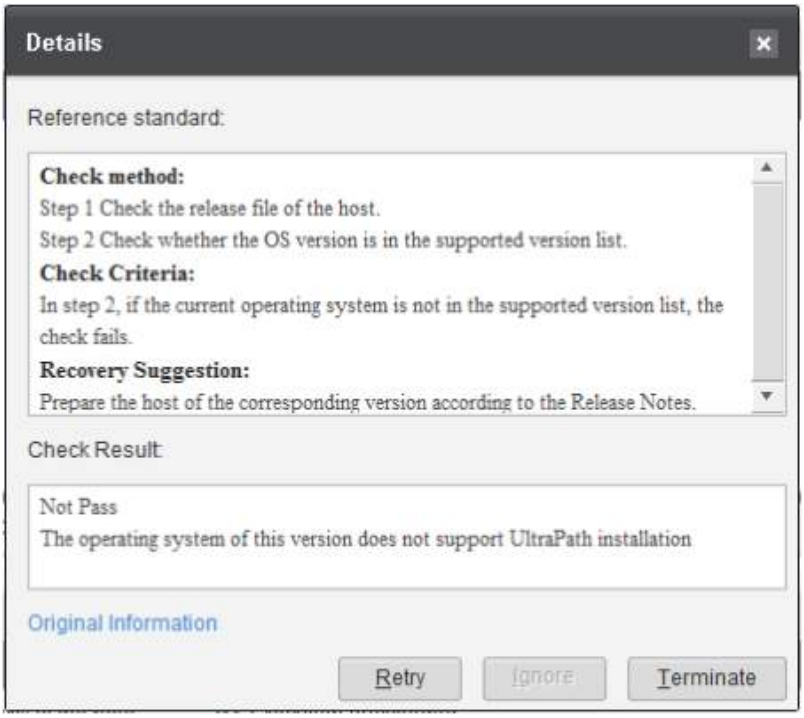
1. **UltraPath Software Package Import**: This step automatically uploads the software package to a host.
2. **Pre-Install Check**: This step checks that a host allows UltraPath to be installed on it.
3. **Install**: This step installs the main program of the UltraPath software.
4. **Post-Install Verification**: This step checks, activates, and validates the UltraPath software.

2. If some check items are not passed or need to be optimized, the system will suspend the installation and **Paused** will be displayed in the **Operation**

column in the upper pane. You can click **View Details** to view the current status. For a specific check item or operation item, click **Details** in the **Operation** column in the lower pane to view information.



3. The system provides a check method, check criteria, and recovery suggestion. If a check item fails, you can handle the problem according to the check result.

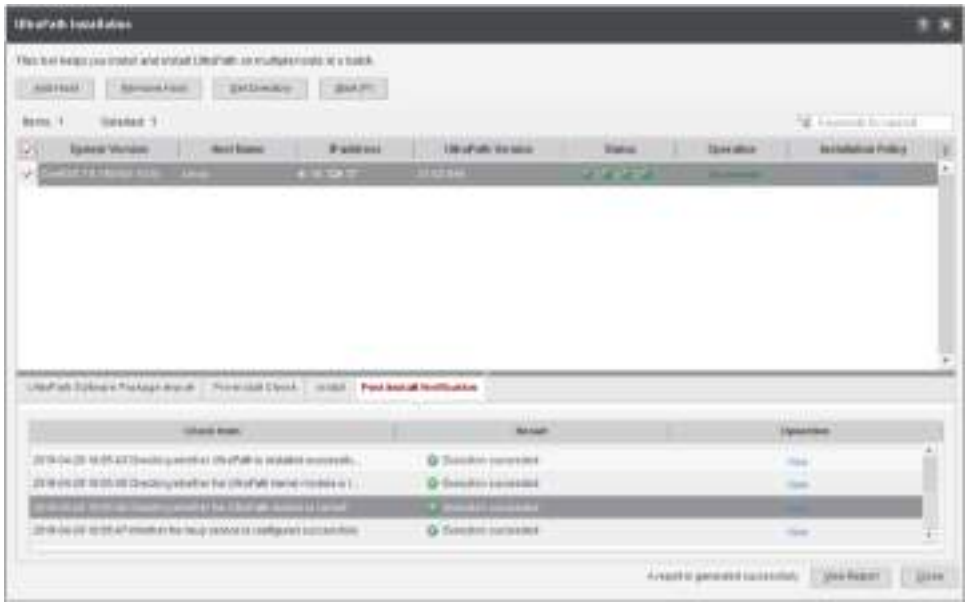


NOTE

Each check item can be retried, ignored, or terminated according to the policy requirements. If the current item does not support an operation, the corresponding button is unavailable.

- **Retry**: After the fault is rectified, click **Retry** to check the current item again.
- **Ignore**: Ignore this item and proceed with subsequent operations if the current check item or operation item can be ignored.
- **Terminate**: If you want to terminate the installation process, click this button. This may cause UltraPath software exceptions on the host. Exercise caution when performing this operation.

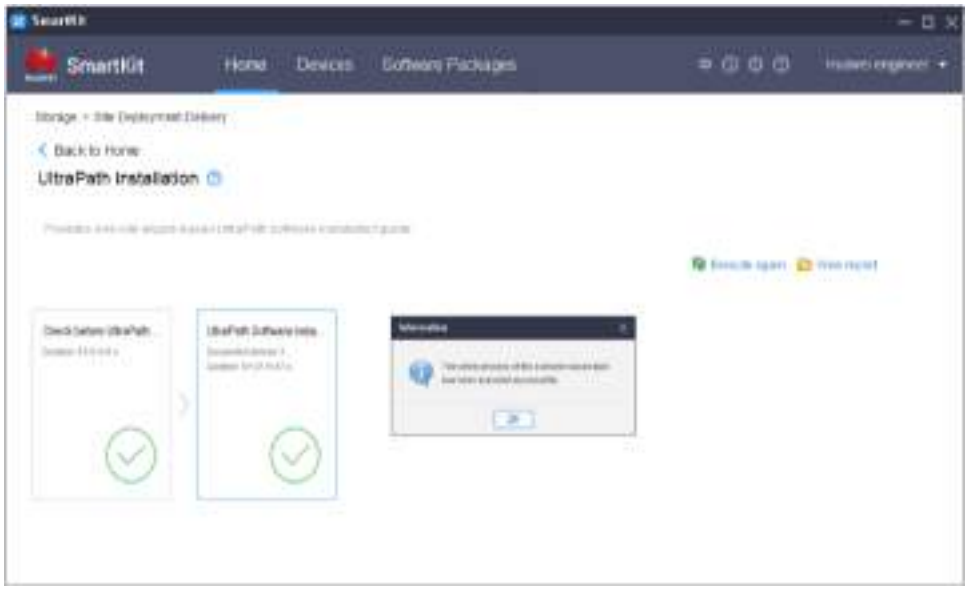
Step 10 After UltraPath has been installed on all the selected hosts, the system automatically generates an installation report in Excel format. Click **View Report** to view detailed information. Click **Close** to finish the installation.



NOTICE

Do not repeatedly install UltraPath on a host. If you need to upgrade UltraPath, use the UltraPath upgrade tool.

Step 11 The main window is displayed, and the UltraPath software installation is complete.



----End

7.4.2 Installing UltraPath

This section describes how to install UltraPath.

- UltraPath must be installed on all hosts.
- For the detailed installation method, see the *UltraPath User Guide* corresponding to your host OS.

  NOTE

  Log in to **https://support.huawei.com/enterprise/** and search for the *UltraPath User Guide* corresponding to your host OS.

7.4.3 Installing OS Native Multipathing Software

This section describes how to install OS native multipathing software.

- OS native multipathing software must be installed on all hosts.
- For the detailed installation method, see the *Host Connectivity Guide*.

7.4.4 Installing the DMP Multipathing Software

This section describes how to install the DMP multipathing software.

For the detailed installation procedure, see the user guide at DMP's official website.

7.5 Configuring an UltraPath Policy

7.5.1 AIX

7.5.1.1 Storage System Configuration

If UltraPath is used, retain the default settings of the initiator and configure **Host Access Mode** and **Preferred Path for HyperMetro** as required. **Table 7-3** lists the detailed settings.

Table 7-3 Storage configurations for interconnection with AIX application servers

HyperMetro Working Mode	Storage System	OS Setting	Host Access Mode	Preferred Path for HyperMetro	Description
Load balancing mode	Local storage	AIX	Load balancing	N/A	The host uses all paths of a disk with equal priority.
	Remote storage	AIX	Load balancing	N/A	
Local preferred mode	Local storage	AIX	Asymmetric	Yes	The host considers the paths from the local storage system as preferred paths, and those from the remote storage system as non-preferred paths.
	Remote storage	AIX	Asymmetric	No	

NOTICE

- For details about the AIX versions, see the **Huawei Storage Interoperability Navigator**.
- To change the LUN mapping on the storage system, including but not limited to changing the host LUN ID, changing the port online, and removing and adding a LUN, follow the instructions in **FAQs** in the *OceanStor UltraPath for AIX User Guide* to correctly change the LUN mapping. Otherwise, services may be interrupted.

7.5.1.2 Host Configuration

Install, configure, and use UltraPath by following instructions in the *OceanStor UltraPath for AIX User Guide*.

NOTE

- To obtain the document, log in to Huawei's technical support website (**https://support.huawei.com/enterprise/**), enter **UltraPath** in the search box, and select the associated path to the documentation page. Then find and download the desired document. To download software, click the **Software Download** tab and find the desired software.
- The UltraPath version matches the storage system version. You can query the version information in the version mapping table:
  1. Log in to **https://support.huawei.com/enterprise/**, enter your storage model in the search box, and select the associated path to the product documentation page.
  2. Find and download the version mapping table.
  3. Query the UltraPath version in the version mapping table.
- In SAN Boot mode, the virtual LUN running the host's operating system must be a common virtual LUN. You can change a common virtual LUN to a HyperMetro virtual LUN only after UltraPath is installed on the host and the host is restarted.
- When NPIV coupled with VIOS is used, the requirements of NPIV on hardware and software must be met.
- When NPIV coupled with VIOS is used, UltraPath must be installed on the client AIX partition.

Step 1 Set the HyperMetro working mode.

You can set the HyperMetro working mode using either of the following methods:

Method 1: Run the **upadm set hypermetro workingmode=auto** command to configure UltraPath to automatically adapt the HyperMetro working mode. This setting enables UltraPath to periodically query the host access mode configured on HyperMetro storage systems and adapt its HyperMetro working mode according to the host access mode.

Method 2: Run the following command to set UltraPath to work in a fixed HyperMetro working mode:

Command	Example
set hypermetro workingmode=*[priority | balance]* **primary_array_id=***ID*	**upadm set hypermetro workingmode=priority primary_array_id=0**

The following table describes the parameters in the command.

Parameter	Description	Default Value
workingmode	HyperMetro working mode. • **priority**: local preferred mode • **balance**: load balancing mode	priority **priority** is recommended. **balance** is applicable when two active-active data centers are in the same equipment room or on the same floor.

Parameter	Description	Default Value
primary_array_id	ID of the preferred storage system. The ID is allocated by UltraPath. Select the storage system that resides in the same data center as the application host. Run the **upadm show array** command to obtain the storage system ID. **NOTE** • In **priority** mode, the value of the parameter indicates the storage system to which I/Os are preferentially delivered. • In **balance** mode, the value of the parameter indicates the storage system where the first slice section resides.	None **NOTE** Mapping relationship between application hosts and storage systems: • Storage system A is the preferred system for all application hosts in data center A. • Storage system B is the preferred system for all application hosts in data center B.

NOTE

If you set UltraPath to automatically adapt the HyperMetro working mode, ensure that the host access mode on the storage system is consistent with that on the physical network.

Step 2 Configure the load balancing policy.

If HyperMetro works in load balancing mode, you can run the **upadm set hypermetro loadbalancemode=***[split-size | round-robin]* command to configure the load balancing policy. The following table describes the parameters in the command.

Parameter	Description	Default Value
loadbalancemode	Load balancing policy for HyperMetro systems. • **split-size**: slicing mode across storage systems. In this mode, UltraPath delivers I/Os to a specific storage system based on the start addresses of I/Os, slice size, and preferred storage system. For example, if the slice size is 128 MB, the I/Os whose start addresses range from 0 to 128 MB (excluding 128 MB) are preferentially delivered to the preferred storage system and the I/Os whose start addresses range from 128 MB to 256 MB (excluding 256 MB) are delivered to the non-preferred storage system. The default slice size is 128 MB. You can run the **upadm set hypermetro split_size** command to change it. • **round-robin**: round-robin mode across storage systems. In this mode, UltraPath selects two storage systems in turn to deliver I/Os.	split-size

----End

7.5.2 Red Hat

7.5.2.1 Storage System Configuration

If UltraPath is used, retain the default settings of the initiator and configure **Host Access Mode** and **Preferred Path for HyperMetro** as required. Table 7-4 lists the detailed settings.

Table 7-4 Storage configurations for interconnection with Red Hat application servers

HyperMetro Working Mode	Storage System	OS Setting	Host Access Mode	Preferred Path for HyperMetro	Description
Load balancing mode	Local storage	Linux	Load balancing	N/A	The host uses all paths of a disk with equal priority.
	Remote storage	Linux	Load balancing	N/A	

HyperMetro Working Mode	Storage System	OS Setting	Host Access Mode	Preferred Path for HyperMetro	Description
Local preferred mode	Local storage	Linux	Asymmetric	Yes	The host considers the paths from the local storage system as preferred paths, and those from the remote storage system as non-preferred paths.
	Remote storage	Linux	Asymmetric	No	

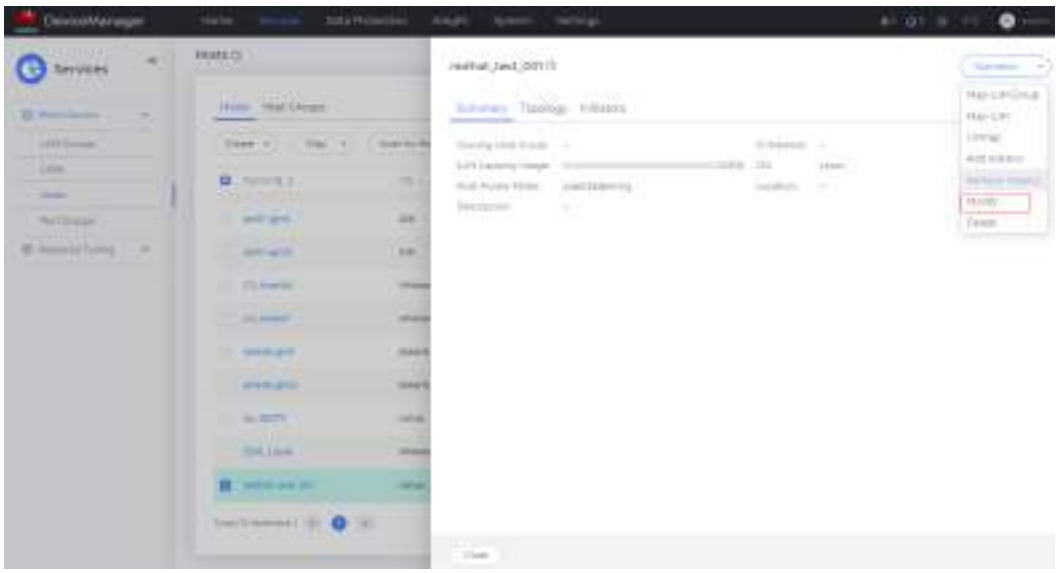
NOTICE

- For details about the Red Hat versions, see the **Huawei Storage Interoperability Navigator**.
- If a LUN has been mapped to a host, you must restart the host for the configuration to take effect after you modify **Host Access Mode** or **Preferred Path for HyperMetro**. If you map the LUN for the first time, restart is not needed.

Configuring the Load Balancing Mode

Step 1 Click the host name and choose **Operation** > **Modify**.

Figure 7-1 Modifying the host properties

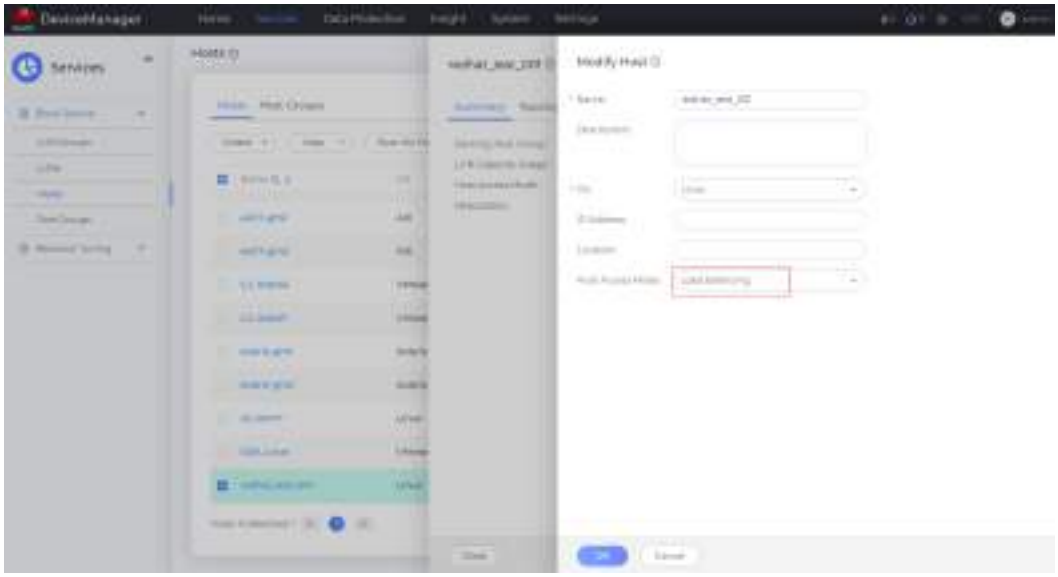


NOTE

The information displayed on the GUI may vary slightly with the product version.

Step 2 Set **Host Access Mode** to **Load balancing** for both the local and remote storage systems.

Figure 7-2 Setting the host access mode

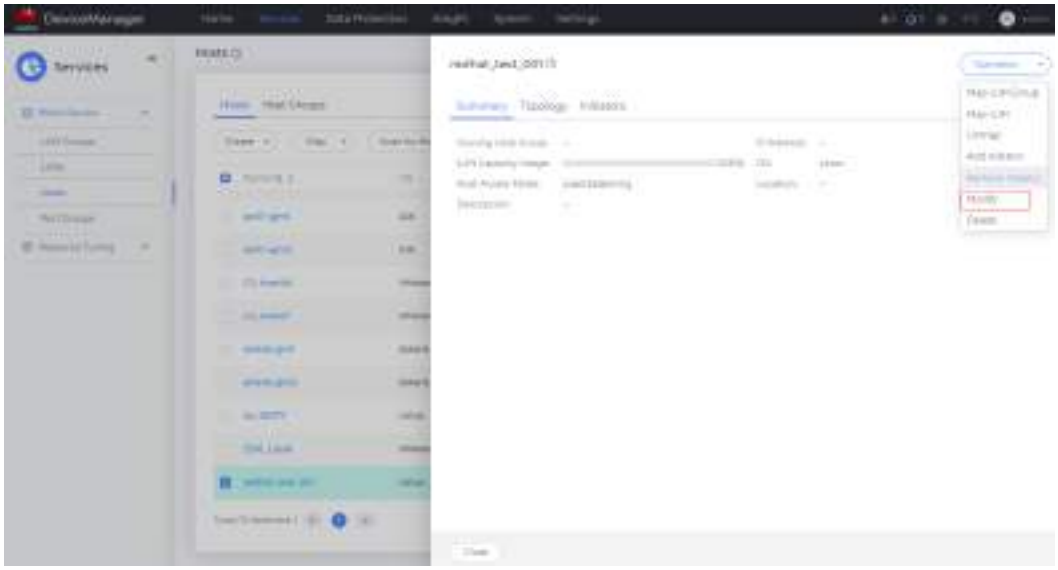


----End

Configuring the Local Preferred Mode

Step 1 Click the host name and choose **Operation** > **Modify**.

Figure 7-3 Modifying the host properties



NOTE

The information displayed on the GUI may vary slightly with the product version.

Step 2 For the local storage system, set **Host Access Mode** to **Asymmetric** and **Preferred Path for HyperMetro** to **Yes**. For the remote storage system, set **Host Access Mode** to **Asymmetric** and **Preferred Path for HyperMetro** to **No**.

Figure 7-4 Settings on the local storage system

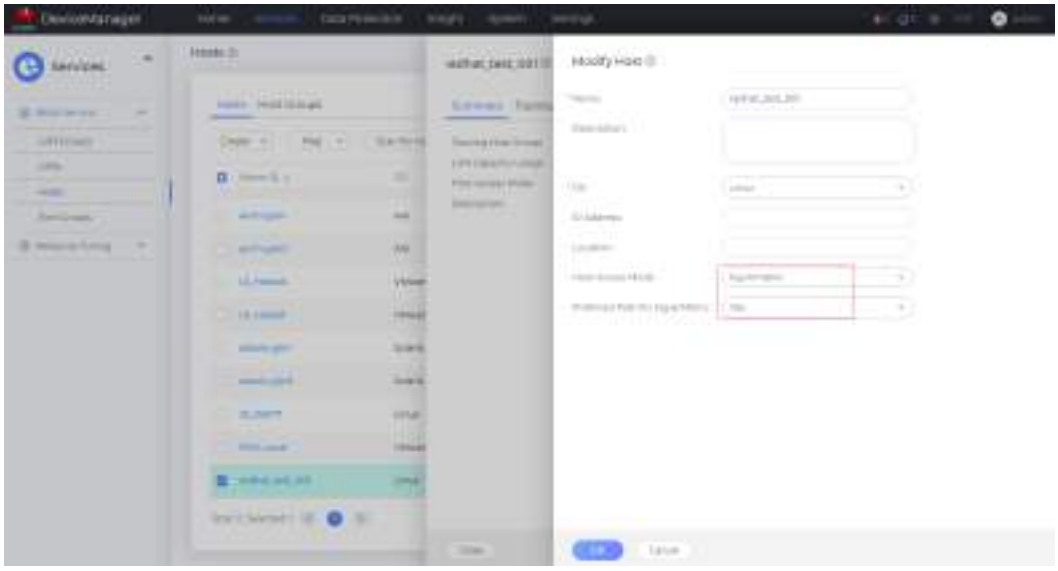
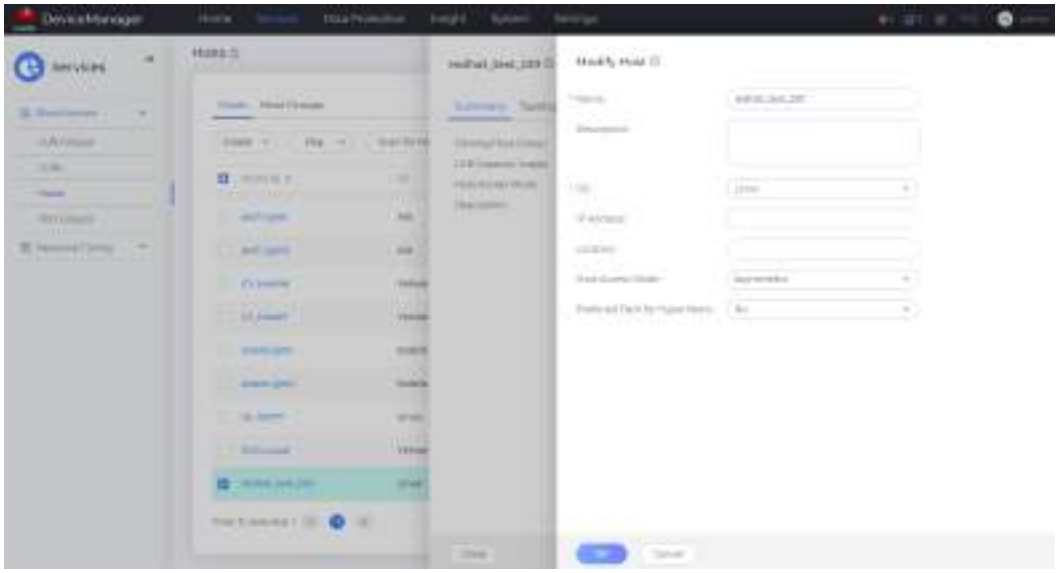


Figure 7-5 Settings on the remote storage system



----End

7.5.2.2 Host Configuration

Install, configure, and use UltraPath by following instructions in the *OceanStor UltraPath for Linux User Guide*.

NOTE

- To obtain the document, log in to Huawei's technical support website (**https://support.huawei.com/enterprise/**), enter **UltraPath** in the search box, and select the associated path to the documentation page. Then find and download the desired document. To download software, click the **Software Download** tab and find the desired software.
- The UltraPath version matches the storage system version. You can query the version information in the version mapping table:
  1. Log in to **https://support.huawei.com/enterprise/**, enter your storage model in the search box, and select the associated path to the product documentation page.
  2. Find and download the version mapping table.
  3. Query the UltraPath version in the version mapping table.

Step 1 Set the HyperMetro working mode.

You can set the HyperMetro working mode using either of the following methods:

Method 1: Run the **upadm set hypermetro workingmode=auto** command to configure UltraPath to automatically adapt the HyperMetro working mode. This setting enables UltraPath to periodically query the host access mode configured on HyperMetro storage systems and adapt its HyperMetro working mode according to the host access mode.

Method 2: Run the following command to set UltraPath to work in a fixed HyperMetro working mode:

Command	Example
set hypermetro workingmode=*[priority | balance]* **primary_array_id=***ID*	**upadm set hypermetro workingmode=priority primary_array_id=0**

The following table describes the parameters in the command.

Parameter	Description	Default Value
workingmode	HyperMetro working mode. • **priority**: local preferred mode • **balance**: load balancing mode	priority **priority** is recommended. **balance** is applicable when two active-active data centers are in the same equipment room or on the same floor.

Parameter	Description	Default Value
primary_array_id	ID of the preferred storage system. The ID is allocated by UltraPath. Select the storage system that resides in the same data center as the application host. Run the **upadm show array** command to obtain the storage system ID. **NOTE** • In **priority** mode, the value of the parameter indicates the storage system to which I/Os are preferentially delivered. • In **balance** mode, the value of the parameter indicates the storage system where the first slice section resides.	None **NOTE** Mapping relationship between application hosts and storage systems: • Storage system A is the preferred system for all application hosts in data center A. • Storage system B is the preferred system for all application hosts in data center B.

NOTE

If you set UltraPath to automatically adapt the HyperMetro working mode, ensure that the host access mode on the storage system is consistent with that on the physical network.

Step 2 Configure the load balancing policy.

If HyperMetro works in load balancing mode, you can run the **upadm set hypermetro loadbalancemode=***[split-size | round-robin]* command to configure the load balancing policy. The following table describes the parameters in the command.

Parameter	Description	Default Value
loadbalancemode	Load balancing policy for HyperMetro systems. • **split-size**: slicing mode across storage systems. In this mode, UltraPath delivers I/Os to a specific storage system based on the start addresses of I/Os, slice size, and preferred storage system. For example, if the slice size is 128 MB, the I/Os whose start addresses range from 0 to 128 MB (excluding 128 MB) are preferentially delivered to the preferred storage system and the I/Os whose start addresses range from 128 MB to 256 MB (excluding 256 MB) are delivered to the non-preferred storage system. The default slice size is 128 MB. You can run the **upadm set hypermetro split_size** command to change it. • **round-robin**: round-robin mode across storage systems. In this mode, UltraPath selects two storage systems in turn to deliver I/Os.	split-size

----End

7.5.3 Solaris

7.5.3.1 Storage System Configuration

If UltraPath is used, retain the default settings of the initiator and configure **Host Access Mode** and **Preferred Path for HyperMetro** as required. Table 7-5 lists the detailed settings.

Table 7-5 Storage configurations for interconnection with Solaris application servers

HyperMetro Working Mode	Storage System	OS Setting	Host Access Mode	Preferred Path for HyperMetro	Description
Load balancing mode	Local storage	Solaris	Asymmetric	Yes	The host uses all paths of a disk with equal priority.
	Remote storage	Solaris	Asymmetric	Yes	

HyperMetro Working Mode	Storage System	OS Setting	Host Access Mode	Preferred Path for HyperMetro	Description
Local preferred mode	Local storage	Solaris	Asymmetric	Yes	The host considers the paths from the local storage system as preferred paths, and those from the remote storage system as non-preferred paths.
	Remote storage	Solaris	Asymmetric	No	

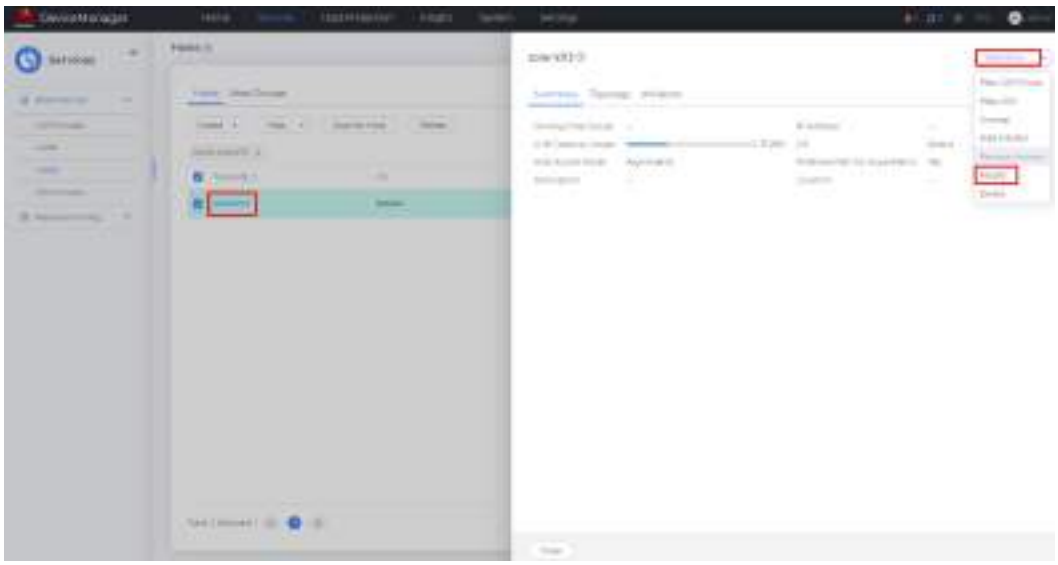
NOTICE

For details about the Solaris versions, see the **Huawei Storage Interoperability Navigator**.

Configuring the Load Balancing Mode

Step 1 Click the host name and choose **Operation** > **Modify**.

Figure 7-6 Modifying the host properties

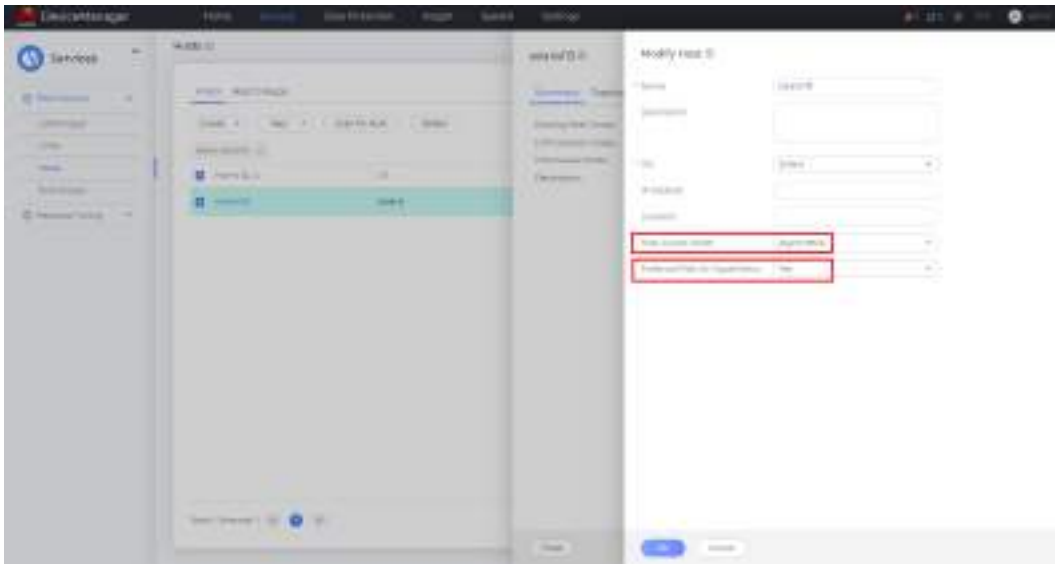


NOTE

The information displayed on the GUI may vary slightly with the product version.

Step 2 Set **Host Access Mode** to **Asymmetric** and **Preferred Path for HyperMetro** to **Yes** for both the local and remote storage systems.

Figure 7-7 Settings on the local and remote storage systems

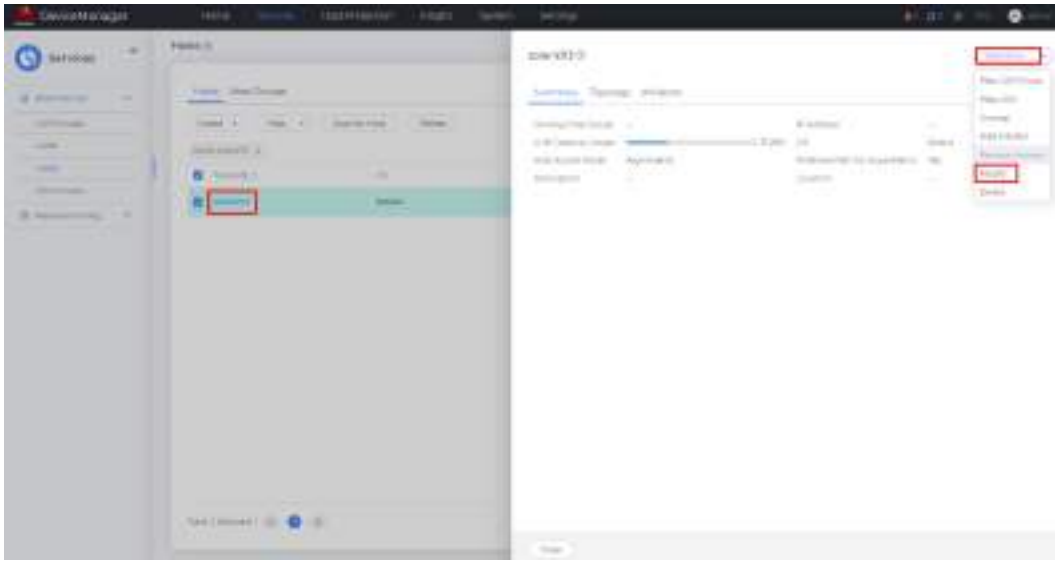


----End

Configuring the Local Preferred Mode

Step 1 Click the host name and choose **Operation** > **Modify**.

Figure 7-8 Modifying the host properties



NOTE

The information displayed on the GUI may vary slightly with the product version.

Step 2 For the local storage system, set **Host Access Mode** to **Asymmetric** and **Preferred Path for HyperMetro** to **Yes**. For the remote storage system, set **Host Access Mode** to **Asymmetric** and **Preferred Path for HyperMetro** to **No**.

Figure 7-9 Settings on the local storage system

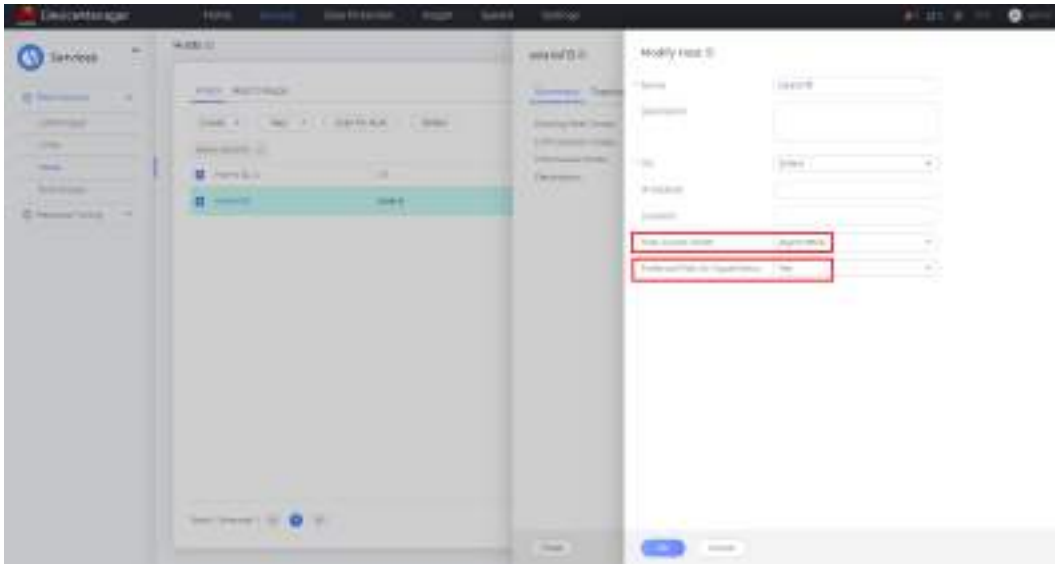
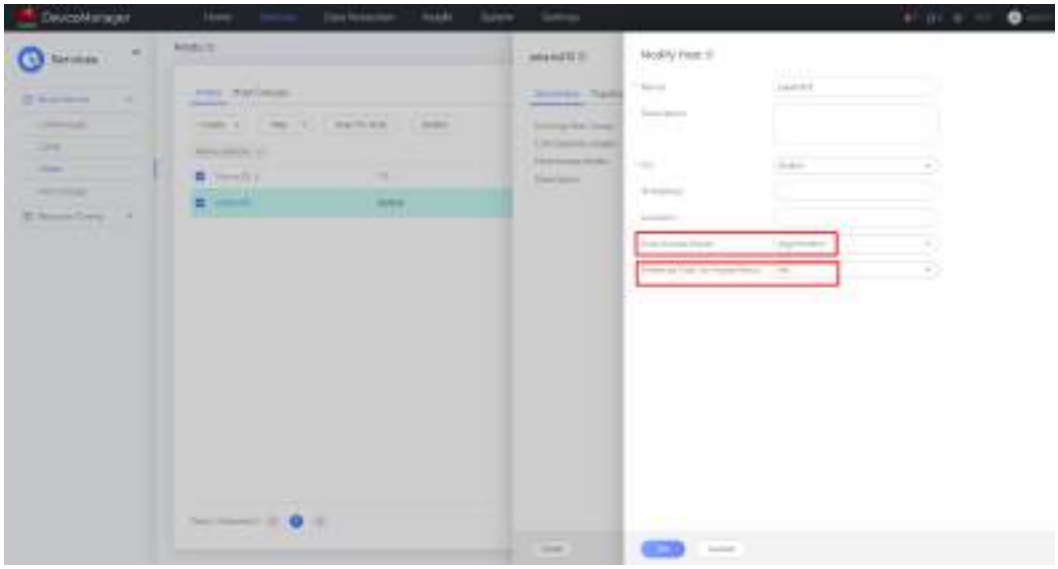


Figure 7-10 Settings on the remote storage system



----End

7.5.3.2 Host Configuration

Install UltraPath by following instructions in the *OceanStor UltraPath for Solaris User Guide*.

NOTE

- To obtain the document, log in to Huawei's technical support website (**https://support.huawei.com/enterprise/**), enter **UltraPath** in the search box, and select the associated path to the documentation page. Then find and download the desired document. To download software, click the **Software Download** tab and find the desired software.
- The UltraPath version matches the storage system version. You can query the version information in the version mapping table:
  1. Log in to **https://support.huawei.com/enterprise/**, enter your storage model in the search box, and select the associated path to the product documentation page.
  2. Find and download the version mapping table.
  3. Query the UltraPath version in the version mapping table.

Step 1 Set the HyperMetro working mode.

You can set the HyperMetro working mode using either of the following methods:

Method 1: Run the **upadm set hypermetro workingmode=auto** command to configure UltraPath to automatically adapt the HyperMetro working mode. This setting enables UltraPath to periodically query the host access mode configured on HyperMetro storage systems and adapt its HyperMetro working mode according to the host access mode.

Method 2: Run the following command to set UltraPath to work in a fixed HyperMetro working mode:

Command	Example
set hypermetro workingmode=*[priority | balance]* **primary_array_id=***ID*	**upadm set hypermetro workingmode=priority primary_array_id=0**

The following table describes the parameters in the command.

Parameter	Description	Default Value
workingmode	HyperMetro working mode. • **priority**: local preferred mode • **balance**: load balancing mode	priority **priority** is recommended. **balance** is applicable when two active-active data centers are in the same equipment room or on the same floor.

Parameter	Description	Default Value
primary_array_id	ID of the preferred storage system. The ID is allocated by UltraPath. Select the storage system that resides in the same data center as the application host. Run the **upadm show array** command to obtain the storage system ID. **NOTE** • In **priority** mode, the value of the parameter indicates the storage system to which I/Os are preferentially delivered. • In **balance** mode, the value of the parameter indicates the storage system where the first slice section resides.	None **NOTE** Mapping relationship between application hosts and storage systems: • Storage system A is the preferred system for all application hosts in data center A. • Storage system B is the preferred system for all application hosts in data center B.

NOTE

If you set UltraPath to automatically adapt the HyperMetro working mode, ensure that the host access mode on the storage system is consistent with that on the physical network.

Step 2 Configure the load balancing policy.

If HyperMetro works in load balancing mode, you can run the **upadm set hypermetro loadbalancemode=***[split-size | round-robin]* command to configure the load balancing policy. The following table describes the parameters in the command.

Parameter	Description	Default Value
loadbalancemode	Load balancing policy for HyperMetro systems. • **split-size**: slicing mode across storage systems. In this mode, UltraPath delivers I/Os to a specific storage system based on the start addresses of I/Os, slice size, and preferred storage system. For example, if the slice size is 128 MB, the I/Os whose start addresses range from 0 to 128 MB (excluding 128 MB) are preferentially delivered to the preferred storage system and the I/Os whose start addresses range from 128 MB to 256 MB (excluding 256 MB) are delivered to the non-preferred storage system. The default slice size is 128 MB. You can run the **upadm set hypermetro split_size** command to change it. • **round-robin**: round-robin mode across storage systems. In this mode, UltraPath selects two storage systems in turn to deliver I/Os.	split-size

----End

7.5.4 SUSE

7.5.4.1 Storage System Configuration

If UltraPath is used, retain the default settings of the initiator and configure **Host Access Mode** and **Preferred Path for HyperMetro** as required. Table 7-6 lists the detailed settings.

Table 7-6 Storage configurations for interconnection with SUSE application servers

HyperMetro Working Mode	Storage System	OS Setting	Host Access Mode	Preferred Path for HyperMetro	Description
Load balancing mode	Local storage	Linux	Load balancing	N/A	The host uses all paths of a disk with equal priority.
	Remote storage	Linux	Load balancing	N/A	

HyperMetro Working Mode	Storage System	OS Setting	Host Access Mode	Preferred Path for HyperMetro	Description
Local preferred mode	Local storage	Linux	Asymmetric	Yes	The host considers the paths from the local storage system as preferred paths, and those from the remote storage system as non-preferred paths.
	Remote storage	Linux	Asymmetric	No	

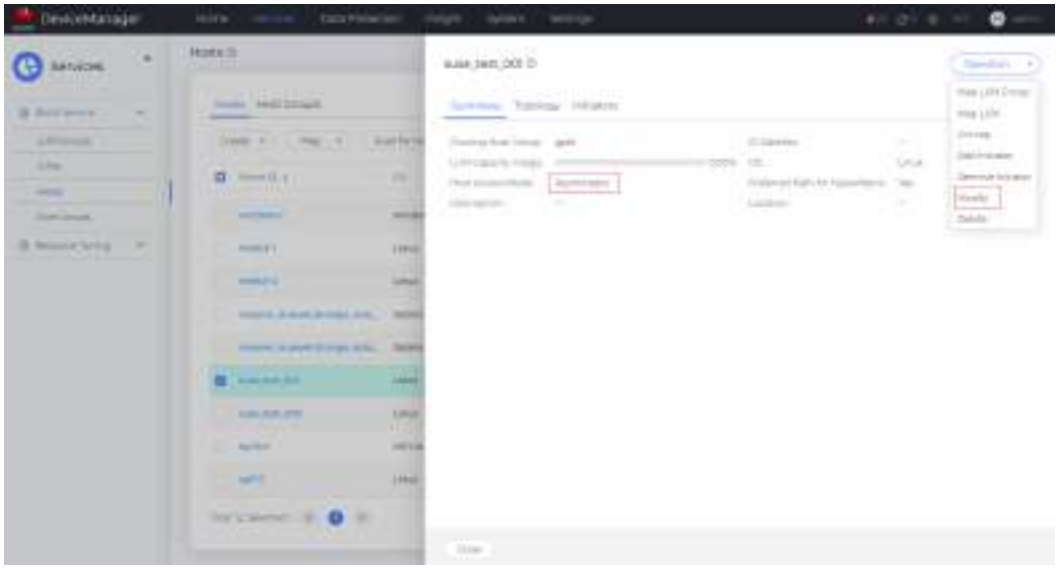
NOTE

For details about the SUSE versions, see the **Huawei Storage Interoperability Navigator**.

Configuring the Load Balancing Mode

Step 1 Click the host name and choose **Operation** > **Modify**.

Figure 7-11 Modifying the host properties

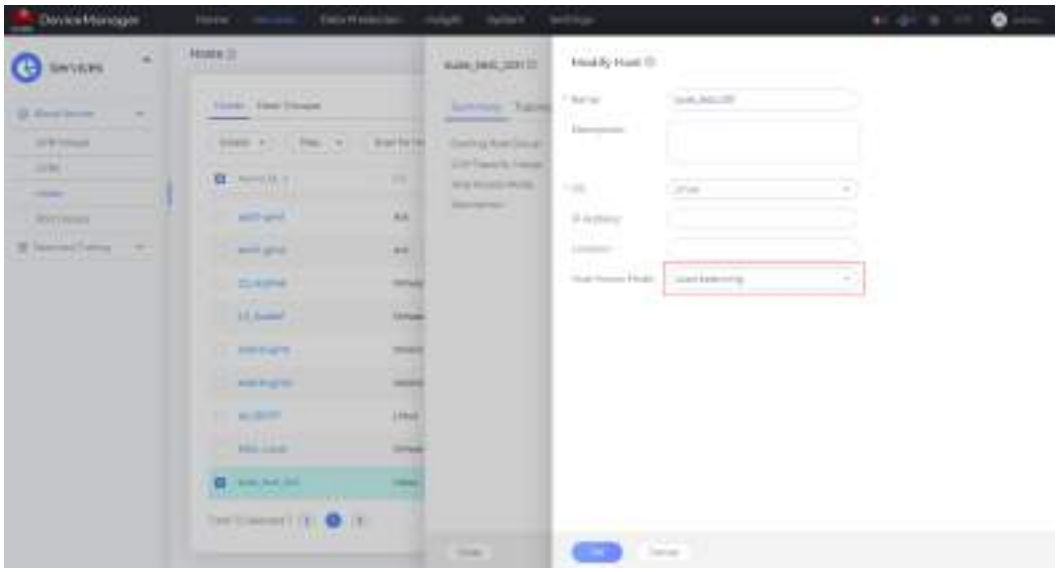


NOTE

The information displayed on the GUI may vary slightly with the product version.

Step 2 Set **Host Access Mode** to **Load balancing** for both the local and remote storage systems.

Figure 7-12 Setting the host access mode

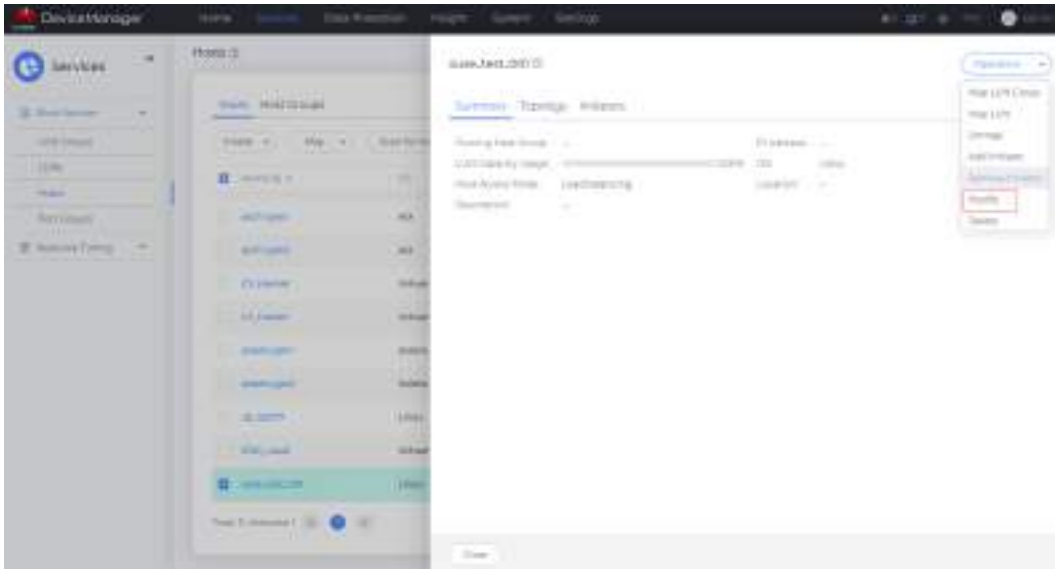


----End

Configuring the Local Preferred Mode

Step 1 Click the host name and choose **Operation** > **Modify**.

Figure 7-13 Modifying the host properties



NOTE

The information displayed on the GUI may vary slightly with the product version.

Step 2 For the local storage system, set **Host Access Mode** to **Asymmetric** and **Preferred Path for HyperMetro** to **Yes**. For the remote storage system, set **Host Access Mode** to **Asymmetric** and **Preferred Path for HyperMetro** to **No**.

Figure 7-14 Settings on the local storage system

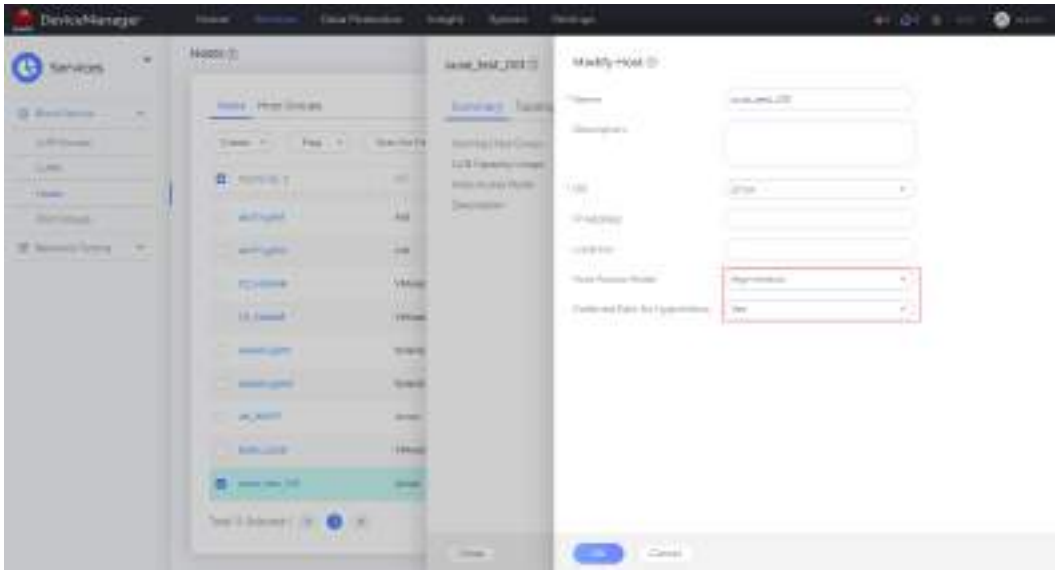
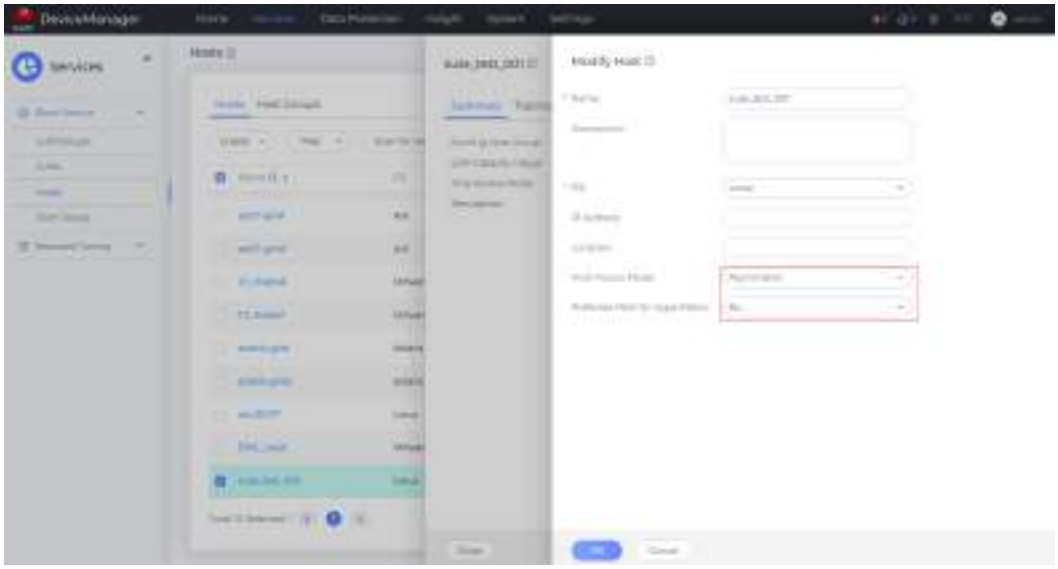


Figure 7-15 Settings on the remote storage system



----End

7.5.4.2 Host Configuration

Install, configure, and use UltraPath by following instructions in the *OceanStor UltraPath for Linux User Guide*.

NOTE

- To obtain the document, log in to Huawei's technical support website (**https://support.huawei.com/enterprise/**), enter **UltraPath** in the search box, and select the associated path to the documentation page. Then find and download the desired document. To download software, click the **Software Download** tab and find the desired software.
- The UltraPath version matches the storage system version. You can query the version information in the version mapping table:
  1. Log in to **https://support.huawei.com/enterprise/**, enter your storage model in the search box, and select the associated path to the product documentation page.
  2. Find and download the version mapping table.
  3. Query the UltraPath version in the version mapping table.

Step 1 Set the HyperMetro working mode.

You can set the HyperMetro working mode using either of the following methods:

Method 1: Run the **upadm set hypermetro workingmode=auto** command to configure UltraPath to automatically adapt the HyperMetro working mode. This setting enables UltraPath to periodically query the host access mode configured on HyperMetro storage systems and adapt its HyperMetro working mode according to the host access mode.

Method 2: Run the following command to set UltraPath to work in a fixed HyperMetro working mode:

Command	Example
set hypermetro workingmode=*[priority | balance]* **primary_array_id=***ID*	**upadm set hypermetro workingmode=priority primary_array_id=0**

The following table describes the parameters in the command.

Parameter	Description	Default Value
workingmode	HyperMetro working mode. • **priority**: local preferred mode • **balance**: load balancing mode	priority **priority** is recommended. **balance** is applicable when two active-active data centers are in the same equipment room or on the same floor.

Parameter	Description	Default Value
primary_array_id	ID of the preferred storage system. The ID is allocated by UltraPath. Select the storage system that resides in the same data center as the application host. Run the **upadm show array** command to obtain the storage system ID. **NOTE** • In **priority** mode, the value of the parameter indicates the storage system to which I/Os are preferentially delivered. • In **balance** mode, the value of the parameter indicates the storage system where the first slice section resides.	None **NOTE** Mapping relationship between application hosts and storage systems: • Storage system A is the preferred system for all application hosts in data center A. • Storage system B is the preferred system for all application hosts in data center B.

NOTE

If you set UltraPath to automatically adapt the HyperMetro working mode, ensure that the host access mode on the storage system is consistent with that on the physical network.

Step 2 Configure the load balancing policy.

If HyperMetro works in load balancing mode, you can run the **upadm set hypermetro loadbalancemode=***[split-size | round-robin]* command to configure the load balancing policy. The following table describes the parameters in the command.

Parameter	Description	Default Value
loadbalancemode	Load balancing policy for HyperMetro systems. • **split-size**: slicing mode across storage systems. In this mode, UltraPath delivers I/Os to a specific storage system based on the start addresses of I/Os, slice size, and preferred storage system. For example, if the slice size is 128 MB, the I/Os whose start addresses range from 0 to 128 MB (excluding 128 MB) are preferentially delivered to the preferred storage system and the I/Os whose start addresses range from 128 MB to 256 MB (excluding 256 MB) are delivered to the non-preferred storage system. The default slice size is 128 MB. You can run the **upadm set hypermetro split_size** command to change it. • **round-robin**: round-robin mode across storage systems. In this mode, UltraPath selects two storage systems in turn to deliver I/Os.	split-size

----End

7.5.5 VMware ESXi

7.5.5.1 Storage System Configuration

This section provides recommended configurations on HyperMetro storage systems for interconnection with VMware ESXi hosts.

Table 7-7 Recommended configurations on 6.x series storage systems

HyperMetro Working Mode	Storage System	OS Setting	Host Access Mode	Preferred Path for HyperMetro	Description
Load balancing mode	Local storage	VMware ESXi	Load balancing	N/A	The host uses all paths of a disk with equal priority.
	Remote storage	VMware ESXi	Load balancing	N/A	

HyperMetro Working Mode	Storage System	OS Setting	Host Access Mode	Preferred Path for HyperMetro	Description
Local preferred mode	Local storage	VMware ESXi	Asymmetric	Yes	The host considers the paths from the local storage system as preferred paths, and those from the remote storage system as non-preferred paths.
	Remote storage	VMware ESXi	Asymmetric	No	

NOTICE

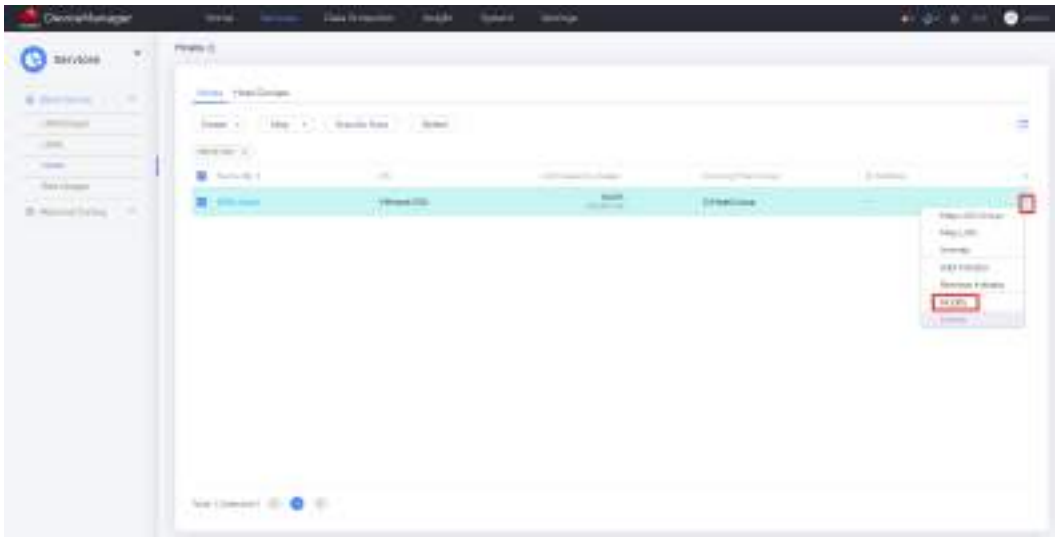
- Use the recommended configurations in **Table 7-7**. Other configurations may cause problems.
- If a LUN has been mapped to a host, you must restart the host for the configuration to take effect after you modify **Host Access Mode**. If you map the LUN for the first time, restart is not needed.
- When a LUN of a HyperMetro pair is mapped to all ESXi hosts in a cluster, the LUN must have the same host LUN ID on all of the hosts. You are advised to add all ESXi hosts in a cluster that are served by the same storage device to a host group and to the same mapping.

Configuring the Load Balancing Mode

Perform the following operations to configure the load balancing mode:

Step 1 On DeviceManager, choose **Services** > **Hosts**. Select the desired host, click ⋮ on the right, and choose **Modify**.

Figure 7-16 Modifying the host properties

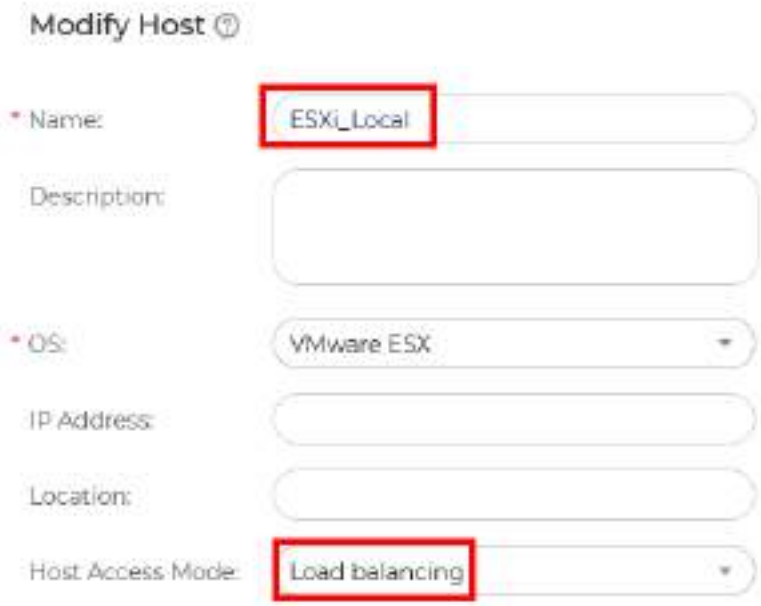


NOTE

- The information displayed on the GUI may vary slightly with the product version.

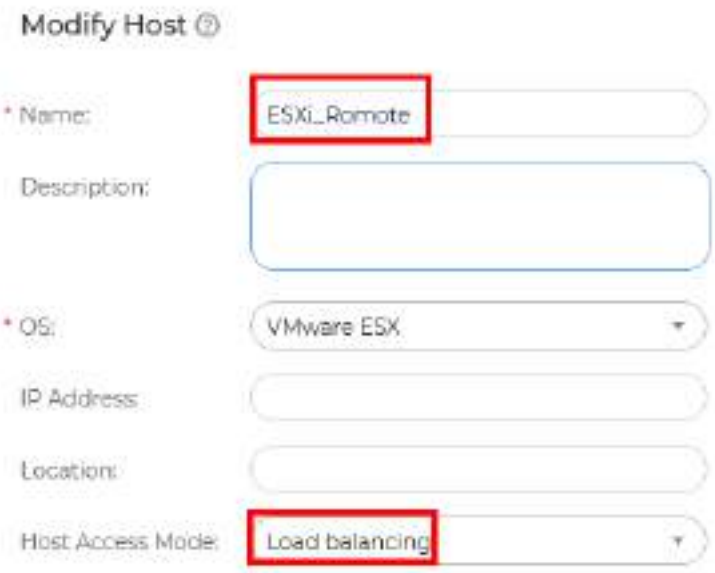
Step 2 On the **Modify Host** page, set **Host Access Mode** to **Load balancing**.

Figure 7-17 Settings on the local storage system



Step 3 Repeat the preceding steps to set **Host Access Mode** of the remote storage system to **Load balancing**.

Figure 7-18 Settings on the remote storage system



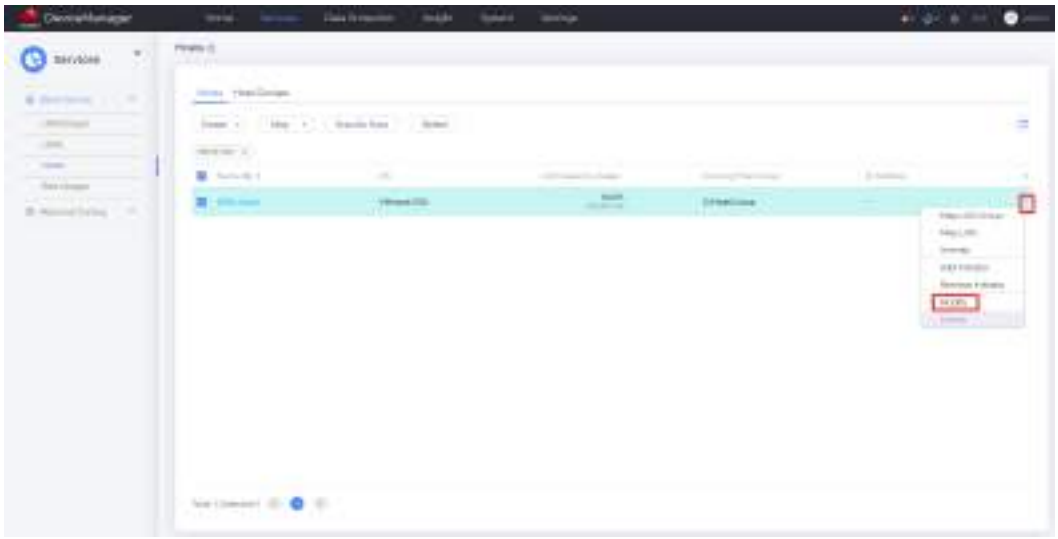
----End

Configuring the Local Preferred Mode

Perform the following operations to configure the local preferred mode:

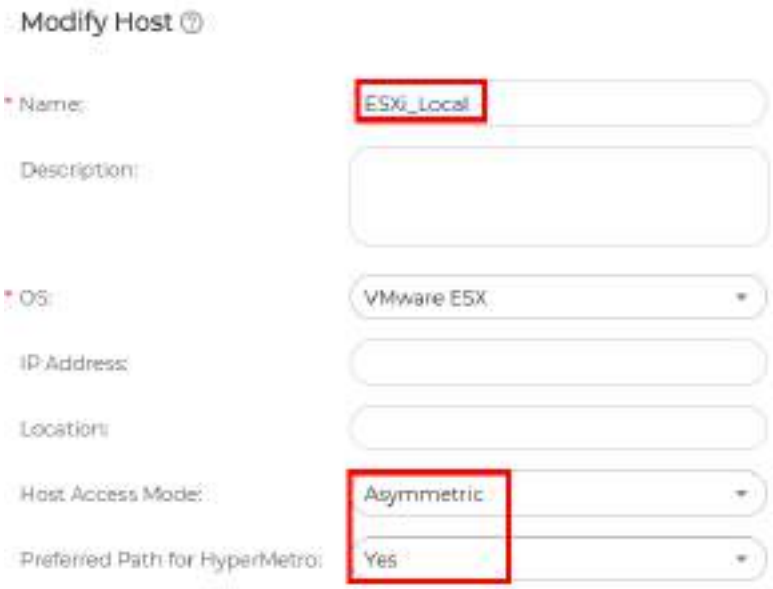
Step 1 On DeviceManager, choose **Services** > **Hosts**. Select the desired host, click ⋮ on the right, and choose **Modify**, as shown in.

Figure 7-19 Modifying the host properties



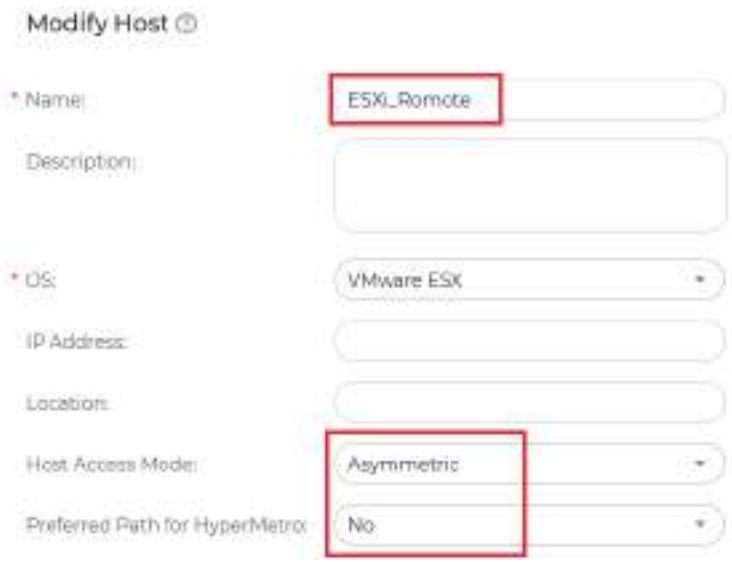
Step 2 For the local storage system, set **Host Access Mode** to **Asymmetric** and **Preferred Path for HyperMetro** to **Yes**.

Figure 7-20 Settings on the local storage system



Step 3 For the remote storage system, set **Host Access Mode** to **Asymmetric** and **Preferred Path for HyperMetro** to **No**.

Figure 7-21 Settings on the remote storage system



----End

NOTE

For details about the VMware ESXi versions, see the **Huawei Storage Interoperability Navigator**.

7.5.5.2 Host Configuration

Install UltraPath by following instructions in the *OceanStor UltraPath for vSphere User Guide*.

Context

This configuration must be performed separately on all hosts.

NOTE

UltraPath 21.3.0 and earlier versions support Secure Boot on servers.

Prerequisites

VMware has the following requirements on storage LUN IDs:

- All path LUN IDs of a LUN are consistent for a host.
- All host LUN IDs of a LUN shared by multiple hosts are consistent across these hosts. For details, see **Setting LUN Allocations** at the VMware office site.

If LUN IDs do not meet the preceding requirements, correct them by referring to "ID Description" in the ***Host Connectivity Guide***.

Configuring UltraPath

Step 1 Set the HyperMetro working mode.

Use either of the following methods to set the HyperMetro working mode for UltraPath:

Method 1: Run the **esxcli upadm set hypermetro workingmode -m auto** command to configure UltraPath to automatically adapt the HyperMetro working mode. This setting enables UltraPath to periodically query the host access mode configured on HyperMetro storage systems and adapt its HyperMetro working mode according to the host access mode.

Method 2: Run the following command to set UltraPath to work in a fixed HyperMetro working mode:

Table 7-8 Command for setting the HyperMetro working mode for UltraPath

Command	Example
set hypermetro workingmode -m *[priority | balance]* **-p** *primary_array_id*	**esxcli upadm set hypermetro workingmode -m priority -p 0**
NOTE In VMware vSphere, adding **esxcli upadm** in front of a command navigates the user to the UltraPath CLI.	

Table 7-9 describes the command parameters.

Table 7-9 Parameter description

Parameter	Description	Default Value
-m *mode*	HyperMetro working mode. • **priority**: local preferred mode • **balance**: load balancing mode	**priority** **priority** is recommended. **balance** is applicable when two active-active data centers are in the same building.

Parameter	Description	Default Value
-p *primary_array_id*	ID of the preferred storage array. The ID is allocated by UltraPath. The storage array that is in the same data center as the application hosts reside is preferred. Run the **esxcli upadm show diskarray** command to obtain the storage array ID. **NOTE** • In **priority** mode, this parameter indicates the storage array to which I/Os are preferentially delivered. • In **balance** mode, this parameter indicates the storage array where the first slice section resides.	None **NOTE** Mapping relationship between application hosts and storage arrays: • Storage array A is the preferred array for all application hosts in data center A. • Storage array B is the preferred array for all application hosts in data center B.

NOTICE

If you set UltraPath to automatically adapt the HyperMetro working mode, ensure that the host access mode on the storage system is consistent with that on the physical network.

Step 2 Configure the load balancing policy.

If HyperMetro works in load balancing mode, you can run the **esxcli upadm set hypermetro loadbalancemode –m** *[split-size | round-robin]* command to configure the load balancing policy. The following table describes the parameters in the command.

Parameter	Description	Default Value
-m *mode*	Load balancing policy for HyperMetro systems. • **split-size**: slicing mode across storage systems. In this mode, UltraPath delivers I/Os to a specific storage system based on the start addresses of I/Os, slice size, and preferred storage system. For example, if the slice size is 128 MB, the I/Os whose start addresses range from 0 to 128 MB (excluding 128 MB) are preferentially delivered to the preferred storage system and the I/Os whose start addresses range from 128 MB to 256 MB (excluding 256 MB) are delivered to the non-preferred storage system. The default slice size is 128 MB. You can run the **esxcli upadm set hypermetro split_size** command to change it. • **round-robin**: round-robin mode across storage systems. In this mode, UltraPath selects two storage systems in turn to deliver I/Os.	split-size

Step 3 Set timeout parameters.

FC networking does not require setting of timeout parameters.

For iSCSI networking, perform the following operations on ESXi hosts. You must restart the host for the configuration to take effect. Exercise caution when performing this operation.

1. Obtain the iSCSI adapter name.
```
[root@esxi16113:~] esxcfg-scsidevs -a | grep -i iscsi
vmhba35 iscsi_vmk        online    iqn.XXXX-XX.com.vmware:esxi16113-xxxxxxxxxSCSI Software Adapte
```
   In the command output, the iSCSI adapter name is **vmhba35**.
2. Query the current timeout parameter settings.
```
[root@esxi16113:~] esxcli iscsi adapter param get -A vmhba35 | egrep 'NoopOutInterval|
NoopOutTimeout|RecoveryTimeout'
NoopOutInterval       15          15          1    60           true    false
NoopOutTimeout        10          10          10   30           true    false
RecoveryTimeout       10          10          1    120          true    false
```
3. Set the timeout parameters.
```
esxcli iscsi adapter param set -A vmhba35 -k NoopOutInterval -v 1
esxcli iscsi adapter param set -A vmhba35 -k NoopOutTimeout -v 10
esxcli iscsi adapter param set -A vmhba35 -k RecoveryTimeout -v 1
```


NOTE

- All the preceding commands are available only in VMware ESXi 5.5, 6.0, 6.5, and 6.7. For details on the VMware versions supported in HyperMetro, see the **Huawei Storage Interoperability Navigator**.
- The information in bold is the iSCSI adapter. Change it based on the site requirements. (Run the **esxcfg-scsidevs -a** command to query the iSCSI adapter.)
- You must restart the host for the configuration to take effect.
- The settings shorten the path switchover time to about 16s. In comparison, the default ESXi settings may result in an up-to-25s path switchover time.

4. Verify the modification.

```
[root@esxi16113:~] esxcli iscsi adapter param get -A vmhba35 | egrep 'NoopOutInterval|
NoopOutTimeout|RecoveryTimeout'
NoopOutInterval       1          15         1    60          true    false
NoopOutTimeout        10          10          10   30           true    false
RecoveryTimeout       1          10         1    120          true    false
```

----End

Configuring a VMware Cluster

Table 7-10 Cluster configuration when UltraPath is used

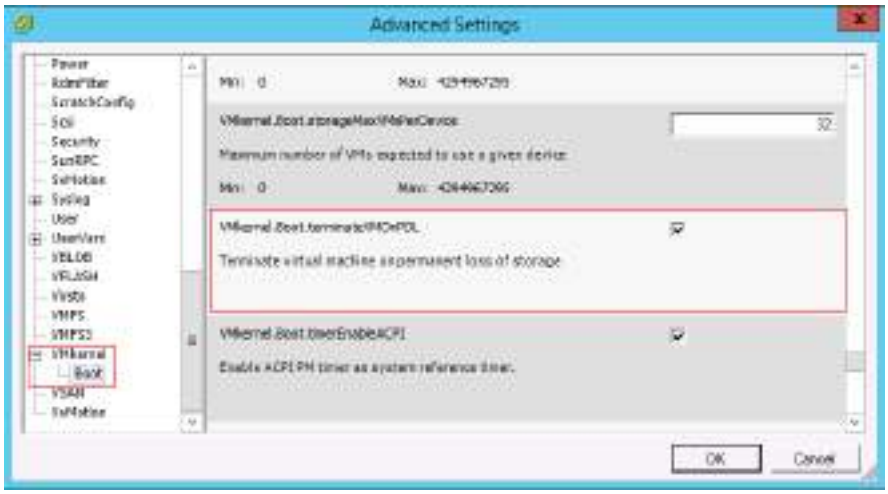
VMware vSphere ESXi Version	Host Parameter		Cluster Parameter (VM Policy for APD and PDL)	Remarks
5.0 U1 5.1	Log in to each ESXi host using SSH, open the **/etc/vmware/settings** file, and add **Disk.terminateVMOnPDL-Default = True** to the file.		Use the vSphere Client to log in to each ESXi host. In the advanced settings, set **das.maskCleanShutdownEnabled = True**.	After configuring host parameters, restart the host for the configuration to take effect.
5.5.*	VMkernel.Boot.terminateVMOnPDL=True	Disk.AutoremoveOnPDL=0	Select **Turn on vSphere HA**.	After configuring an ESXi 5.5.* host, you must restart the host for the configuration to take effect. After configuring cluster parameters, re-enable HA for the configuration to take effect.

VMware vSphere ESXi Version	Host Parameter		Cluster Parameter (VM Policy for APD and PDL)	Remarks
6.0 GA 6.0 U1				After configuring an ESXi 6.0 GA or ESXi 6.0 U1 host, you do not need to restart the host because the parameters take effect immediately. After configuring cluster parameters, re-enable HA for the configuration to take effect.
6.0 U2 6.0 U3 6.5.* 6.7.*	VMkernel.Boot.terminateVMOnPDL=False (Retain the default value.)	Disk.AutoremoveOnPDL=1 (Retain the default value.)	1. Select **Turn on vSphere HA**. 2. Set **Datastore with PDL** to **Power off and restart VMs**. 3. Set **Datastore with APD** to **Power off and restart VMs - Aggressive restart policy**.	Retain the default host parameter settings. You only need to enable HA again in vCenter for the settings to take effect. On a parallel network, set **Datastore with PDL** and **Datastore with APD** to **Power off and restart VMs** to ensure that VMs can be switched to the peer end in the case of a single point of failure. On a standard network, this setting is optional and you can determine whether to use this setting based on site requirements.

- A VM service network requires L2 interworking between data centers so that VM migration between data centers will not affect VM services.
- For VMware vSphere 5.0 u1, later 5.0 versions, and vSphere 5.1:
  - Cluster parameter configuration: Use the vSphere Client to log in to each ESXi host. In the advanced settings, set **das.maskCleanShutdownEnabled = True**.
  - Host parameter configuration: Log in to each ESXi host using SSH and add **Disk.terminateVMOnPDLDefault = True** to the **/etc/vmware/settings** file. After configuring host parameters, restart the host for the configuration to take effect.
- For VMware vSphere 5.5.*, 6.0 u1, and versions between them:
  - Cluster parameter configuration: Use vSphere Web Client to connect to vCenter, go to the cluster HA configuration page, and select **Turn on vSphere HA**. After configuring cluster parameters, re-enable HA for the configuration to take effect.
  - Host parameter configuration: Log in to each ESXi host using vSphere Client or vCenter and complete the following advanced settings.

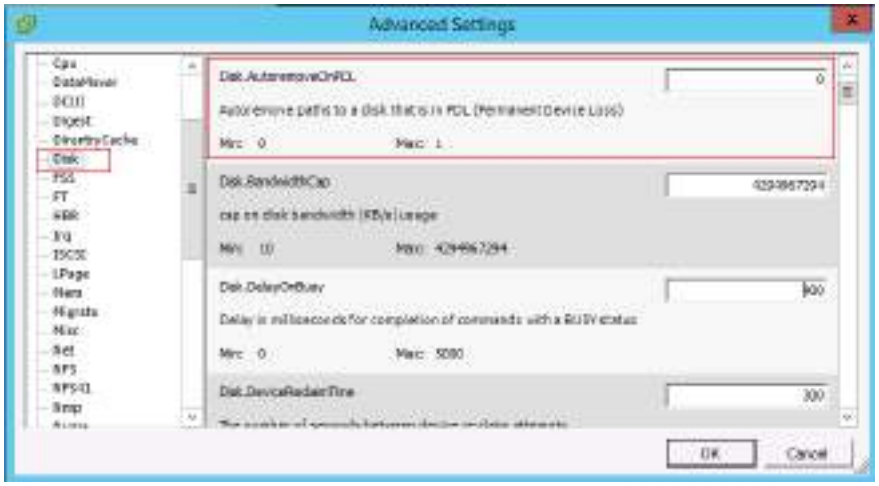
    Set **VMkernel.Boot.terminateVMOnPDL = True**. The parameter forcibly powers off VMs on a datastore when the datastore enters the PDL state.

    Figure 7-22 Boot parameter settings

    Set **Disk.AutoremoveOnPDL = 0**. This setting ensures that datastores in the PDL state will not be automatically removed.

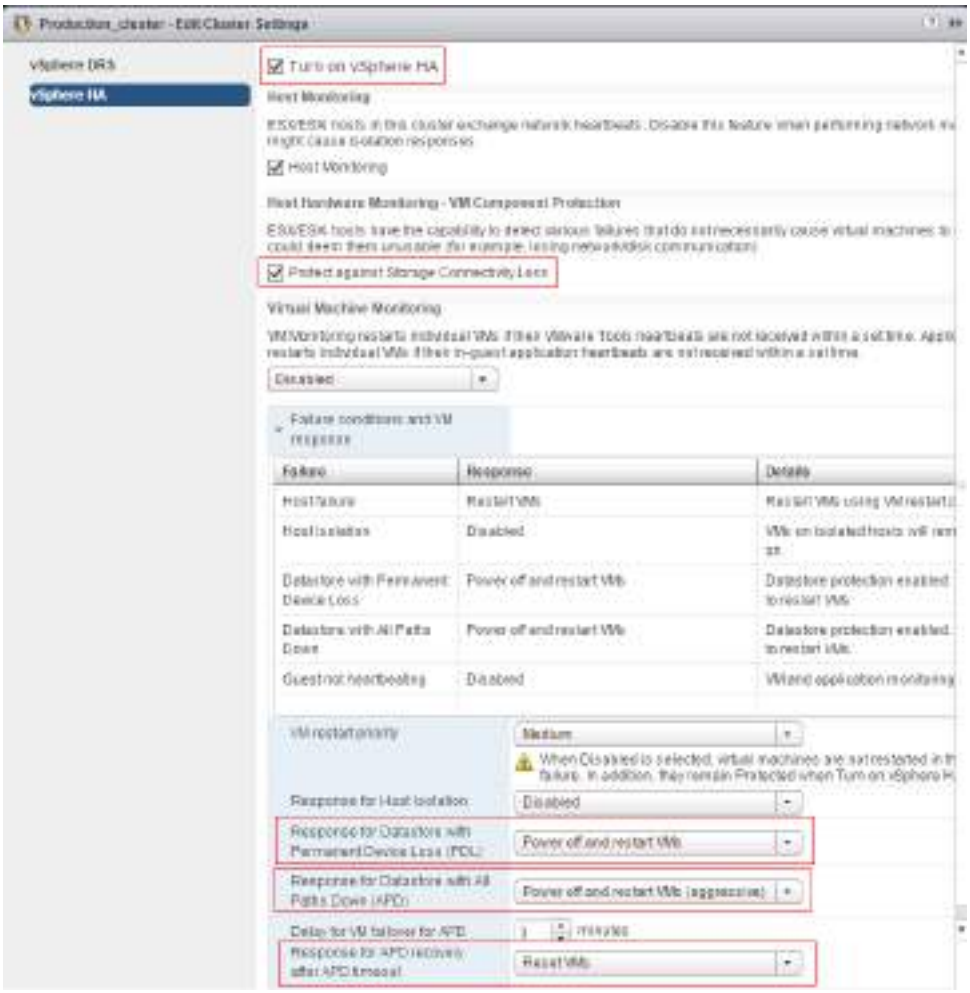
Figure 7-23 Disk parameter settings



- For VMware vSphere 6.0 u2 and later updates:

  After connecting to vCenter through the vSphere Web Client, enter the cluster HA configuration and set the parameters as follows.

Figure 7-24 vSphere 6.0 cluster configuration



- For VMware vSphere 6.5:

After connecting to vCenter through the vSphere Web Client, enter the cluster HA configuration and set the parameters as follows.

Figure 7-25 vSphere 6.5 cluster configuration-1

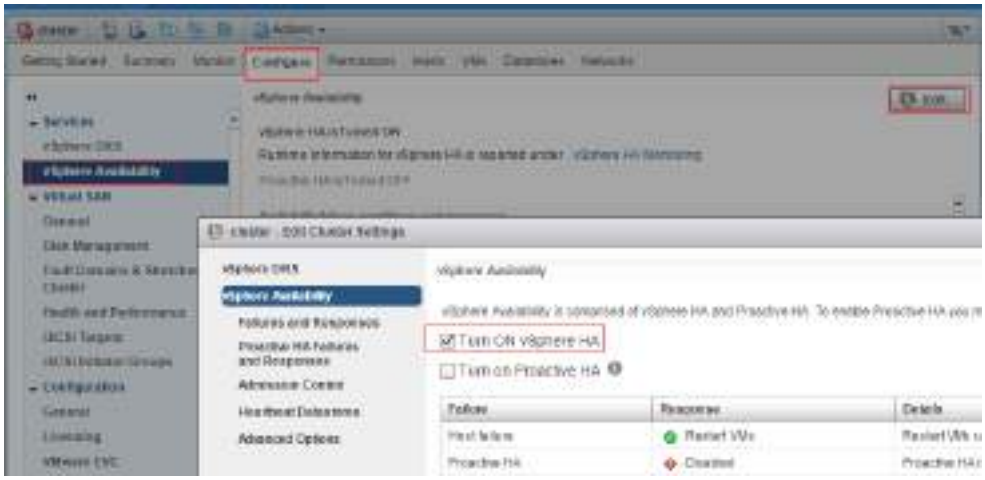
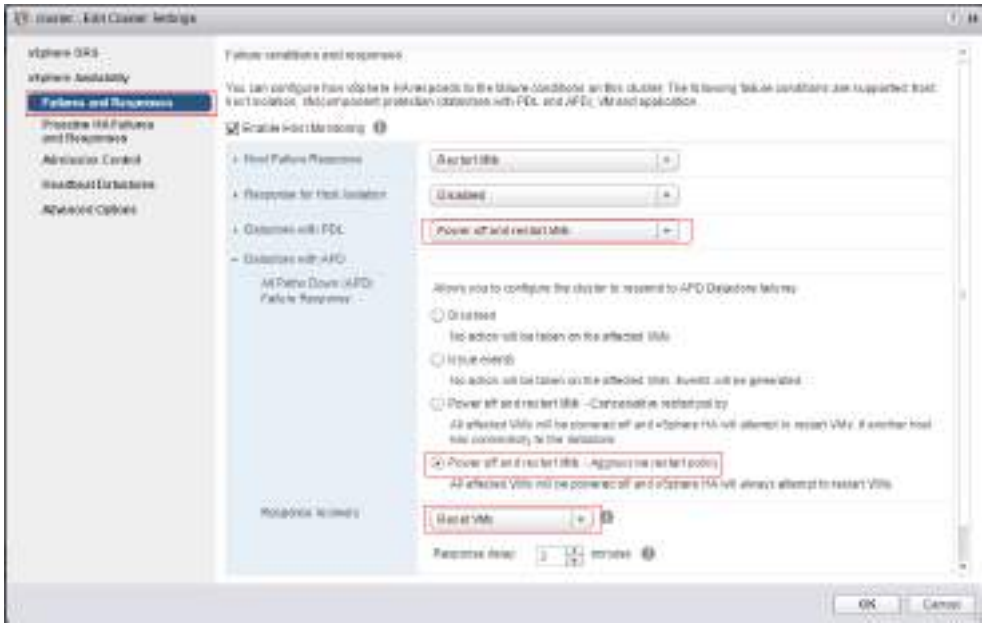


Figure 7-26 vSphere 6.5 cluster configuration-2

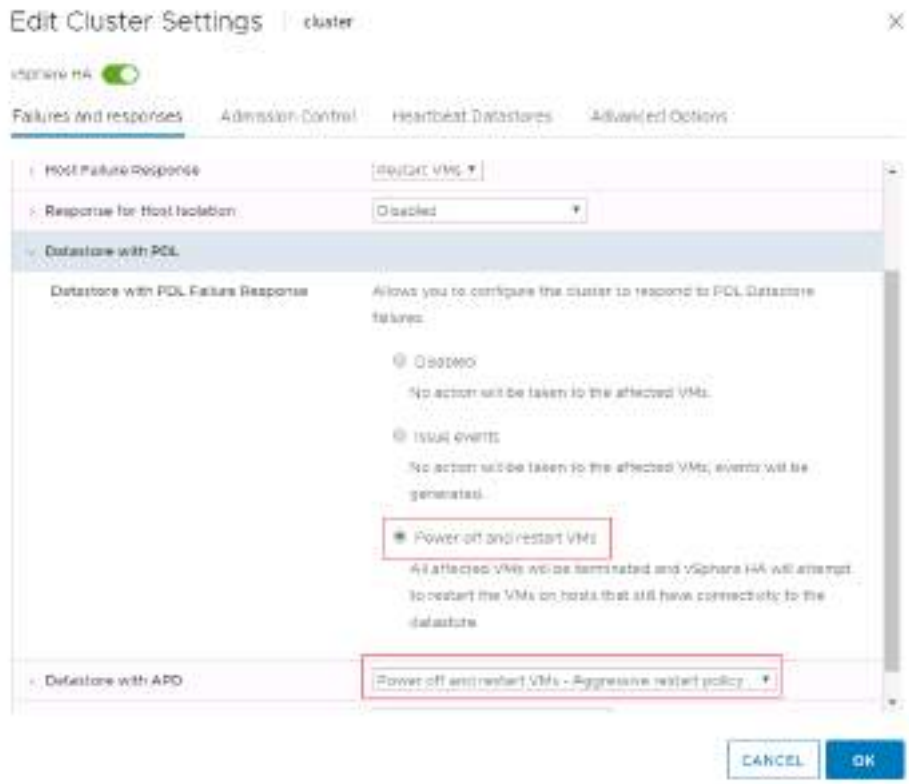


- For VMware vSphere 6.7 and later updates:

  After connecting to vCenter through the vSphere Web Client, enter the cluster HA configuration and set the parameters as follows.

Figure 7-27 vSphere 6.7 cluster configuration-1

Figure 7-28 vSphere 6.7 cluster configuration-2



Recommended configuration items:

- Configure the vMotion, service, and management networks with different VLAN IDs to prevent network interference.
- Configure the management network to include the vCenter Server management node and ESXi hosts. Deny access from external applications.
- Divide the service network into VLANs to ensure logical isolation and control broadcast domains.
- Configure a DRS group to ensure that VMs can be recovered first in the local data center in the event of the breakdown of a single host.

7.5.5.3 Verification

In VMware vSphere, run the **esxcli upadm show upconfig** command.

NOTE

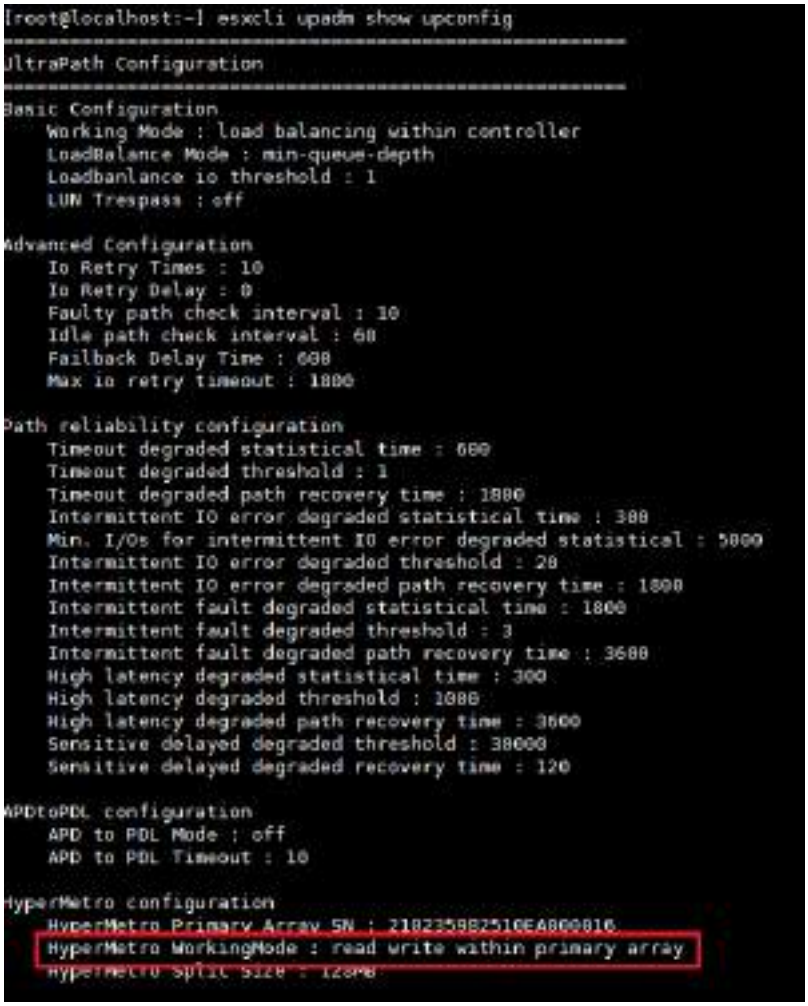
In VMware vSphere, adding **esxcli upadm** in front of a command navigates the user to the UltraPath CLI.

If the command output contains the following information, the configuration is successful.

```
HyperMetro WorkingMode : read write within primary array
```

Figure 7-29 provides an example.

Figure 7-29 Verifying the HyperMetro working mode



7.5.6 Windows

7.5.6.1 Storage System Configuration

If UltraPath is used, retain the default settings of the initiator and configure **Host Access Mode** and **Preferred Path for HyperMetro** as required. **Table 7-11** lists the detailed settings.

Table 7-11 Storage configurations for interconnection with Windows application servers

HyperMetro Working Mode	Storage System	OS Setting	Host Access Mode	Preferred Path for HyperMetro	Description
Load balancing mode	Local storage	Windows	Asymmetric	Yes	The host uses all paths of a disk with equal priority.
	Remote storage	Windows	Asymmetric	Yes	
Local preferred mode	Local storage	Windows	Asymmetric	Yes	The host considers the paths from the local storage system as preferred paths, and those from the remote storage system as non-preferred paths.
	Remote storage	Windows	Asymmetric	No	

Configuring the Load Balancing Mode

Perform the following operations to configure the load balancing mode:

Step 1 On DeviceManager, choose **Services** > **Hosts**. Select the desired host, click ⋮ on the right, and choose **Modify**.

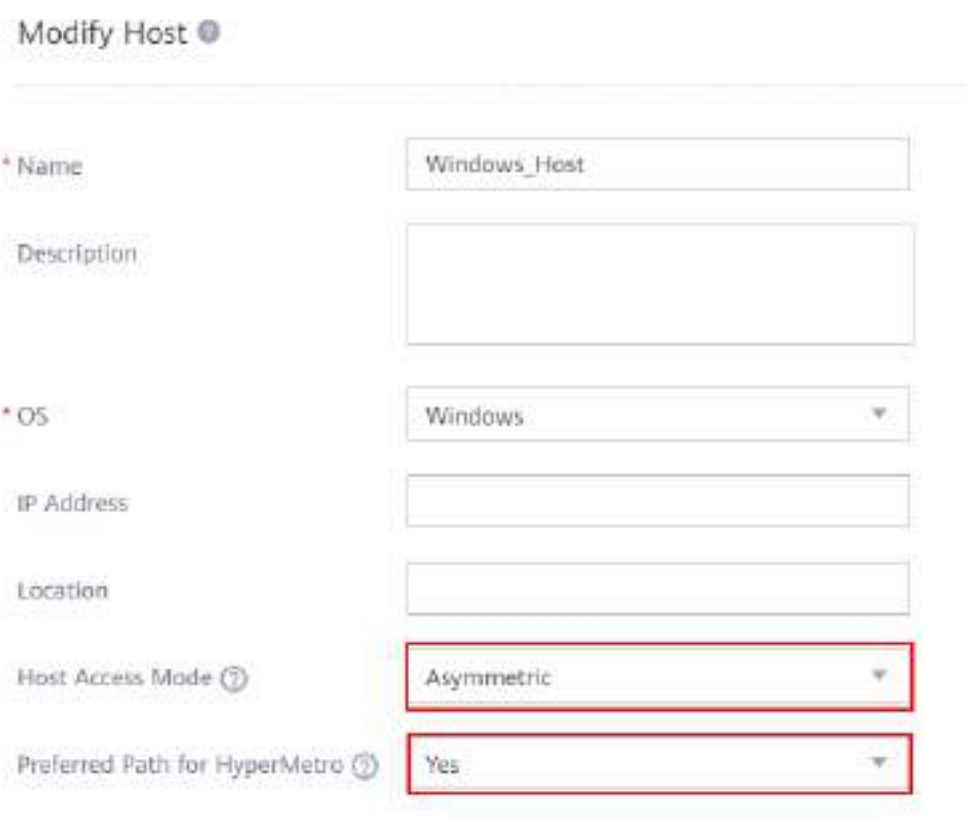
Figure 7-30 Modifying the host properties

NOTE

- The information displayed on the GUI may vary slightly with the product version.

Step 2 On the **Modify Host** page, set **Host Access Mode** of the local storage system to **Asymmetric** and **Preferred Path for HyperMetro** to **Yes**.

Figure 7-31 Settings on the local storage system



Step 3 Repeat the preceding steps to set **Host Access Mode** of the remote storage system to **Asymmetric** and **Preferred Path for HyperMetro** to **Yes**.

----End

Configuring the Local Preferred Mode

Perform the following operations to configure the local preferred mode:

Step 1 On DeviceManager, choose **Services** > **Hosts**. Select the desired host, click ⋮ on the right, and choose **Modify**.

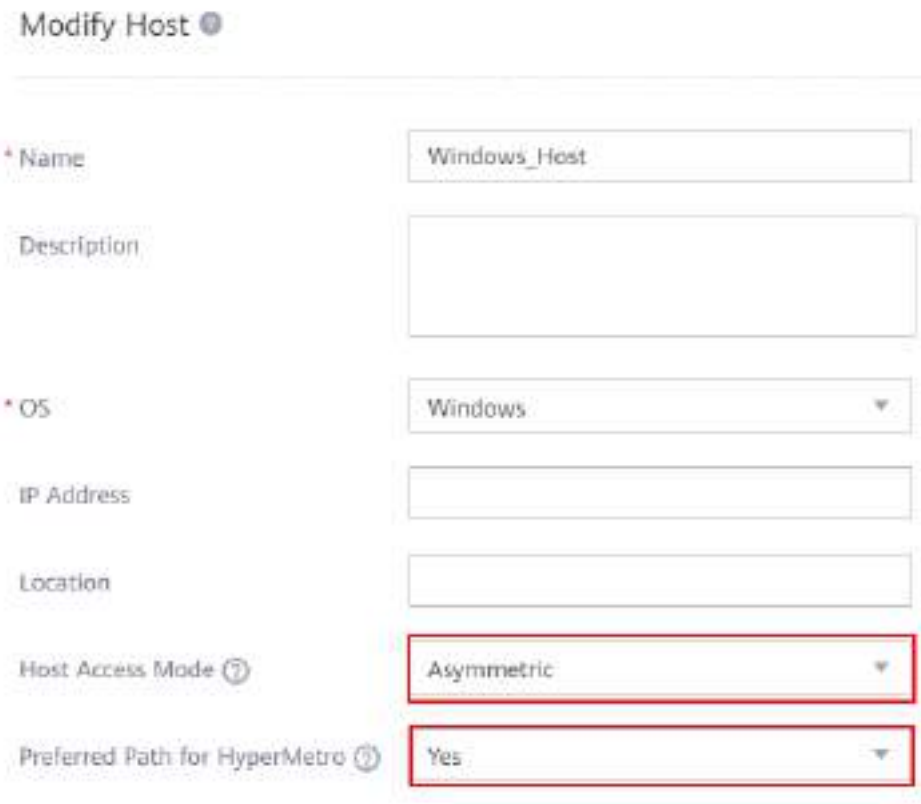
Figure 7-32 Modifying the host properties

NOTE

- The information displayed on the GUI may vary slightly with the product version.

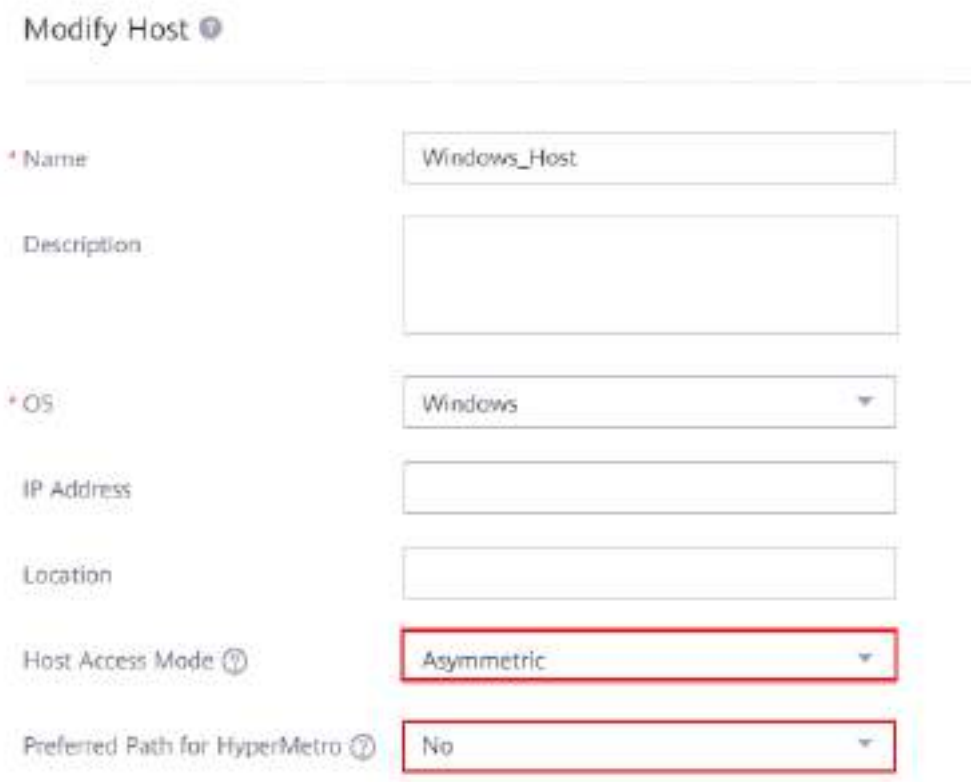
Step 2 For the local storage system, set **Host Access Mode** to **Asymmetric** and **Preferred Path for HyperMetro** to **Yes**.

Figure 7-33 Settings on the local storage system



Step 3 For the remote storage system, set **Host Access Mode** to **Asymmetric** and **Preferred Path for HyperMetro** to **No**.

Figure 7-34 Settings on the remote storage system



----End

NOTE

- For details about the Windows versions, see **Huawei Storage Interoperability Navigator**.
- Before configuring HyperMetro, enable automatic LUN SN synchronization on both storage systems. If this function is not enabled, one HyperMetro LUN may be identified as two disks by host applications. For details, see section "What Can I Do If the Host Identifies One HyperMetro LUN as Two Disks?" in the *HyperMetro Feature Guide for Block*.

7.5.6.2 Host Configuration

Install, configure, and use UltraPath by following instructions in the *OceanStor UltraPath for Windows User Guide*.

NOTICE

- If NPIV-enabled Windows VMs will directly access LUNs of the storage system, disable the alarm function of UltraPath after installing UltraPath.
- In a Windows server cluster, if NPIV-enabled Hyper-V VMs have been migrated (in online or fast mode) between servers, the NPIV paths managed by UltraPath will become disordered due to Windows mechanism defects. To ensure that services on Hyper-V VMs will not be interrupted, you are advised to run the **upadm set npiv_strategy={ off | check | force-check | update}** command to set the path detection mode to **update** in this scenario.

NOTE

- To obtain the document, log in to Huawei's technical support website (**https://support.huawei.com/enterprise/**), enter **UltraPath** in the search box, and select the associated path to the documentation page. Then find and download the desired document. To download software, click the **Software Download** tab and find the desired software.
- The UltraPath version matches the storage system version. You can query the version information in the version mapping table:
  1. Log in to **https://support.huawei.com/enterprise/**, enter your storage model in the search box, and select the associated path to the product documentation page.
  2. Find and download the version mapping table.
  3. Query the UltraPath version in the version mapping table.

Step 1 Set the HyperMetro working mode.

Use either of the following methods to set the HyperMetro working mode for UltraPath:

Method 1: Run the **upadm set hypermetro workingmode=auto** command to configure UltraPath to automatically adapt the HyperMetro working mode. This setting enables UltraPath to periodically query the host access mode configured on HyperMetro storage systems and adapt its HyperMetro working mode according to the host access mode.

Method 2: Run the following command to set UltraPath to work in a fixed HyperMetro working mode:

Command	Example
set hypermetro workingmode=*[priority | balance]* **primary_array_id=***ID*	**upadm set hypermetro workingmode=priority primary_array_id=0**

The following table describes the parameters in the command.

Parameter	Description	Default Value
workingmode	HyperMetro working mode. • **priority**: local preferred mode • **balance**: load balancing mode	priority **priority** is recommended. **balance** is applicable when two active-active data centers are in the same equipment room or on the same floor.
primary_array_id	ID of the preferred storage system. The ID is allocated by UltraPath. The storage array that is in the same data center as the application hosts reside is preferred. Run the **upadm show array** command to obtain the storage system ID. **NOTE** • In **priority** mode, the value of the parameter indicates the storage system to which I/Os are preferentially delivered. • In **balance** mode, the value of the parameter indicates the storage system where the first slice section resides.	None **NOTE** Mapping relationship between application hosts and storage systems: • Storage system A is the preferred system for all application hosts in data center A. • Storage system B is the preferred system for all application hosts in data center B.

NOTE

If you set UltraPath to automatically adapt the HyperMetro working mode, ensure that the host access mode on the storage system is consistent with that on the physical network.

Step 2 Configure the load balancing policy.

If HyperMetro works in load balancing mode, you can run the **upadm set hypermetro loadbalancemode=***[split-size | round-robin]* command to configure the load balancing policy. The following table describes the parameters in the command.

Parameter	Description	Default Value
loadbalancemode	Load balancing policy for HyperMetro systems. • **split-size**: slicing mode across storage systems. In this mode, UltraPath delivers I/Os to a specific storage system based on the start addresses of I/Os, slice size, and preferred storage system. For example, if the slice size is 128 MB, the I/Os whose start addresses range from 0 to 128 MB (excluding 128 MB) are preferentially delivered to the preferred storage system and the I/Os whose start addresses range from 128 MB to 256 MB (excluding 256 MB) are delivered to the non-preferred storage system. The default slice size is 128 MB. You can run the **upadm set hypermetro split_size** command to change it. • **round-robin**: round-robin mode across storage systems. In this mode, UltraPath selects two storage systems in turn to deliver I/Os.	split-size

----End

NOTICE

If a path switchover takes a long period of time, you can modify the timeout time for a driver by following instructions in "How Do I Modify the Timeout Time for the FC HBA Port Driver" and "How Do I Modify the iSCSI Initiator's Driver Timeout Time" in the ***Host Connectivity Guide***, thereby shortening I/O interruption.

7.6 Configuring an OS Native Multipathing Policy

7.6.1 AIX

7.6.1.1 Storage System Configuration

If the OS native multipathing software is used, retain the default settings of the initiator and configure **Host Access Mode** and **Preferred Path for HyperMetro** as required. **Table 7-12** lists the detailed settings.

Table 7-12 Storage configurations for interconnection with AIX application servers

HyperMetro Working Mode	Storage System	OS Setting	Host Access Mode	Preferred Path for HyperMetro	Description
Load balancing mode	Local storage	AIX	Load balancing	N/A	The host uses all paths of a disk with equal priority.
	Remote storage	AIX	Load balancing	N/A	
Local preferred mode	Local storage	AIX	Asymmetric	Yes	The host considers the paths from the local storage system as preferred paths, and those from the remote storage system as non-preferred paths.
	Remote storage	AIX	Asymmetric	No	

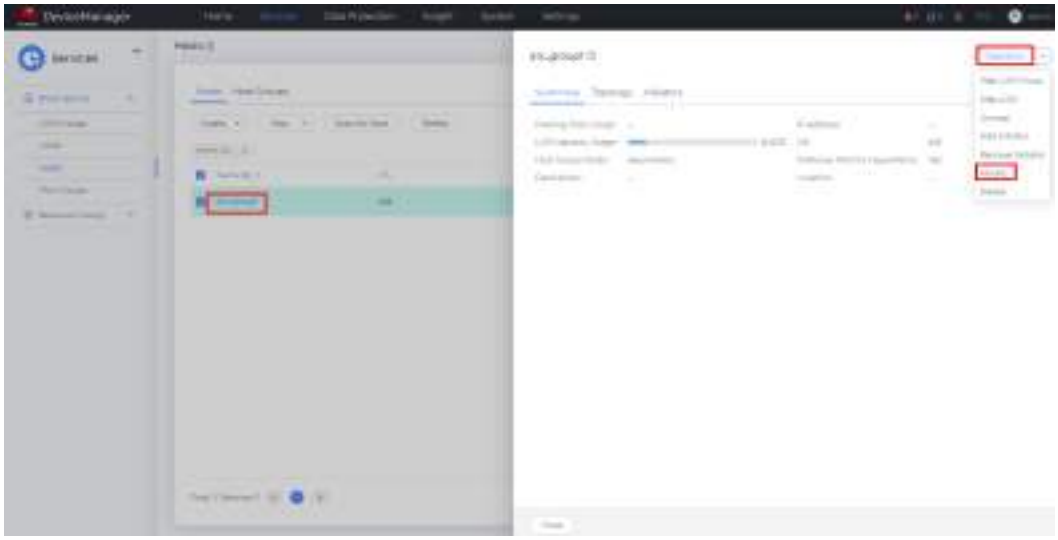
NOTICE

- For details about the AIX versions, see the **Huawei Storage Interoperability Navigator**.
- If a LUN has been mapped to a host, you must restart the host for the configuration to take effect after you modify **Host Access Mode** or **Preferred Path for HyperMetro**. If you map the LUN for the first time, restart is not needed.
- To change the LUN mapping on the storage system, including but not limited to changing the host LUN ID, changing the port online, and removing and adding a LUN, follow the instructions in "How Can I Change LUN Mappings When Non-Huawei Multipathing Software Is Used?" in the ***Host Connectivity Guide*** to correctly change the LUN mapping. Otherwise, services may be interrupted.
- When data is migrated from other Huawei storage systems (including OceanStor Dorado V3, OceanStor V3, and OceanStor V5) to 6.x series storage systems, configure the storage system by following instructions in "FAQs" in the ***Host Connectivity Guide***.

Configuring the Load Balancing Mode

Step 1 Click the host name and choose **Operation** > **Modify**.

Figure 7-35 Modifying the host properties

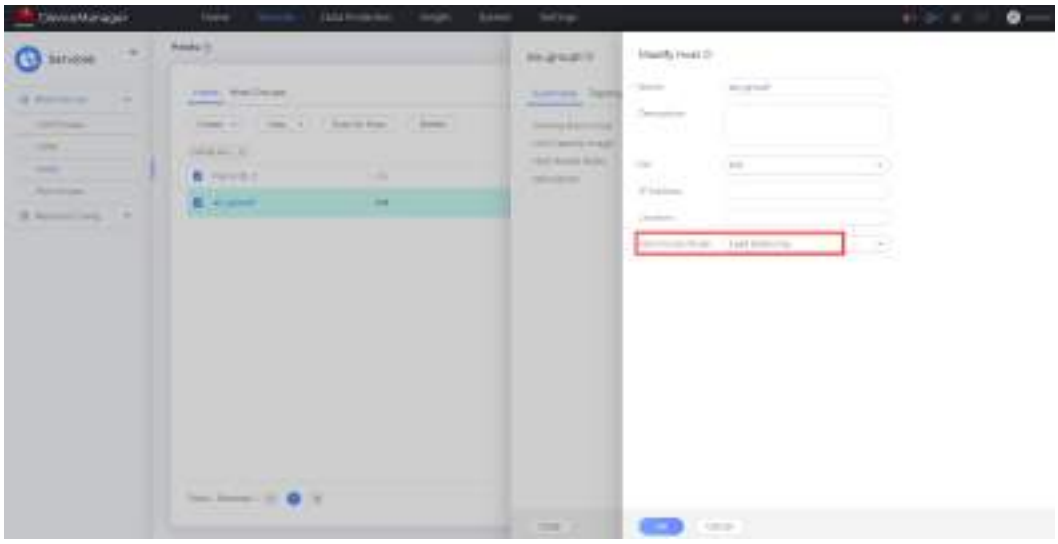


NOTE

The information displayed on the GUI may vary slightly with the product version.

Step 2 Set **Host Access Mode** to **Load balancing** for both the local and remote storage systems.

Figure 7-36 Setting the host access mode

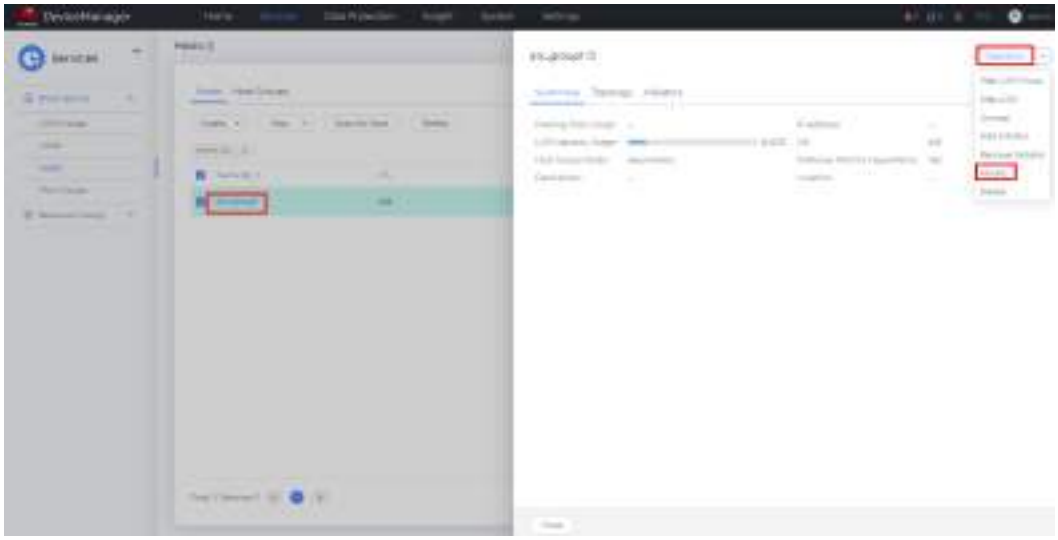


----End

Configuring the Local Preferred Mode

Step 1 Click the host name and choose **Operation** > **Modify**.

Figure 7-37 Modifying the host properties



Step 2 For the local storage system, set **Host Access Mode** to **Asymmetric** and **Preferred Path for HyperMetro** to **Yes**. For the remote storage system, set **Host Access Mode** to **Asymmetric** and **Preferred Path for HyperMetro** to **No**.

Figure 7-38 Settings on the local storage system

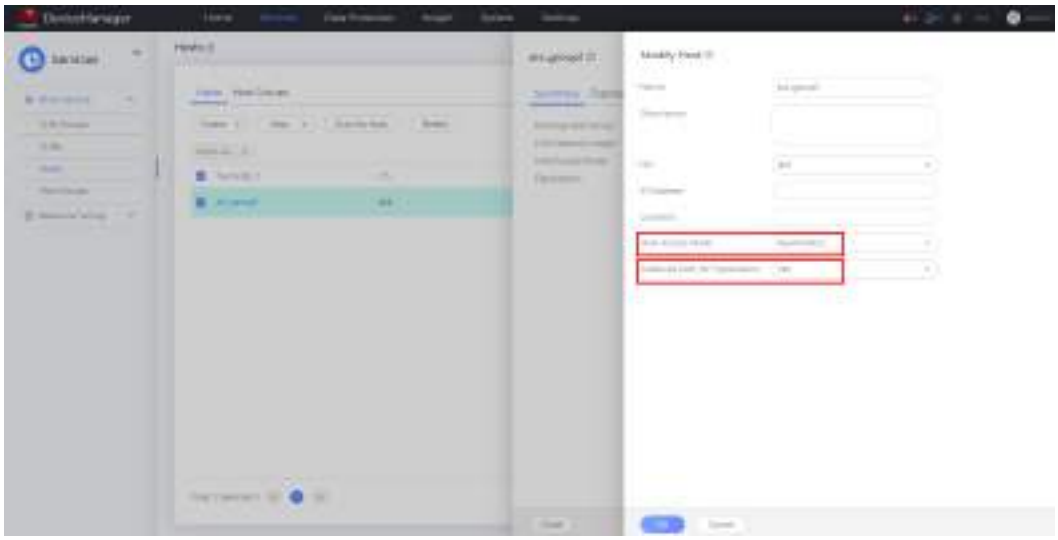
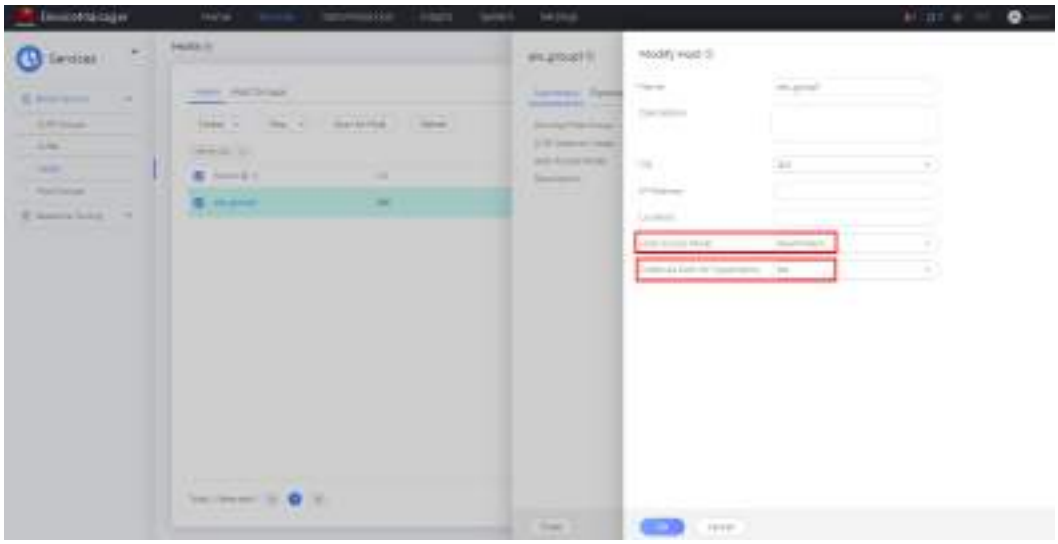


Figure 7-39 Settings on the remote storage system



----End

7.6.1.2 Host Configuration

Operating Environment Requirements

- In SAN Boot mode, the virtual LUN running the host's operating system must be a common virtual LUN. You can change a common virtual LUN to a HyperMetro virtual LUN only after ODM is installed on the host and the host is restarted.
- When NPIV coupled with VIOS is used, the requirements of NPIV on hardware and software must be met.

Installing and Enabling Multipathing Software

AIX native MPIO can take over Huawei storage disks only if the AIX ODM package has been installed. After AIX ODM has been installed, the **fc_err_recov** and **dyntrk** parameters of the FC HBAs must be set. For details on how to install AIX ODM, see the *AIX ODM for MPIO User Guide*.

Run the **lsdev -Cc disk** command to verify that MPIO has taken over the disks from Huawei storage. **Figure 7-40** is an example.

Figure 7-40 MPIO takeover

```
bash-3.2# lsdev -Cc disk
hdisk0  Defined            Virtual SCSI Disk Drive
hdisk1  Available 00-00-01 HUAWEI MPIO FC Disk Drive
hdisk2  Available 02-00-00 SAS RAID 0 Disk Array
hdisk3  Available 07-00-00 SAS RAID 0 Disk Array
hdisk4  Available 07-00-00 SAS RAID 0 Disk Array
hdisk13 Available 02-00-00 SAS RAID 0 Disk Array
bash-3.2#
```


NOTE

Before checking MPIO takeover, run the **cfgmgr -v** command to scan LUNs.

Configuring Multipathing Software

The default I/O policy is **fail_over**. I/Os can be delivered only on one path. To deliver I/Os to the paths of both active-active arrays, run the following command to change the I/O policy to **round_robin**. In UltraPath 31.0.2 and later, the default path selection algorithm of AIX ODM for MPIO is changed from **fail_over** to **round_robin**.

NOTICE

- When native MPIO is used, services must be suspended before you change the I/O policy for hdisk.
- In AIX 6.1 TL9 and later or AIX 7.1 TL5 and later, if the disk type is not **SCSI-2 reserves**, use the **shortest_queue** path selection algorithm to maximize SAN resource usage. When the load is light, the **shortest_queue** algorithm is similar to the **round_robin** algorithm. Once a path is congested, the system automatically allocates more I/Os to other lightly loaded paths. The **queue_depth** parameter can be modified based on the customer's host service configurations.

```
bash-3.2# chdev -l hdisk1 -a algorithm=round_robin
hdisk1 changed
bash-3.2# lsattr -EHl hdisk1
attribute       value            description                    user_settable

PCM             PCM/friend/MPIOpcm Path Control Module            False
PR_key_value    none             Persistant Reserve Key Value     True
algorithm       round_robin      Algorithm                        True
clr_q           no               Device CLEARS its Queue on error True
dist_err_pcnt   0                Distributed Error Percentage     True
dist_tw_width   50               Distributed Error Sample Time    True
hcheck_cmd      test_unit_rdy    Health Check Command             True
hcheck_interval 30               Health Check Interval            True
hcheck_mode     nonactive        Health Check Mode                True
location                         Location Label                   True
lun_id          0x1000000000000  Logical Unit Number ID           False
lun_reset_spt   yes              LUN Level Reset                  True
max_transfer    0x40000          Maximum TRANSFER Size            True
node_name       0x2100010203040509 FC Node Name                   False
pvid            none             Physical volume identifier       False
q_err           yes              Use QERR bit                     True
q_type          simple           Queuing TYPE                     True
queue_depth     32               Queue DEPTH                      True
reassign_to     120              REASSIGN time out value          True
reserve_policy  no_reserve       Reserve Policy                   True
rw_timeout      30               READ/WRITE time out value        True
scsi_id         0x10400          SCSI ID                          False
start_timeout   60               START unit time out value        True
timeout_policy  fail_path        Timeout Policy                   True
ww_name         0x2991010203040509 FC World Wide Name             False
bash-3.2#
```


7.6.1.3 Verification

Verifying the Load Balancing Mode

Step 1 Run the **lsdev -Cc disk** command to check whether HyperMetro LUNs have been aggregated on the host. Aggregated disks are identified as **HUAWEI MPIO FC Disk Drive**.

```
bash-3.2# lsdev -Cc disk
hdisk0  Defined          Virtual SCSI Disk Drive
hdisk1  Available 00-00-01 HUAWEI MPIO FC Disk Drive
hdisk2  Available 02-00-00 SAS RAID 0 Disk Array
hdisk3  Available 07-00-00 SAS RAID 0 Disk Array
hdisk4  Available 07-00-00 SAS RAID 0 Disk Array
hdisk13 Available 02-00-00 SAS RAID 0 Disk Array
bash-3.2#
```

Step 2 Run the **lsmpio -l hdisk1** command to check the path status and number of paths. The number of paths should be the sum of the logical paths on both storage systems (consistent with the actual configuration).

```
bash-3.2# lsmpio -l hdisk1
name    path_id  status   path_status  parent  connection

hdisk1  0       Enabled  Clo         fscsi0  2991010203040509,1000000000000
hdisk1  1       Enabled  Clo         fscsi0  2811010203040509,1000000000000
hdisk1  2       Enabled  Clo         fscsi0  2992010203040509,1000000000000
hdisk1  3       Enabled  Clo         fscsi0  2812010203040509,1000000000000
hdisk1  4       Enabled  Clo         fscsi1  2991010203040509,1000000000000
hdisk1  5       Enabled  Clo         fscsi1  2811010203040509,1000000000000
hdisk1  6       Enabled  Clo         fscsi1  2992010203040509,1000000000000
hdisk1  7       Enabled  Clo         fscsi1  2812010203040509,1000000000000
hdisk1  8       Enabled  Clo         fscsi0  2201002d52f14ac3,1000000000000
hdisk1  9       Enabled  Clo         fscsi0  2211002d52f14ac3,1000000000000
hdisk1  10      Enabled  Clo         fscsi0  2202002d52f14ac3,1000000000000
hdisk1  11      Enabled  Clo         fscsi0  2212002d52f14ac3,1000000000000
hdisk1  12      Enabled  Clo         fscsi1  2201002d52f14ac3,1000000000000
hdisk1  13      Enabled  Clo         fscsi1  2211002d52f14ac3,1000000000000
hdisk1  14      Enabled  Clo         fscsi1  2202002d52f14ac3,1000000000000
hdisk1  15      Enabled  Clo         fscsi1  2212002d52f14ac3,1000000000000
bash-3.2#
```

In the preceding command output, all paths are in the **Clo** state before service provisioning. There are a total of 16 paths, which equal to the number of configured logical paths (eight on each storage system).

Step 3 Check the path status after service provisioning. In load balancing mode, if all paths are in the **Sel** state and are carrying I/Os, the configuration is successful.

```
bash-3.2# lsmpio -l hdisk1
name    path_id  status   path_status  parent  connection

hdisk1  0       Enabled  Sel         fscsi0  2991010203040509,1000000000000
hdisk1  1       Enabled  Sel         fscsi0  2811010203040509,1000000000000
hdisk1  2       Enabled  Sel         fscsi0  2992010203040509,1000000000000
hdisk1  3       Enabled  Sel         fscsi0  2812010203040509,1000000000000
hdisk1  4       Enabled  Sel         fscsi1  2991010203040509,1000000000000
hdisk1  5       Enabled  Sel         fscsi1  2811010203040509,1000000000000
hdisk1  6       Enabled  Sel         fscsi1  2992010203040509,1000000000000
hdisk1  7       Enabled  Sel         fscsi1  2812010203040509,1000000000000
hdisk1  8       Enabled  Sel         fscsi0  2201002d52f14ac3,1000000000000
hdisk1  9       Enabled  Sel         fscsi0  2211002d52f14ac3,1000000000000
hdisk1  10      Enabled  Sel         fscsi0  2202002d52f14ac3,1000000000000
hdisk1  11      Enabled  Sel         fscsi0  2212002d52f14ac3,1000000000000
hdisk1  12      Enabled  Sel         fscsi1  2201002d52f14ac3,1000000000000
hdisk1  13      Enabled  Sel         fscsi1  2211002d52f14ac3,1000000000000
hdisk1  14      Enabled  Sel         fscsi1  2202002d52f14ac3,1000000000000
```



```
hdisk1  15      Enabled  Sel        fscsi1  2212002d52f14ac3,1000000000000
bash-3.2#
```

----End

Verifying the Local Preferred Mode

Step 1 Run the **lsdev -Cc disk** command to check whether HyperMetro LUNs have been aggregated on the host. Aggregated disks are identified as **HUAWEI MPIO FC Disk Drive**.

```
bash-3.2# lsdev -Cc disk
hdisk0  Defined          Virtual SCSI Disk Drive
hdisk1  Available 00-00-01 HUAWEI MPIO FC Disk Drive
hdisk2  Available 02-00-00 SAS RAID 0 Disk Array
hdisk3  Available 07-00-00 SAS RAID 0 Disk Array
hdisk4  Available 07-00-00 SAS RAID 0 Disk Array
hdisk13 Available 02-00-00 SAS RAID 0 Disk Array
bash-3.2#
```

Step 2 Run the **lsmpio -l hdisk1** command to check the path status and number of paths. The number of paths should be the sum of the logical paths on both storage systems (consistent with the actual configuration).

```
bash-3.2# lsmpio -l hdisk1
name    path_id  status   path_status  parent  connection

hdisk1  0       Enabled  Clo        fscsi0  2991010203040509,1000000000000
hdisk1  1       Enabled  Clo        fscsi0  2811010203040509,1000000000000
hdisk1  2       Enabled  Clo        fscsi0  2992010203040509,1000000000000
hdisk1  3       Enabled  Clo        fscsi0  2812010203040509,1000000000000
hdisk1  4       Enabled  Clo        fscsi1  2991010203040509,1000000000000
hdisk1  5       Enabled  Clo        fscsi1  2811010203040509,1000000000000
hdisk1  6       Enabled  Clo        fscsi1  2992010203040509,1000000000000
hdisk1  7       Enabled  Clo        fscsi1  2812010203040509,1000000000000
hdisk1  8       Enabled  Clo        fscsi0  2201002d52f14ac3,1000000000000
hdisk1  9       Enabled  Clo        fscsi0  2211002d52f14ac3,1000000000000
hdisk1  10      Enabled  Clo        fscsi0  2202002d52f14ac3,1000000000000
hdisk1  11      Enabled  Clo        fscsi0  2212002d52f14ac3,1000000000000
hdisk1  12      Enabled  Clo        fscsi1  2201002d52f14ac3,1000000000000
hdisk1  13      Enabled  Clo        fscsi1  2211002d52f14ac3,1000000000000
hdisk1  14      Enabled  Clo        fscsi1  2202002d52f14ac3,1000000000000
hdisk1  15      Enabled  Clo        fscsi1  2212002d52f14ac3,1000000000000
bash-3.2#
```

Step 3 Check the path status after service provisioning. The local preferred mode involves preferred and non-preferred paths. You must correctly identify the status and number of preferred and non-preferred paths. In this example, there are eight preferred paths (**Opt** state) and eight non-preferred paths (**Non** state). **Sel,Opt** indicates that I/Os are running over the eight **Opt** paths. The configuration is successful.

```
bash-3.2# lsmpio -l hdisk1
name    path_id  status   path_status  parent  connection

hdisk1  0       Enabled  Sel,Opt     fscsi0  2991010203040509,1000000000000
hdisk1  1       Enabled  Sel,Opt     fscsi0  2811010203040509,1000000000000
hdisk1  2       Enabled  Sel,Opt     fscsi0  2992010203040509,1000000000000
hdisk1  3       Enabled  Sel,Opt     fscsi0  2812010203040509,1000000000000
hdisk1  4       Enabled  Sel,Opt     fscsi1  2991010203040509,1000000000000
hdisk1  5       Enabled  Sel,Opt     fscsi1  2811010203040509,1000000000000
hdisk1  6       Enabled  Sel,Opt     fscsi1  2992010203040509,1000000000000
hdisk1  7       Enabled  Sel,Opt     fscsi1  2812010203040509,1000000000000
hdisk1  8       Enabled  Non         fscsi0  2201002d52f14ac3,1000000000000
hdisk1  9       Enabled  Non         fscsi0  2211002d52f14ac3,1000000000000
hdisk1  10      Enabled  Non         fscsi0  2202002d52f14ac3,1000000000000
hdisk1  11      Enabled  Non         fscsi0  2212002d52f14ac3,1000000000000
```



```
hdisk1  12      Enabled  Non      fscsi1  2201002d52f14ac3,1000000000000
hdisk1  13      Enabled  Non      fscsi1  2211002d52f14ac3,1000000000000
hdisk1  14      Enabled  Non      fscsi1  2202002d52f14ac3,1000000000000
hdisk1  15      Enabled  Non      fscsi1  2212002d52f14ac3,1000000000000
bash-3.2#
```

----End

NOTICE

Only AIX 6.1 TL9, AIX 7.1 TL3, and later versions support the **lsmpio** command. For other AIX versions, you can only use the **lspath** command to query paths.

7.6.2 HP-UX

7.6.2.1 Storage System Configuration

If the OS native multipathing software is used, retain the default settings of the initiator and configure **Host Access Mode** and **Preferred Path for HyperMetro** as required. **Table 7-13** lists the detailed settings.

Table 7-13 Storage configurations for interconnection with HP-UX application servers

HyperMetro Working Mode	Storage System	OS Setting	Host Access Mode	Preferred Path for HyperMetro	Description
Load balancing	Local storage	HP-UX	Load balancing	N/A	The host uses all paths of a disk with equal priority.
	Remote storage	HP-UX	Load balancing	N/A	
Local preferred	Local storage	HP-UX	Asymmetric	Yes	The host considers the paths from the local storage system as preferred paths, and those from the remote storage system as non-preferred paths.
	Remote storage	HP-UX	Asymmetric	No	

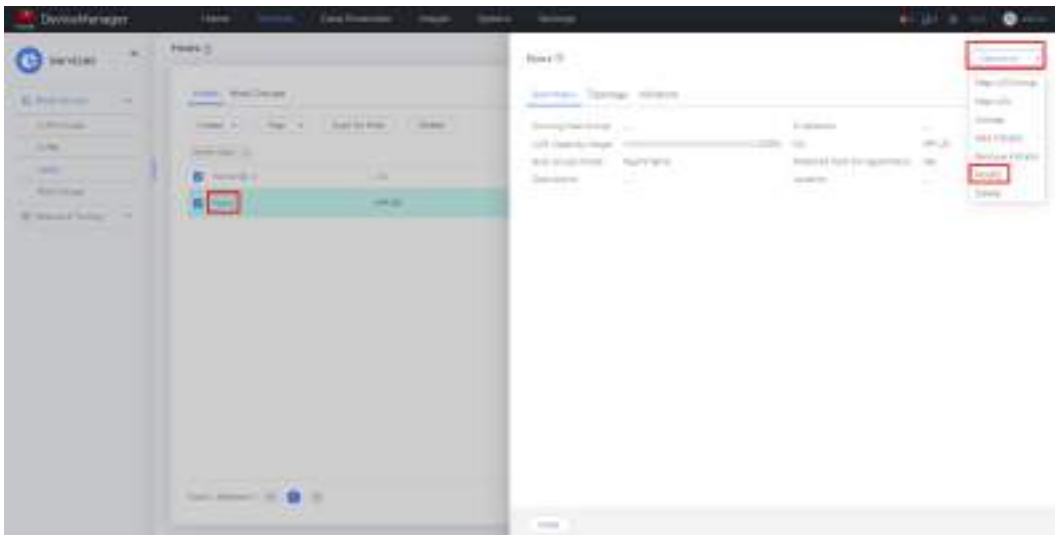
NOTICE

- For details about the HP-UX versions, see the **Huawei Storage Interoperability Navigator**.
- If a LUN has been mapped to a host, you must restart the host for the configuration to take effect after you modify **Host Access Mode** or **Preferred Path for HyperMetro**. If you map the LUN for the first time, restart is not needed.
- Ensure that HyperMetro is working properly when modifying networking.
- When data is migrated from other Huawei storage systems (including OceanStor Dorado V3, OceanStor V3, and OceanStor V5) to OceanStor Dorado V6, configure the storage system by following instructions in "Recommended Configurations for OceanStor Dorado V6 for Taking Over Data from Other Huawei Storage Systems When the Host Uses the OS Native Multipathing Software" in the *OceanStor Dorado Host Connectivity Guide for HP-UX*.

Configuring the Load Balancing Mode

Step 1 Click the host name and choose **Operation** > **Modify**.

Figure 7-41 Modifying the host properties

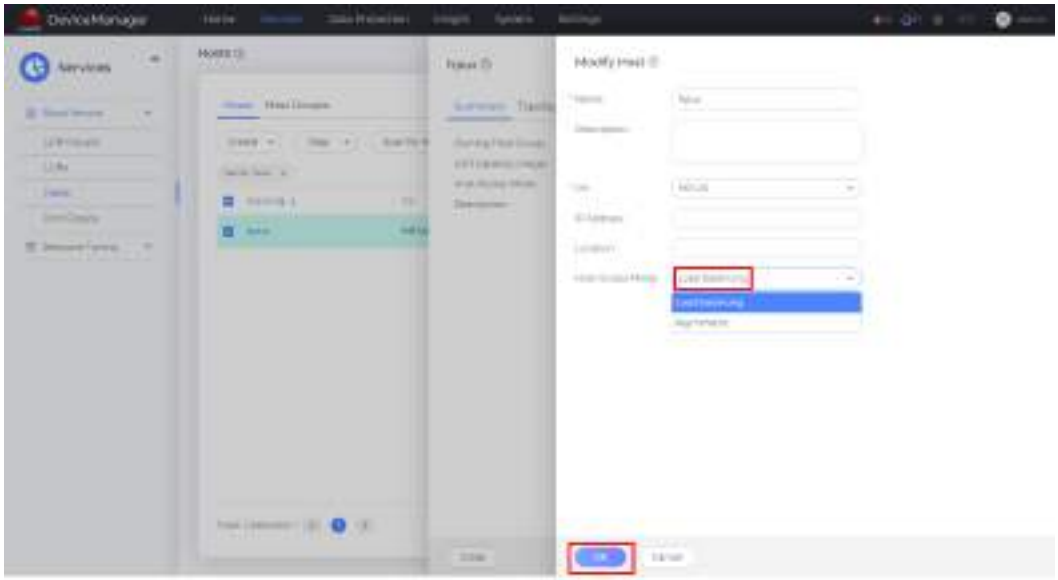


NOTE

The information displayed on the GUI may vary slightly with the product version.

Step 2 For both the local and remote storage systems, set **Host Access Mode** to **Load balancing**.

Figure 7-42 Settings on the local and remote storage systems

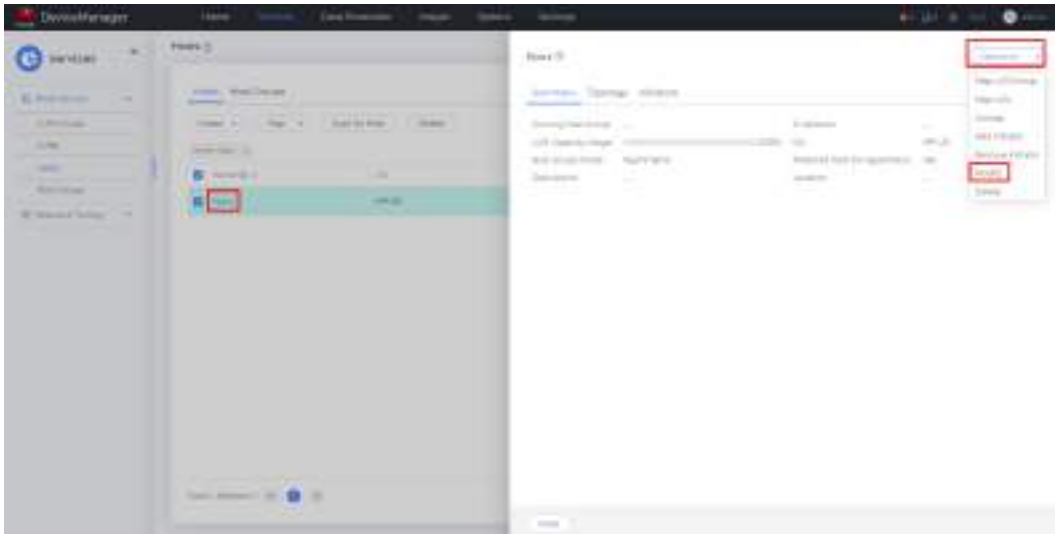


----End

Configuring the Local Preferred Mode

Step 1 Click the host name and choose **Operation** > **Modify**.

Figure 7-43 Modifying the host properties



Step 2 For the local storage system, set **Host Access Mode** to **Asymmetric** and **Preferred Path for HyperMetro** to **Yes**. For the remote storage system, set **Host Access Mode** to **Asymmetric** and **Preferred Path for HyperMetro** to **No**.

Figure 7-44 Settings on the local storage system

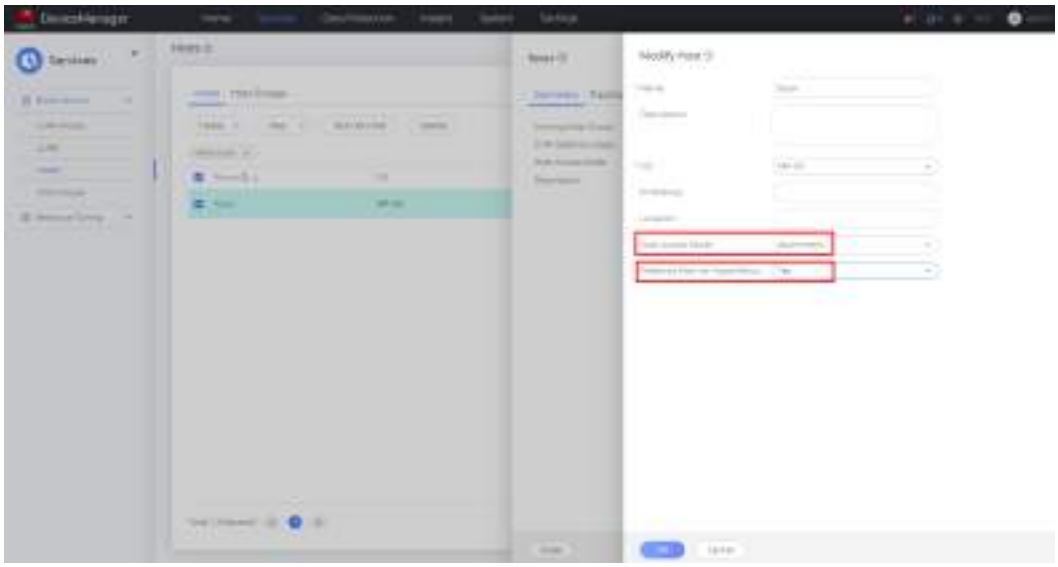
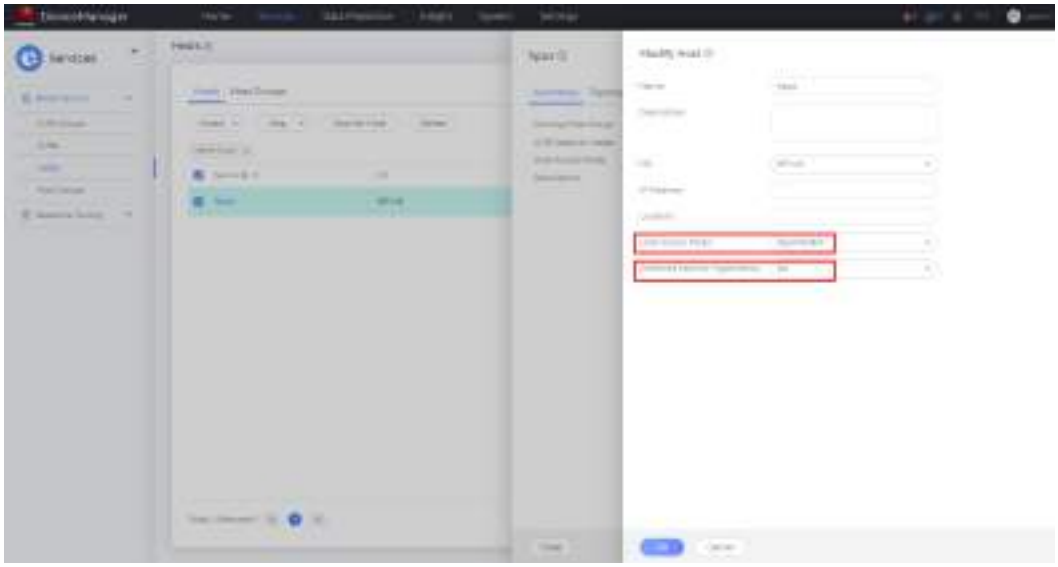


Figure 7-45 Settings on the remote storage system



----End

7.6.2.2 Host Configuration

Verifying Version and Patch Requirements

NMP requires that the operating system should not be earlier than HP-UX 11i v3 Update 4 (11.31.0903).

Run the following command to query the operating system version:

```
bash-4.1# swlist | grep HPUX11i
HPUX11i-DC-OE               B.11.31.1403 HP-UX Data Center Operating Environment
bash-4.1#
```

According to the command output, the version is HP-UX 11i v3 1403, meeting requirements.

Enabling Multipathing Software

By default, NMP is enabled. No extra setting is required.

You can run the following command to check the load balancing policy and ALUA status of a LUN:

```
bash-4.1# scsimgr get_attr -D /dev/rdisk/disk12 -a load_bal_policy

SCSI ATTRIBUTES FOR LUN : /dev/rdisk/disk12

name = load_bal_policy
current = round_robin
default = round_robin
saved =

bash-4.1#
bash-4.1# scsimgr get_attr -D /dev/rdisk/disk12 -a alua_enabled

SCSI ATTRIBUTES FOR LUN : /dev/rdisk/disk12

name = alua_enabled
current = true
default = true
saved =

bash-4.1#
```

According to the command output, the load balancing policy is **round-robin**, and ALUA is enabled.

NOTE

disk12 is a device file created for the mapped LUN after connectivity is configured.

Configuring Multipathing Software

Retain the default settings. You can run the **scsimgr lun_map -D /dev/rdisk/disk#** command to view the disk path information and LUN attributes. For details, see **7.6.2.3 Verification**.

7.6.2.3 Verification

Verifying the Load Balancing Mode

Step 1 Run the **ioscan -funNC disk** command to check whether HyperMetro LUNs have been properly aggregated.

HyperMetro LUNs should be aggregated as a drive letter on the host, such as **disk12** in the following example:

```
bash-4.1# ioscan -funNC disk
Class     I  H/W Path  Driver S/W State   H/W Type     Description
==========================================================================
disk      2  64000/0xfa00/0x0  esdisk   CLAIMED     DEVICE       HP      DG146BB976
                   /dev/disk/disk2      /dev/disk/disk2_p1   /dev/disk/disk2_p2   /dev/rdisk/disk2     /dev/rdisk/
disk2_p1  /dev/rdisk/disk2_p2
disk      3  64000/0xfa00/0x1  esdisk   CLAIMED     DEVICE       HP      DG146BB976
                   /dev/disk/disk3      /dev/disk/disk3_p1   /dev/disk/disk3_p2   /dev/disk/disk3_p3   /dev/rdisk/
disk3     /dev/rdisk/disk3_p1  /dev/rdisk/disk3_p2  /dev/rdisk/disk3_p3
disk      5  64000/0xfa00/0x2  esdisk   CLAIMED     DEVICE       TEAC    DVD-ROM DW-224EV
                   /dev/disk/disk5   /dev/rdisk/disk5
disk     12  64000/0xfa00/0xa  esdisk   CLAIMED     DEVICE       HUAWEI  XSG1
                   /dev/disk/disk12   /dev/rdisk/disk12
```


Step 2 Run the **scsimgr lun_map -D /dev/rdisk/disk#** command to check the path status and number of paths.

The number of paths should be the sum of the logical paths on both storage systems (consistent with the actual configuration).

```
bash-4.1# scsimgr lun_map -D /dev/rdisk/disk12

      LUN PATH INFORMATION FOR LUN : /dev/rdisk/disk12

Total number of LUN paths     = 8
World Wide Identifier(WWID)    = 0x6002d52100f14ac30485420100000015

LUN path : lunpath17
Class                  = lunpath
Instance                = 17
Hardware path              = 0/2/1/0/4/0.0x2992010203040509.0x4001000000000000
SCSI transport protocol      = fibre_channel
State                  = UNOPEN
Last Open or Close state     = ACTIVE

LUN path : lunpath16
Class                  = lunpath
Instance                = 16
Hardware path              = 0/2/1/0/4/0.0x2991010203040509.0x4001000000000000
SCSI transport protocol      = fibre_channel
State                  = UNOPEN
Last Open or Close state     = ACTIVE

LUN path : lunpath19
Class                  = lunpath
Instance                = 19
Hardware path              = 0/2/1/0/4/0.0x2812010203040509.0x4001000000000000
SCSI transport protocol      = fibre_channel
State                  = UNOPEN
Last Open or Close state     = ACTIVE

LUN path : lunpath7
Class                  = lunpath
Instance                = 7
Hardware path              = 0/2/1/0/4/0.0x2211002d52f14ac3.0x4001000000000000
SCSI transport protocol      = fibre_channel
State                  = UNOPEN
Last Open or Close state     = ACTIVE

LUN path : lunpath11
Class                  = lunpath
Instance                = 11
Hardware path              = 0/2/1/0/4/0.0x2212002d52f14ac3.0x4001000000000000
SCSI transport protocol      = fibre_channel
State                  = UNOPEN
Last Open or Close state     = ACTIVE

LUN path : lunpath9
Class                  = lunpath
Instance                = 9
Hardware path              = 0/2/1/0/4/0.0x2202002d52f14ac3.0x4001000000000000
SCSI transport protocol      = fibre_channel
State                  = UNOPEN
Last Open or Close state     = ACTIVE

LUN path : lunpath8
Class                  = lunpath
Instance                = 8
Hardware path              = 0/2/1/0/4/0.0x2201002d52f14ac3.0x4001000000000000
SCSI transport protocol      = fibre_channel
State                  = UNOPEN
Last Open or Close state     = ACTIVE

LUN path : lunpath13
```



```
Class                    = lunpath
Instance                  = 13
Hardware path             = 0/2/1/0/4/0.0x2811010203040509.0x4001000000000000
SCSI transport protocol      = fibre_channel
State                    = UNOPEN
Last Open or Close state     = ACTIVE

bash-4.1#
```

In the preceding command output, **State=ACTIVE** corresponds to preferred paths. **State** of eight paths (**lunpath7**, **lunpath8**, **lunpath9**, **lunpath11**, **lunpath13**, **lunpath16**, **lunpath17**, and **lunpath19**) is **ACTIVE**, which is consistent with the actual configuration. The configuration is successful.

NOTICE

When a LUN mapped to the host does not have any service, the state of paths to this LUN on the host becomes **UNOPEN**. To restore the path status to **ACTIVE**, run the **ioscan** command or read or write the mapped LUN.

----End

Verifying the Local Preferred Mode

Step 1 Run the **ioscan -funNC disk** command to check HyperMetro LUNs have been aggregated.

HyperMetro LUNs should be aggregated as a drive letter on the host, such as **disk12** in the following example:

```
bash-3.2# ioscan -funNC disk
Class     I  H/W Path  Driver S/W State   H/W Type     Description
==========================================================================
disk      2  64000/0xfa00/0x0  esdisk   CLAIMED     DEVICE       HP      DG146BB976
                   /dev/disk/disk2      /dev/disk/disk2_p1   /dev/disk/disk2_p2   /dev/rdisk/disk2     /dev/rdisk/
disk2_p1  /dev/rdisk/disk2_p2
disk      3  64000/0xfa00/0x1  esdisk   CLAIMED     DEVICE       HP      DG146BB976
                   /dev/disk/disk3      /dev/disk/disk3_p1   /dev/disk/disk3_p2   /dev/disk/disk3_p3   /dev/rdisk/
disk3     /dev/rdisk/disk3_p1  /dev/rdisk/disk3_p2  /dev/rdisk/disk3_p3
disk      5  64000/0xfa00/0x2  esdisk   CLAIMED     DEVICE       TEAC    DVD-ROM DW-224EV
                   /dev/disk/disk5   /dev/rdisk/disk5
disk     12  64000/0xfa00/0xa  esdisk   CLAIMED     DEVICE       HUAWEI  XSG1
                   /dev/disk/disk12   /dev/rdisk/disk12
```

Step 2 Run the **scsimgr lun_map -D /dev/rdisk/disk#** command to check the path status and number of paths.

The number of paths should be the sum of the logical paths on both storage systems (consistent with the actual configuration).

```
bash-4.1# scsimgr lun_map -D /dev/rdisk/disk12

      LUN PATH INFORMATION FOR LUN : /dev/rdisk/disk12

Total number of LUN paths     = 8
World Wide Identifier(WWID)    = 0x6002d52100f14ac30485420100000015

LUN path : lunpath13
Class                    = lunpath
Instance                  = 13
Hardware path             = 0/2/1/0/4/0.0x2811010203040509.0x4001000000000000
SCSI transport protocol      = fibre_channel
State                    = UNOPEN
```



```
Last Open or Close state      = STANDBY

LUN path : lunpath7
Class                    = lunpath
Instance                  = 7
Hardware path               = 0/2/1/0/4/0.0x2211002d52f14ac3.0x4001000000000000
SCSI transport protocol      = fibre_channel
State                    = UNOPEN
Last Open or Close state      = ACTIVE

LUN path : lunpath16
Class                    = lunpath
Instance                  = 16
Hardware path               = 0/2/1/0/4/0.0x2991010203040509.0x4001000000000000
SCSI transport protocol      = fibre_channel
State                    = UNOPEN
Last Open or Close state      = STANDBY

LUN path : lunpath9
Class                    = lunpath
Instance                  = 9
Hardware path               = 0/2/1/0/4/0.0x2202002d52f14ac3.0x4001000000000000
SCSI transport protocol      = fibre_channel
State                    = UNOPEN
Last Open or Close state      = ACTIVE

LUN path : lunpath8
Class                    = lunpath
Instance                  = 8
Hardware path               = 0/2/1/0/4/0.0x2201002d52f14ac3.0x4001000000000000
SCSI transport protocol      = fibre_channel
State                    = UNOPEN
Last Open or Close state      = ACTIVE

LUN path : lunpath17
Class                    = lunpath
Instance                  = 17
Hardware path               = 0/2/1/0/4/0.0x2992010203040509.0x4001000000000000
SCSI transport protocol      = fibre_channel
State                    = UNOPEN
Last Open or Close state      = STANDBY

LUN path : lunpath11
Class                    = lunpath
Instance                  = 11
Hardware path               = 0/2/1/0/4/0.0x2212002d52f14ac3.0x4001000000000000
SCSI transport protocol      = fibre_channel
State                    = UNOPEN
Last Open or Close state      = ACTIVE

LUN path : lunpath19
Class                    = lunpath
Instance                  = 19
Hardware path               = 0/2/1/0/4/0.0x2812010203040509.0x4001000000000000
SCSI transport protocol      = fibre_channel
State                    = UNOPEN
Last Open or Close state      = STANDBY
```

In the preceding command output, **State=ACTIVE** corresponds to preferred paths, and **State=STANDBY** corresponds to non-preferred paths. **State** of four paths (**lunpath7**, **lunpath8**, **lunpath9**, and **lunpath11**) is **ACTIVE**, and that of the other four (**lunpath13**, **lunpath16**, **lunpath17**, and **lunpath19**) is **STANDBY**, which are consistent with the actual configuration. The configuration is successful.

NOTICE

When a LUN mapped to the host does not have any service, the state of paths to this LUN on the host becomes **UNOPEN**. To restore the path status to **ACTIVE**, run the **ioscan** command or read or write the mapped LUN.

----End

7.6.3 Red Hat

7.6.3.1 Storage System Configuration

If the OS native multipathing software is used, retain the default settings of the initiator and configure **Host Access Mode** and **Preferred Path for HyperMetro** as required. **Table 7-14** lists the detailed settings.

Table 7-14 Storage configurations for interconnection with Red Hat application servers

HyperMetro Working Mode	Storage System	OS Setting	Host Access Mode	Preferred Path for HyperMetro	Description
Load balancing mode	Local storage	Linux	Load balancing	N/A	The host uses all paths of a disk with equal priority.
	Remote storage	Linux	Load balancing	N/A	
Local preferred mode	Local storage	Linux	Asymmetric	Yes	The host considers the paths from the local storage system as preferred paths, and those from the remote storage system as non-preferred paths.
	Remote storage	Linux	Asymmetric	No	

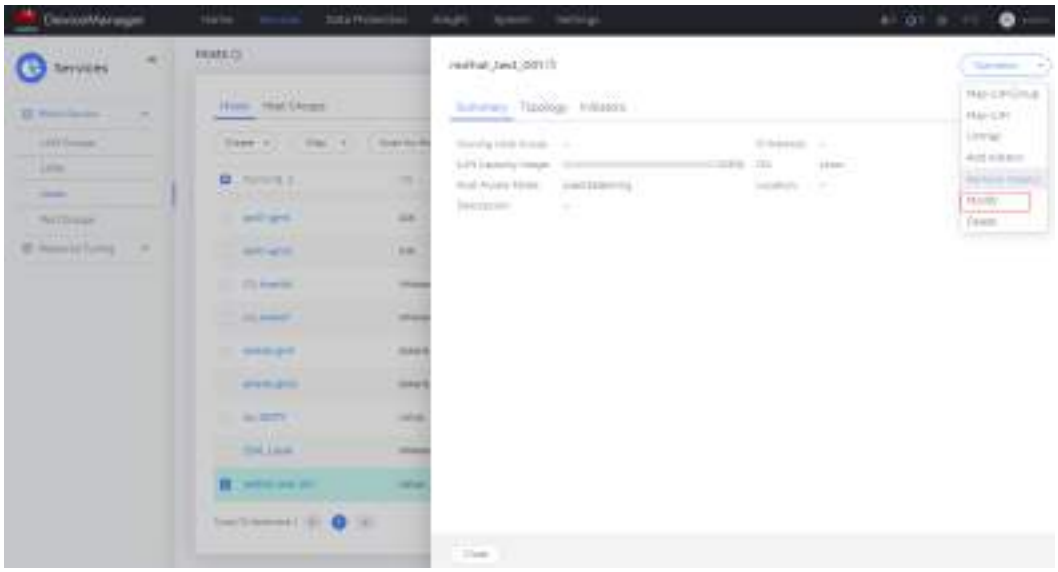
NOTICE

- For details about the Red Hat versions, see the **Huawei Storage Interoperability Navigator**.
- If a LUN has been mapped to a host, you must restart the host for the configuration to take effect after you modify **Host Access Mode** or **Preferred Path for HyperMetro**. If you map the LUN for the first time, restart is not needed.
- When data is migrated from other Huawei storage systems (including OceanStor Dorado V3, OceanStor V3, and OceanStor V5) to OceanStor Dorado V6, configure the storage system by following instructions in "FAQs" in the ***Host Connectivity Guide***.

Configuring the Load Balancing Mode

Step 1 Click the host name and choose **Operation** > **Modify**.

Figure 7-46 Modifying the host properties

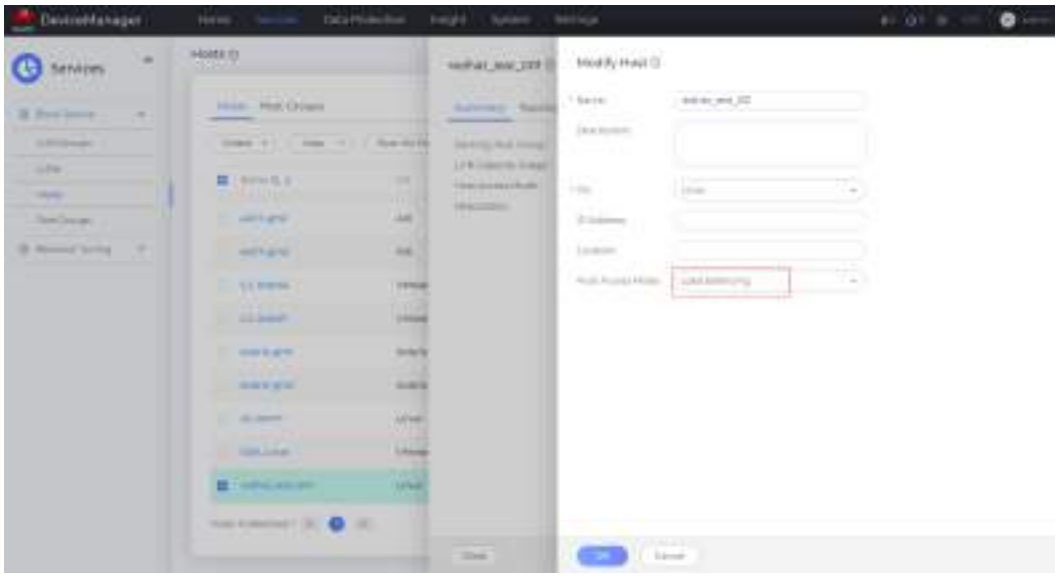


NOTE

The information displayed on the GUI may vary slightly with the product version.

Step 2 Set **Host Access Mode** to **Load balancing** for both the local and remote storage systems.

Figure 7-47 Setting the host access mode

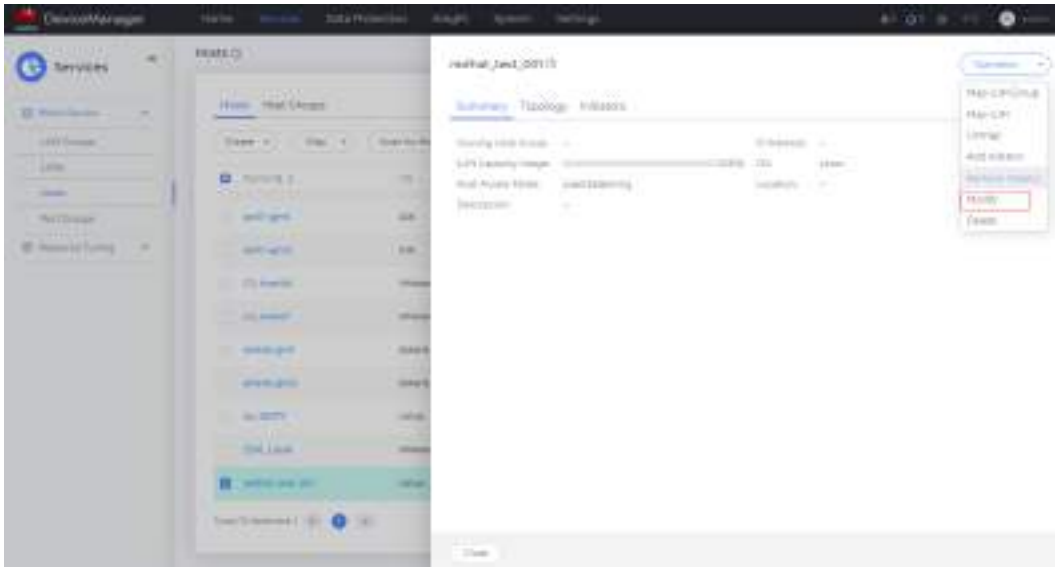


----End

Configuring the Local Preferred Mode

Step 1 Click the host name and choose **Operation** > **Modify**.

Figure 7-48 Modifying the host properties



NOTE

The information displayed on the GUI may vary slightly with the product version.

Step 2 For the local storage system, set **Host Access Mode** to **Asymmetric** and **Preferred Path for HyperMetro** to **Yes**. For the remote storage system, set **Host Access Mode** to **Asymmetric** and **Preferred Path for HyperMetro** to **No**.

Figure 7-49 Settings on the local storage system

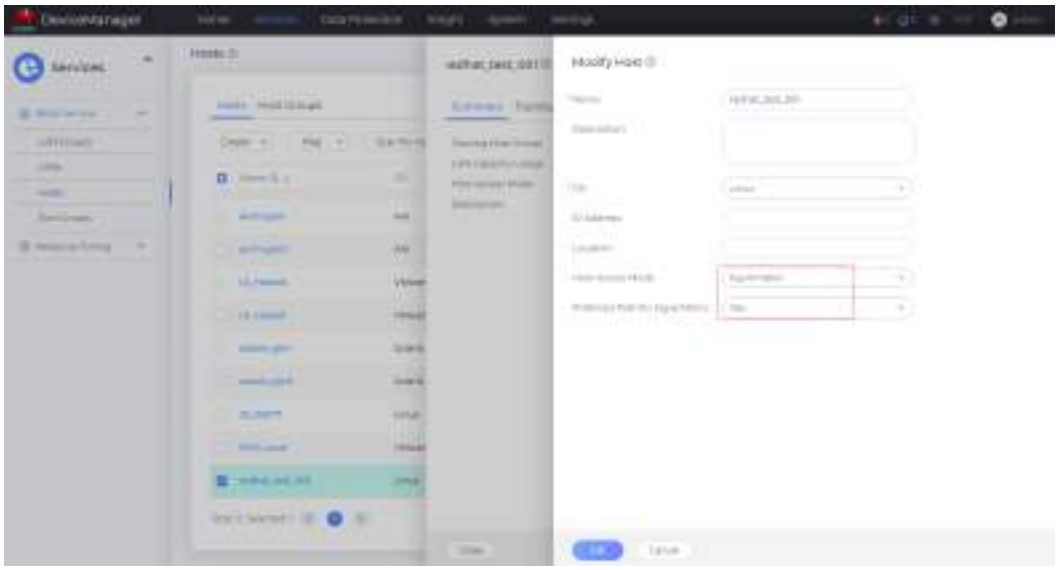
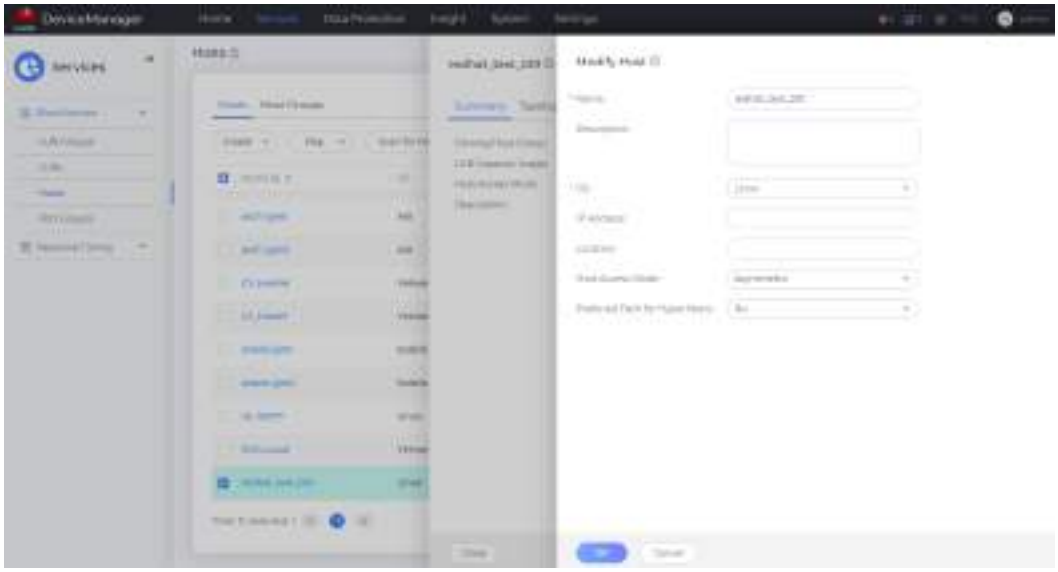


Figure 7-50 Settings on the remote storage system



----End

7.6.3.2 Host Configuration

Installing Multipathing Software

Generally, multipathing software packages in Red Hat are rpm packages starting with **device-mapper-multipath**. If you did not install the multipathing software when installing the operating system, you can obtain the software package from the system image and use the **rpm** command to install it.

Modifying the Configuration File

DM-Multipath's most important configuration file is **/etc/multipath.conf**.

Some operating systems have this file by default. If your operating system does not have this file, you can copy the **multipath.conf** or **multipath.conf.synthetic** file to the **/etc** directory to generate one.

```
[root@localhost ~]# cp /usr/share/doc/device-mapper-multipath-0.4.9/multipath.conf /etc/multipath.conf
```

If the system does not have a template, run the **/sbin/mpathconf --enable** command to manually generate **/etc/multipath.conf**.

If **Host Access Mode** is set to **Load balancing** on the storage system, add the following content to the **devices** field in the **/etc/multipath.conf** file:

```
devices {
    device {
        vendor                "HUAWEI"
        product               "XSG1"
        path_grouping_policy    multibus
        path_checker            tur
        prio                  const
        path_selector           "round-robin 0"
        failback              immediate
        dev_loss_tmo            30
        fast_io_fail_tmo        5
        no_path_retry           15
```



```
}
}
```

If **Host Access Mode** is set to **Asymmetric** on the storage system, add the following content to the **devices** field in the **/etc/multipath.conf** file:

```
devices {
    device {
            vendor                "HUAWEI"
            product               "XSG1"
            path_grouping_policy    group_by_prio
            path_checker            tur
            prio                  alua
            path_selector           "round-robin 0"
            failback              immediate
            dev_loss_tmo            30
            fast_io_fail_tmo        5
            no_path_retry           15
}
}
```

NOTE

- **dev_loss_tmo** and **fast_io_fail_tmo** specify the retry time and switchover time in the event of a link fault. The preceding example provides recommended values for these two parameters, and you can modify them according to your own requirements.
- **no_path_retry** specifies the retry policy if all paths of a LUN are faulty. The preceding retry time is a recommended value and you can modify it according to your own requirements.
- In RHEL 8 and later versions, due to changes to the kernel parameters, the status displayed by the **multipath -ll** command may not be updated in the event of a path fault. You are advised to add **detect_checker no** to the **device** field.
- After modifying **multipath.conf**, run **/etc/init.d/multipathd restart** or **systemctl restart multipathd.service** to restart the multipath service for the modification to take effect.

Starting the Multipathing Software

After configuring the configuration file, run the following command on the host to start the DM-Multipath process on RHEL 6:

```
/etc/init.d/multipathd start
```

For RHEL 7 and RHEL 8, run the following command to start the DM-Multipath process:

```
systemctl start multipathd.service
```

Setting the Multipathing Software to Run at System Startup

For RHEL 6, run the following command to run the multipathing software at startup:

```
chkconfig multipathd on
```

For RHEL 7 and RHEL 8, run the following command:

```
systemctl enable multipathd.service
```


7.6.3.3 Verification

Verifying the Load Balancing Mode

Run the **multipath -ll** command to verify that the configuration has taken effect. In load balancing mode, all paths are active. The following is an example.

```
[root@localhost ~]# multipath -ll
mpathaf (361603041002d0306003e6dc300000009) dm-9 HUAWEI  ,XSG1
size=5.0G features='0' hwhandler='0' wp=rw
`-+- policy='round-robin 0' prio=1 status=active
  |- 2:0:2:4 sde  8:64   active ready running
  |- 9:0:2:4 sdq  65:0   active ready running
  |- 2:0:3:4 sdaw 67:0   active ready running
  |- 9:0:3:4 sdas 66:192 active ready running
  |- 2:0:0:4 sdi  8:128  active ready running
  |- 9:0:0:4 sdak 66:64  active ready running
  |- 2:0:1:4 sdo  8:224  active ready running
  `- 9:0:1:4 sdao 66:128 active ready running
mpathae (361603041002d0306003e549f00000000) dm-3 HUAWEI  ,XSG1
size=50G features='0' hwhandler='0' wp=rw
`-+- policy='round-robin 0' prio=1 status=active
  |- 2:0:2:1 sdb  8:16   active ready running
  |- 9:0:2:1 sdm  8:192  active ready running
  |- 2:0:3:1 sdat 66:208 active ready running
  |- 9:0:3:1 sdap 66:144 active ready running
  |- 2:0:0:1 sdf  8:80   active ready running
  |- 9:0:0:1 sdah 66:16  active ready running
  |- 2:0:1:1 sdj  8:144  active ready running
  `- 9:0:1:1 sdal 66:80  active ready running
```

Verifying the Local Preferred Mode

Run the **multipath -ll** command to verify that the configuration has taken effect. In local preferred mode, **status=active** corresponds to the preferred paths on the local storage system, and **status=enabled** corresponds to the non-preferred paths on the remote storage system. The following command output indicates that the configuration has taken effect. Generally, the **prio** value of a preferred path on a Linux system is **50**, and that of a non-preferred path is **10**. The following is an example:

```
[root@localhost ~]# multipath -ll
mpathaf (361603041002d0306003e6dc300000009) dm-9 HUAWEI  ,XSG1
size=5.0G features='0' hwhandler='0' wp=rw
|-+- policy='round-robin 0' prio=50 status=active
| |- 2:0:2:4 sdak 66:64  active ready running
| |- 9:0:2:4 sdba 67:64  active ready running
| |- 2:0:3:4 sdao 66:128 active ready running
| |- 9:0:3:4 sdbe 67:128 active ready running
`-+- policy='round-robin 0' prio=10 status=enabled
  |- 2:0:0:4 sdh  8:112  active ready running
  |- 9:0:0:4 sdi  8:128  active ready running
  |- 2:0:1:4 sdp  8:240  active ready running
  |- 9:0:1:4 sdq  65:0   active ready running
```

7.6.4 Solaris

7.6.4.1 Storage System Configuration

If the OS native multipathing software is used, retain the default settings of the initiator and configure **Host Access Mode** and **Preferred Path for HyperMetro** as required. **Table 7-15** lists the detailed settings.

Table 7-15 Configurations of storage systems earlier than 6.1.3 for interconnection with Solaris application servers

HyperMetro Working Mode	Storage System	OS Setting	Host Access Mode	Preferred Path for HyperMetro	Description
Load balancing mode	Local storage	Solaris	Asymmetric	Yes	The host uses all paths of a disk with equal priority.
	Remote storage	Solaris	Asymmetric	Yes	
Local preferred mode	Local storage	Solaris	Asymmetric	Yes	The host considers the paths from the local storage system as preferred paths, and those from the remote storage system as non-preferred paths.
	Remote storage	Solaris	Asymmetric	No	

Table 7-16 Configurations of storage systems 6.1.3 or later for interconnection with Solaris application servers

HyperMetro Working Mode	Storage System	OS Setting	Host Access Mode	Preferred Path for HyperMetro	Description
Load balancing mode	Local storage	Solaris	Load balancing	N/A	The host uses all paths of a disk with equal priority.
	Remote storage	Solaris	Load balancing	N/A	
Local preferred mode	Local storage	Solaris	Asymmetric	Yes	The host considers the paths from the local storage system as preferred paths, and those from the remote storage system as non-preferred paths.
	Remote storage	Solaris	Asymmetric	No	

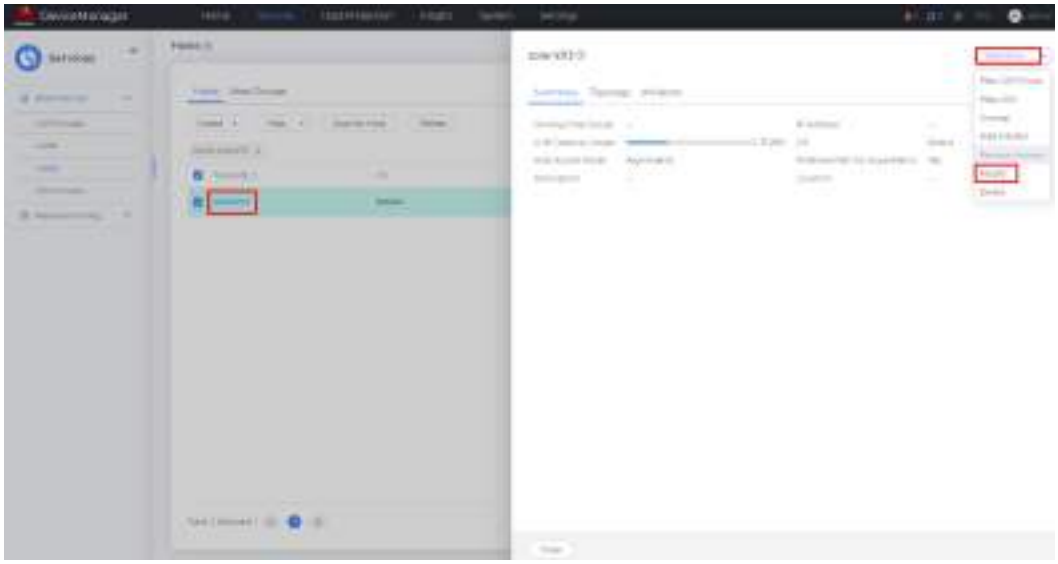
NOTICE

- For details about the Solaris versions, see the **Huawei Storage Interoperability Navigator**.
- If a LUN has been mapped to a host, you must restart the host for the configuration to take effect after you modify **Host Access Mode** or **Preferred Path for HyperMetro**. If you map the LUN for the first time, restart is not needed.
- When data is migrated from other Huawei storage systems (including OceanStor Dorado V3, OceanStor V3, and OceanStor V5) to 6.x series storage systems, configure the storage system by following instructions in "FAQs" in the ***Host Connectivity Guide***.

Configuring the Load Balancing Mode on Storage Systems Earlier Than 6.1.3

Step 1 Click the host name and choose **Operation** > **Modify**.

Figure 7-51 Modifying the host properties

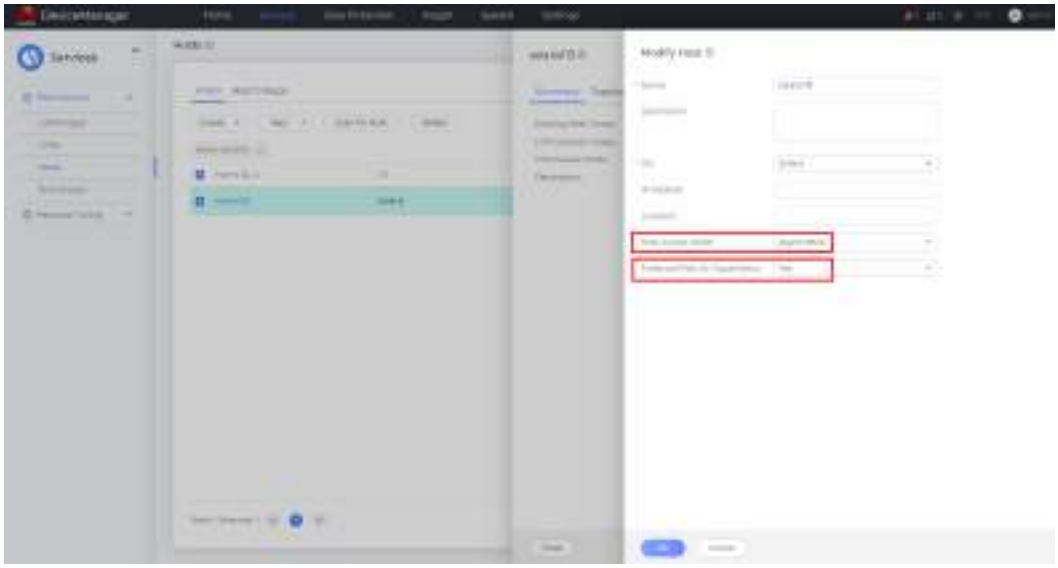


NOTE

The information displayed on the GUI may vary slightly with the product version.

Step 2 Set **Host Access Mode** to **Asymmetric** and **Preferred Path for HyperMetro** to **Yes** for both the local and remote storage systems.

Figure 7-52 Settings on the local and remote storage systems

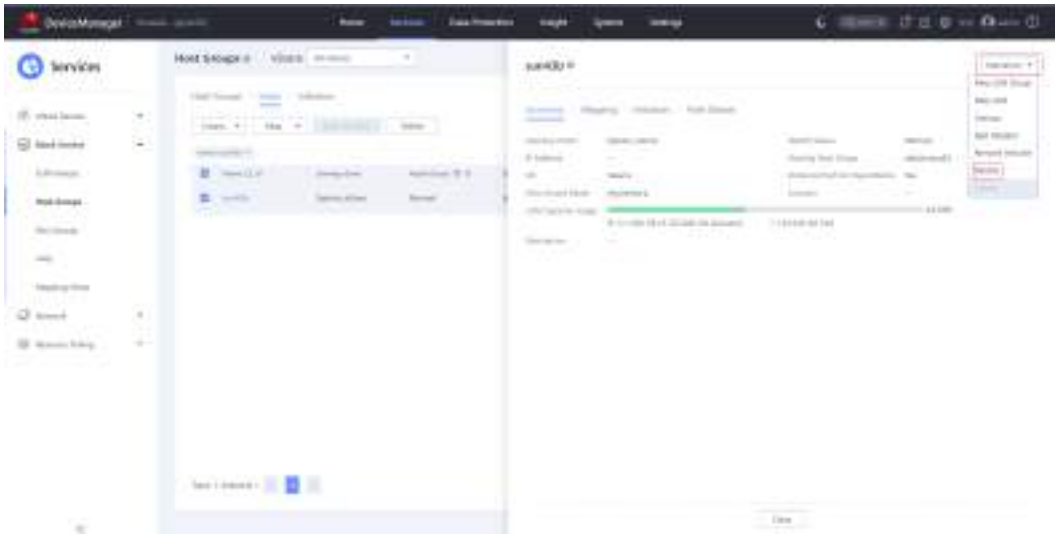


----End

Configuring the Load Balancing Mode on Storage Systems 6.1.3 and Later

Step 1 Click the host name and choose **Operation** > **Modify**.

Figure 7-53 Modifying the host properties

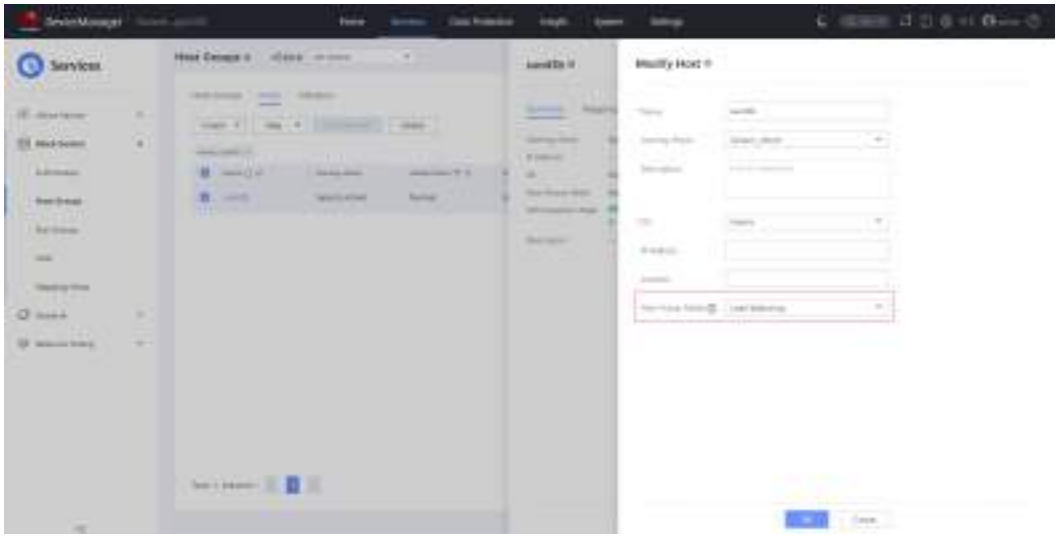


NOTE

The information displayed on the GUI may vary slightly with the product version.

Step 2 Set **Host Access Mode** to **Load balancing** for both the local and remote storage systems.

Figure 7-54 Settings on the local and remote storage systems

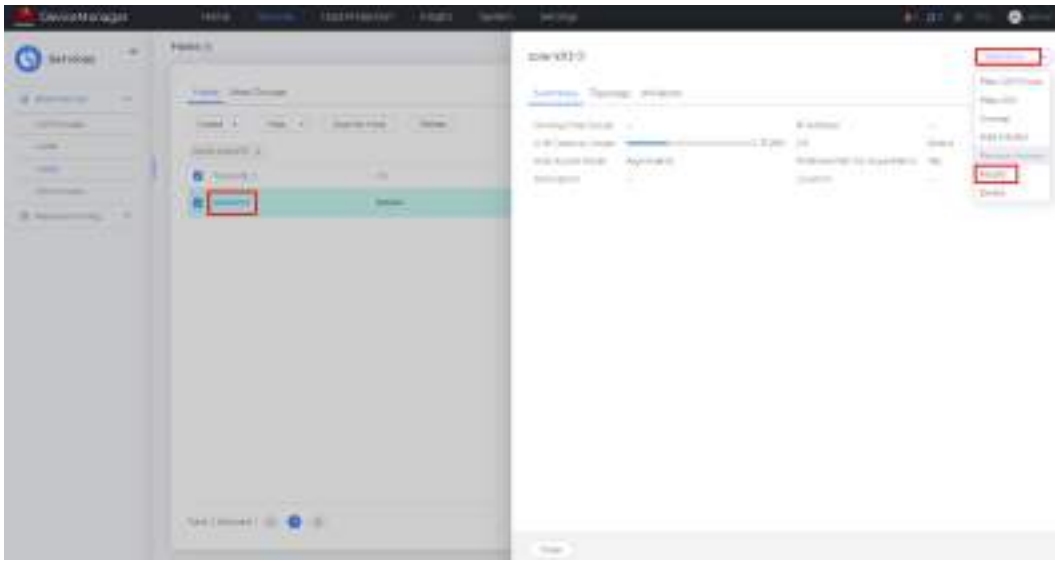


----End

Configuring the Local Preferred Mode

Step 1 Click the host name and choose **Operation** > **Modify**.

Figure 7-55 Modifying the host properties



NOTE

The information displayed on the GUI may vary slightly with the product version.

Step 2 For the local storage system, set **Host Access Mode** to **Asymmetric** and **Preferred Path for HyperMetro** to **Yes**. For the remote storage system, set **Host Access Mode** to **Asymmetric** and **Preferred Path for HyperMetro** to **No**.

Figure 7-56 Settings on the local storage system

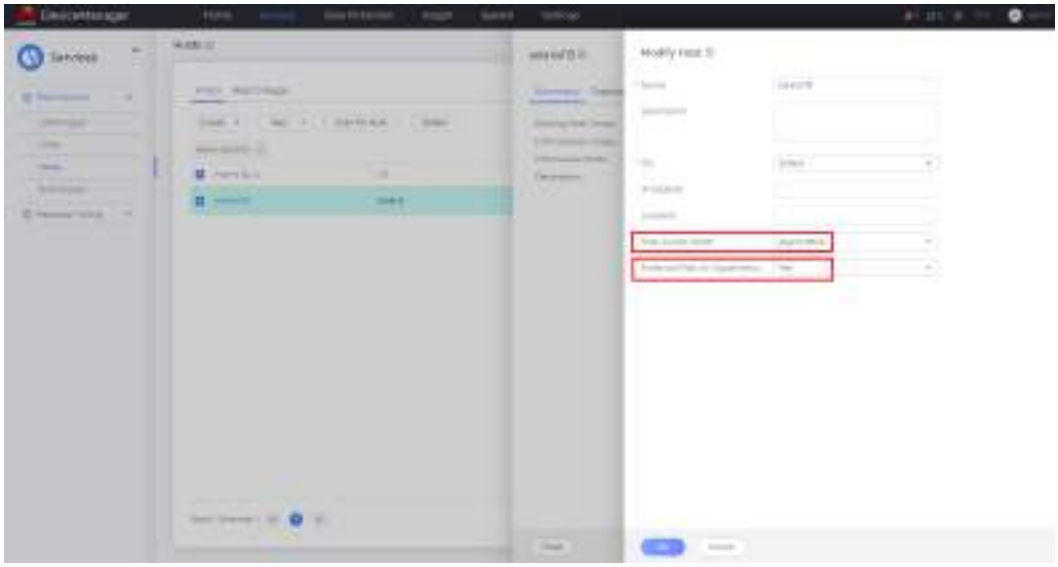
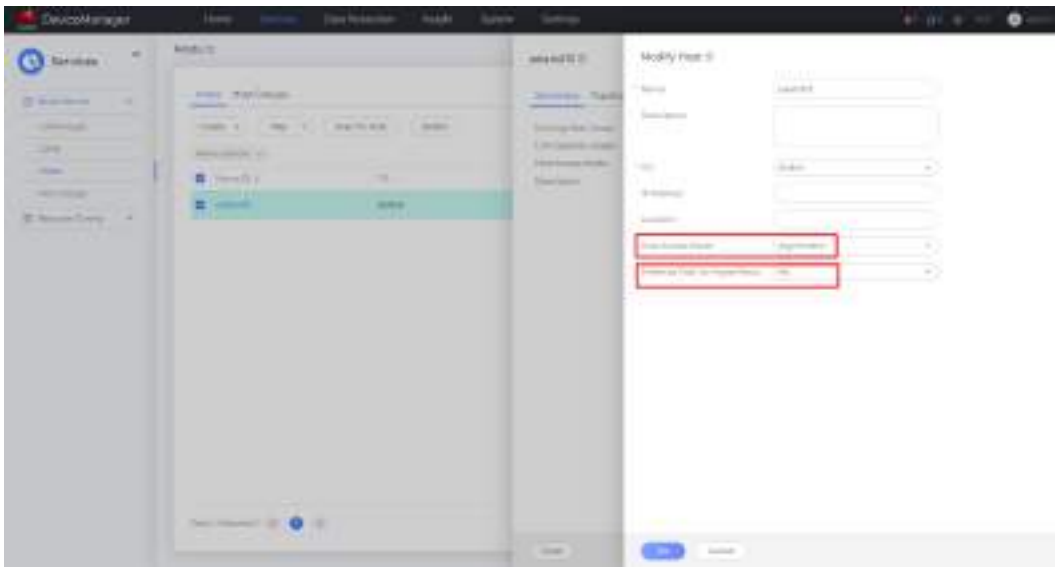


Figure 7-57 Settings on the remote storage system



----End

7.6.4.2 Host Configuration

Solaris 10

In Solaris 10, the multipathing software has been installed by default, but is not enabled.

After **Host Access Mode** is set to **Asymmetric** on the storage systems, run the **stmsboot -D fp -e** command on the host to enable the multipathing software. You do not need to configure the software on the host. For storage systems of 6.1.3 and later versions, **Host Access Mode** is **Load balancing**, and the **scsi_vhci.conf** configuration file of the host must be modified by following

instructions in "How Can I Modify the Multipathing Configuration File scsi_vhci.conf?" in the ***Host Connectivity Guide***.

CAUTION

For storage systems earlier than 6.1.3, comment out the vendor ID and product ID of Huawei storage in the **scsi_vhci.conf** configuration file. For storage systems of 6.1.3 and later versions, add the vendor ID and product ID of Huawei storage to the **scsi_vhci.conf** configuration file. For details, see "How Can I Modify the Multipathing Configuration File scsi_vhci.conf?" in the ***Host Connectivity Guide***.

The following is an example:

```
bash-3.2# stmsboot -D fp -e
WARNING: This operation will require a reboot.
Do you want to continue ? [y/n] (default: y) y
The changes will come into effect after rebooting the system.
Reboot the system now ? [y/n] (default: y) y
updating /platform/sun4u/boot_archive
```

NOTICE

The host restarts after the preceding operation is performed.

After the host restarts, the following LUN information is displayed.

```
bash-3.2# format
 Searching for disks...done


AVAILABLE DISK SELECTIONS:
       0. c0t60102031000405770 01ACD6C00000025d0 <HUAWEI-XSG1-6000 cyl 11700 alt 2 hd 224 sec
56>
          /scsi_vhci/ssd@g60102031000405770 01acd6c00000025
       1. c2t0d0 <drive type unknown>
          /pci@0/pci@0/pci@2/scsi@0/sd@0,0
       2. c2t1d0 <drive type unknown>
          /pci@0/pci@0/pci@2/scsi@0/sd@1,0
       3. c2t2d0 <drive type unknown>
          /pci@0/pci@0/pci@2/scsi@0/sd@2,0
       4. c2t3d0 <SEAGATE-ST914602SSUN146G-0603 cyl 14087 alt 2 hd 24 sec 848>
          /pci@0/pci@0/pci@2/scsi@0/sd@3,0
       5. c2t4d0 <drive type unknown>
          /pci@0/pci@0/pci@2/scsi@0/sd@4,0
       6. c2t5d0 <drive type unknown>
          /pci@0/pci@0/pci@2/scsi@0/sd@5,0
       7. c2t6d0 <drive type unknown>
          /pci@0/pci@0/pci@2/scsi@0/sd@6,0
Specify disk (enter its number):
```

NOTE

The path format is **scsi_vhci**, indicating that this path an aggregation of multiple paths.

Solaris 11

When **Host Access Mode** is **Asymmetric** on the storage systems, the method for configuring Solaris 11 is the same as that for Solaris 10. For details, see **Solaris 10**.

7.6.4.3 Verification

Verifying the Load Balancing Mode on Storage Systems Earlier Than 6.1.3

After the LUNs have been mapped to the host, scan the LUNs on the host and verify that the number and status of the preferred paths are correct. The following is an example:

```
bash-3.2# mpathadm show lu /dev/rdsk/c0t60102031000405770001ACD6C00000025d0s2
Logical Unit:  /dev/rdsk/c0t60102031000405770001ACD6C00000025d0s2
        mpath-support:  libmpscsi_vhci.so
        Vendor:  HUAWEI
        Product:  XSG1
        Revision:  6000
        Name Type:  unknown type
        Name:  60102031000405770001acd6c00000025
        Asymmetric:  yes
        Current Load Balance:  round-robin
        Logical Unit Group ID:  NA
        Auto Failback:  on
        Auto Probing:  NA

        Paths:
                Initiator Port Name:  2100000e1e1a9b30
                Target Port Name:  2991010203040577
                Override Path:  NA
                Path State:  OK
                Disabled:  no

                Initiator Port Name:  2100000e1e1a9b31
                Target Port Name:  2991010203040577
                Override Path:  NA
                Path State:  OK
                Disabled:  no

                Initiator Port Name:  2100000e1e1a9b31
                Target Port Name:  201016212c374217
                Override Path:  NA
                Path State:  OK
                Disabled:  no

                Initiator Port Name:  2100000e1e1a9b31
                Target Port Name:  201116212c374217
                Override Path:  NA
                Path State:  OK
                Disabled:  no

                Initiator Port Name:  2100000e1e1a9b30
                Target Port Name:  201016212c374217
                Override Path:  NA
                Path State:  OK
                Disabled:  no

                Initiator Port Name:  2100000e1e1a9b30
                Target Port Name:  201116212c374217
                Override Path:  NA
                Path State:  OK
                Disabled:  no

                Initiator Port Name:  2100000e1e1a9b31
                Target Port Name:  200016212c374217
                Override Path:  NA
                Path State:  OK
                Disabled:  no

                Initiator Port Name:  2100000e1e1a9b30
                Target Port Name:  200016212c374217
                Override Path:  NA
```



```
        Path State:  OK
        Disabled:  no

        Initiator Port Name:  2100000e1e1a9b30
        Target Port Name:  28b0010203040577
        Override Path:  NA
        Path State:  OK
        Disabled:  no

        Initiator Port Name:  2100000e1e1a9b30
        Target Port Name:  2990010203040577
        Override Path:  NA
        Path State:  OK
        Disabled:  no

        Initiator Port Name:  2100000e1e1a9b30
        Target Port Name:  200116212c374217
        Override Path:  NA
        Path State:  OK
        Disabled:  no

        Initiator Port Name:  2100000e1e1a9b30
        Target Port Name:  28b1010203040577
        Override Path:  NA
        Path State:  OK
        Disabled:  no

        Initiator Port Name:  2100000e1e1a9b31
        Target Port Name:  28b0010203040577
        Override Path:  NA
        Path State:  OK
        Disabled:  no

        Initiator Port Name:  2100000e1e1a9b31
        Target Port Name:  200116212c374217
        Override Path:  NA
        Path State:  OK
        Disabled:  no

        Initiator Port Name:  2100000e1e1a9b31
        Target Port Name:  28b1010203040577
        Override Path:  NA
        Path State:  OK
        Disabled:  no

        Initiator Port Name:  2100000e1e1a9b31
        Target Port Name:  2990010203040577
        Override Path:  NA
        Path State:  OK
        Disabled:  no

    Target Port Groups:
        ID:  1
        Explicit Failover:  no
        Access State:  active optimized
        Target Ports:
            Name:  2991010203040577
            Relative ID:  8

            Name:  28b0010203040577
            Relative ID:  3

            Name:  2990010203040577
            Relative ID:  2

            Name:  28b1010203040577
            Relative ID:  12

        ID:  2
```

```
        Explicit Failover:  no
        Access State:  active optimized
        Target Ports:
            Name:  201016212c374217
            Relative ID:  8197

            Name:  201116212c374217
            Relative ID:  8202

            Name:  200016212c374217
            Relative ID:  8198

            Name:  200116212c374217
            Relative ID:  8201
bash-3.2#
```

In the command output:

- The value of **Asymmetric** is **yes**, indicating that the storage system is in asymmetric mode.
- If **Access State** is **active optimized**, the path is a preferred path.

In this example, there are eight target ports (**2991010203040577**, **28b0010203040577**, **2990010203040577**, **28b1010203040577**, **201016212c374217**, **201116212c374217**, **200016212c374217**, and **200116212c374217**) and 16 paths, which are all preferred paths and are consistent with the actual configuration. The configuration is successful.

Verifying the Load Balancing Mode on Storage Systems 6.1.3 and Later

After the LUNs have been mapped to the host, scan the LUNs on the host and verify that the number and status of the preferred paths are correct. The following is an example:

```
bash-3.2# mpathadm show lu /dev/rdsk/c0t60102031000405770001ACD6C00000025d0s2
Logical Unit:  /dev/rdsk/c0t60102031000405770001ACD6C00000025d0s2
    mpath-support:  libmpscsi_vhci.so
    Vendor:  HUAWEI
    Product:  XSG1
    Revision:  6000
    Name Type:  unknown type
    Name:  60102031000405770001acd6c00000025
    Asymmetric:  no
    Current Load Balance:  round-robin
    Logical Unit Group ID:  NA
    Auto Failback:  on
    Auto Probing:  NA

    Paths:
        Initiator Port Name:  2100000e1e1a9b30
        Target Port Name:  2991010203040577
        Override Path:  NA
        Path State:  OK
        Disabled:  no

        Initiator Port Name:  2100000e1e1a9b31
        Target Port Name:  2991010203040577
        Override Path:  NA
        Path State:  OK
        Disabled:  no

        Initiator Port Name:  2100000e1e1a9b31
        Target Port Name:  201016212c374217
        Override Path:  NA
        Path State:  OK
```



```
Disabled:  no

Initiator Port Name:  2100000e1e1a9b31
Target Port Name:  201116212c374217
Override Path:  NA
Path State:  OK
Disabled:  no

Initiator Port Name:  2100000e1e1a9b30
Target Port Name:  201016212c374217
Override Path:  NA
Path State:  OK
Disabled:  no

Initiator Port Name:  2100000e1e1a9b30
Target Port Name:  201116212c374217
Override Path:  NA
Path State:  OK
Disabled:  no

Initiator Port Name:  2100000e1e1a9b31
Target Port Name:  200016212c374217
Override Path:  NA
Path State:  OK
Disabled:  no

Initiator Port Name:  2100000e1e1a9b30
Target Port Name:  200016212c374217
Override Path:  NA
Path State:  OK
Disabled:  no

Initiator Port Name:  2100000e1e1a9b30
Target Port Name:  28b0010203040577
Override Path:  NA
Path State:  OK
Disabled:  no

Initiator Port Name:  2100000e1e1a9b30
Target Port Name:  2990010203040577
Override Path:  NA
Path State:  OK
Disabled:  no

Initiator Port Name:  2100000e1e1a9b30
Target Port Name:  200116212c374217
Override Path:  NA
Path State:  OK
Disabled:  no

Initiator Port Name:  2100000e1e1a9b30
Target Port Name:  28b1010203040577
Override Path:  NA
Path State:  OK
Disabled:  no

Initiator Port Name:  2100000e1e1a9b31
Target Port Name:  28b0010203040577
Override Path:  NA
Path State:  OK
Disabled:  no

Initiator Port Name:  2100000e1e1a9b31
Target Port Name:  200116212c374217
Override Path:  NA
Path State:  OK
Disabled:  no

Initiator Port Name:  2100000e1e1a9b31
```

```
            Target Port Name:  28b1010203040577
            Override Path:  NA
            Path State:  OK
            Disabled:  no

            Initiator Port Name:  2100000e1e1a9b31
            Target Port Name:  2990010203040577
            Override Path:  NA
            Path State:  OK
            Disabled:  no

      Target Port Groups:
            ID:  1
            Explicit Failover:  no
            Access State:  active optimized
            Target Ports:
                  Name:  2991010203040577
                  Relative ID:  8

                  Name:  28b0010203040577
                  Relative ID:  3

                  Name:  2990010203040577
                  Relative ID:  2

                  Name:  28b1010203040577
                  Relative ID:  12

            ID:  2
            Explicit Failover:  no
            Access State:  active optimized
            Target Ports:
                  Name:  201016212c374217
                  Relative ID:  8197

                  Name:  201116212c374217
                  Relative ID:  8202

                  Name:  200016212c374217
                  Relative ID:  8198

                  Name:  200116212c374217
                  Relative ID:  8201
bash-3.2#
```

In the command output:

- The value of **Asymmetric** is **no**, indicating that the storage system is in load balancing mode.
- If **Access State** is **active optimized**, the path is a preferred path.

In this example, there are eight target ports (**2991010203040577**, **28b0010203040577**, **2990010203040577**, **28b1010203040577**, **201016212c374217**, **201116212c374217**, **200016212c374217**, and **200116212c374217**) and 16 paths, which are all preferred paths and are consistent with the actual configuration. The configuration is successful.

Verifying the Local Preferred Mode

After the LUNs have been mapped to the host, scan the LUNs on the host and verify that the numbers and status of the preferred and non-preferred paths are correct. The following is an example:

```
root@S113:~# mpathadm show lu /dev/rdsk/c0t60102031000405770 01ACD6C00000025d0s2
Logical Unit:  /dev/rdsk/c0t60102031000405770 01ACD6C00000025d0s2
```



```
mpath-support:  libmpscsi_vhci.so
Vendor:  HUAWEI
Product:  XSG1
Revision:  6000
Name Type:  unknown type
Name:  60102031000405770 01acd6c00000025
Asymmetric:  yes
Current Load Balance:  round-robin
Logical Unit Group ID:  NA
Auto Failback:  on
Auto Probing:  NA

Paths:
    Initiator Port Name:  2100000e1e1a9b30
    Target Port Name:  2991010203040577
    Override Path:  NA
    Path State:  OK
    Disabled:  no

    Initiator Port Name:  2100000e1e1a9b31
    Target Port Name:  2991010203040577
    Override Path:  NA
    Path State:  OK
    Disabled:  no

    Initiator Port Name:  2100000e1e1a9b30
    Target Port Name:  201116212c374217
    Override Path:  NA
    Path State:  OK
    Disabled:  no

    Initiator Port Name:  2100000e1e1a9b31
    Target Port Name:  201016212c374217
    Override Path:  NA
    Path State:  OK
    Disabled:  no

    Initiator Port Name:  2100000e1e1a9b31
    Target Port Name:  201116212c374217
    Override Path:  NA
    Path State:  OK
    Disabled:  no

    Initiator Port Name:  2100000e1e1a9b31
    Target Port Name:  200016212c374217
    Override Path:  NA
    Path State:  OK
    Disabled:  no

    Initiator Port Name:  2100000e1e1a9b31
    Target Port Name:  200116212c374217
    Override Path:  NA
    Path State:  OK
    Disabled:  no

    Initiator Port Name:  2100000e1e1a9b31
    Target Port Name:  2990010203040577
    Override Path:  NA
    Path State:  OK
    Disabled:  no

    Initiator Port Name:  2100000e1e1a9b30
    Target Port Name:  201016212c374217
    Override Path:  NA
    Path State:  OK
    Disabled:  no

    Initiator Port Name:  2100000e1e1a9b30
    Target Port Name:  28b0010203040577
```



```
        Override Path:  NA
        Path State:  OK
        Disabled:  no

        Initiator Port Name:  2100000e1e1a9b31
        Target Port Name:  28b1010203040577
        Override Path:  NA
        Path State:  OK
        Disabled:  no

        Initiator Port Name:  2100000e1e1a9b31
        Target Port Name:  28b0010203040577
        Override Path:  NA
        Path State:  OK
        Disabled:  no

        Initiator Port Name:  2100000e1e1a9b30
        Target Port Name:  200016212c374217
        Override Path:  NA
        Path State:  OK
        Disabled:  no

        Initiator Port Name:  2100000e1e1a9b30
        Target Port Name:  28b1010203040577
        Override Path:  NA
        Path State:  OK
        Disabled:  no

        Initiator Port Name:  2100000e1e1a9b30
        Target Port Name:  200116212c374217
        Override Path:  NA
        Path State:  OK
        Disabled:  no

        Initiator Port Name:  2100000e1e1a9b30
        Target Port Name:  2990010203040577
        Override Path:  NA
        Path State:  OK
        Disabled:  no

    Target Port Groups:
        ID:  1
        Explicit Failover:  no
        Access State:  active optimized
        Target Ports:
            Name:  2991010203040577
            Relative ID:  8

            Name:  2990010203040577
            Relative ID:  2

            Name:  28b0010203040577
            Relative ID:  3

            Name:  28b1010203040577
            Relative ID:  12

        ID:  2
        Explicit Failover:  no
        Access State:  active not optimized
        Target Ports:
            Name:  201116212c374217
            Relative ID:  8202

            Name:  201016212c374217
            Relative ID:  8197

            Name:  200016212c374217
            Relative ID:  8198
```



```
                Name:  200116212c374217
                Relative ID:  8201
root@S113:~#
```

In the command output:

- The value of **Asymmetric** is **yes**, indicating that the storage system is in asymmetric mode.
- If **Access State** is **active optimized**, the path is a preferred path.
- If **Access State** is **active not optimized**, the path is a non-preferred path.

In this example, there are four target ports (**2991010203040577**, **2990010203040577**, **28b0010203040577**, and **28b1010203040577**) and eight preferred paths from the local storage system, and another four target ports (**201116212c374217**, **201016212c374217**, **200016212c374217**, and **200116212c374217**) and eight non-preferred paths from the remote storage system. The number of paths is consistent with the actual configuration. The configuration is successful.

7.6.5 SUSE

7.6.5.1 Storage System Configuration

If the OS native multipathing software is used, retain the default settings of the initiator and configure **Host Access Mode** and **Preferred Path for HyperMetro** as required. **Table 7-17** lists the detailed settings.

Table 7-17 Storage configurations for interconnection with SUSE application servers

HyperMetro Working Mode	Storage System	OS Setting	Host Access Mode	Preferred Path for HyperMetro	Description
Load balancing mode	Local storage	Linux	Load balancing	N/A	The host uses all paths of a disk with equal priority.
	Remote storage	Linux	Load balancing	N/A	
Local preferred mode	Local storage	Linux	Asymmetric	Yes	The host considers the paths from the local storage system as preferred paths, and those from the remote storage system as non-preferred paths.
	Remote storage	Linux	Asymmetric	No	

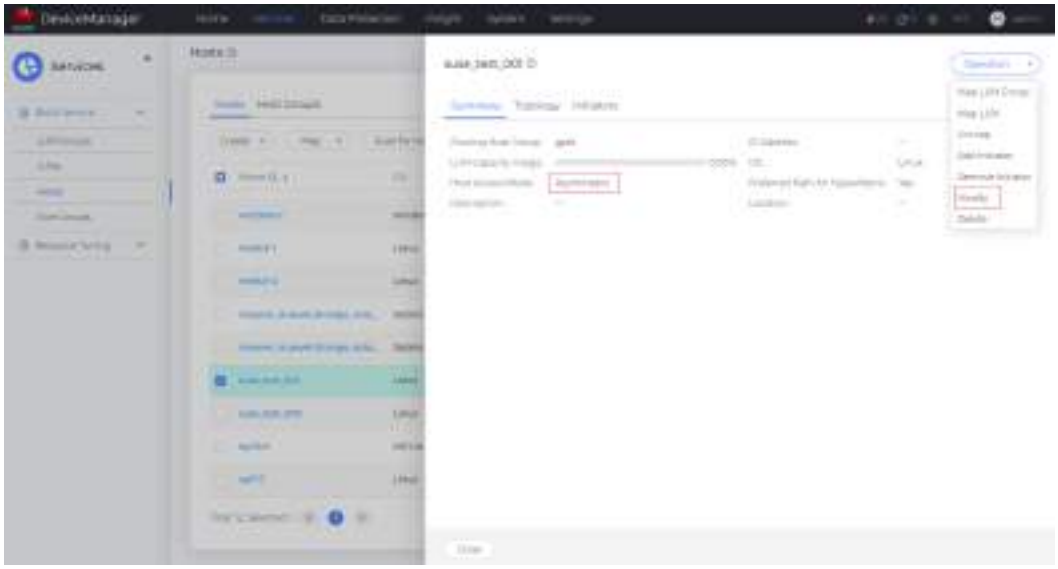
NOTICE

- For details about the SUSE versions, see the **Huawei Storage Interoperability Navigator**.
- If a LUN has been mapped to a host, you must restart the host for the configuration to take effect after you modify **Host Access Mode** or **Preferred Path for HyperMetro**. If you map the LUN for the first time, restart is not needed.
- When data is migrated from other Huawei storage systems (including OceanStor Dorado V3, OceanStor V3, and OceanStor V5) to 6.x series storage systems, configure the storage system by following instructions in "FAQs" in the ***Host Connectivity Guide***.

Configuring the Load Balancing Mode

Step 1 Click the host name and choose **Operation** > **Modify**.

Figure 7-58 Modifying the host properties

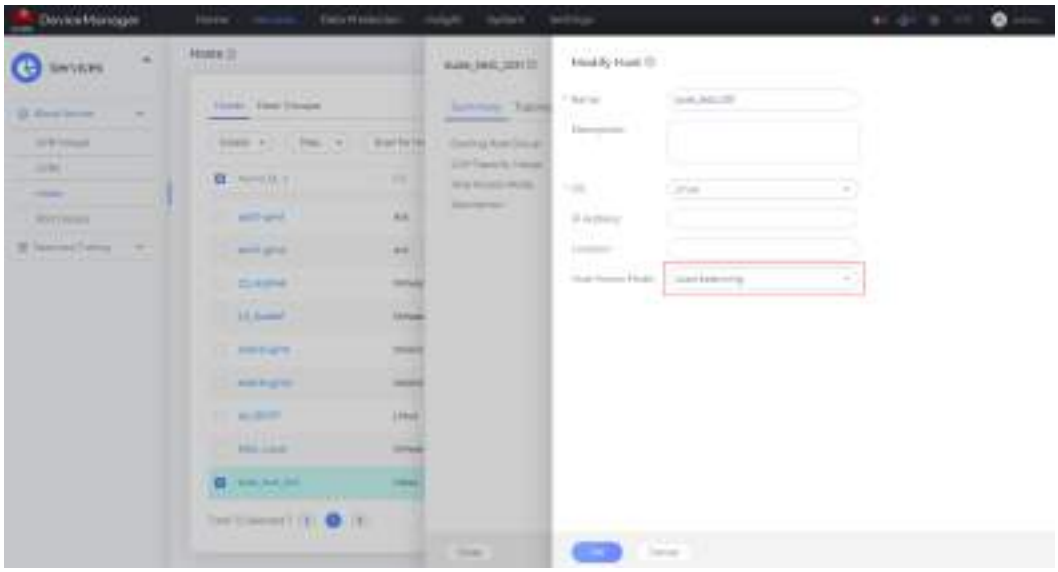


NOTE

The information displayed on the GUI may vary slightly with the product version.

Step 2 Set **Host Access Mode** to **Load balancing** for both the local and remote storage systems.

Figure 7-59 Setting the host access mode

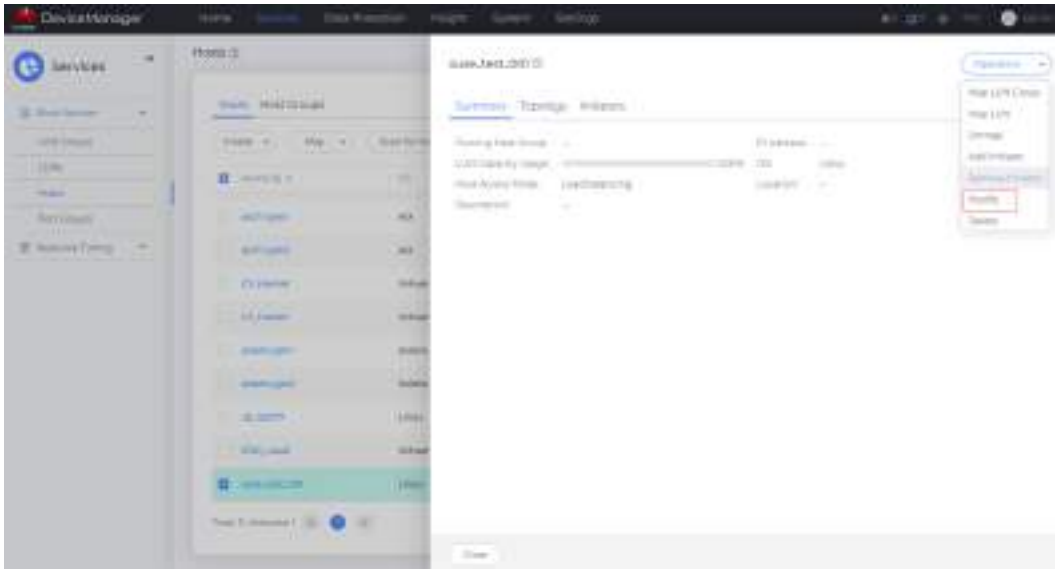


----End

Configuring the Local Preferred Mode

Step 1 Click the host name and choose **Operation** > **Modify**.

Figure 7-60 Modifying the host properties



NOTE

The information displayed on the GUI may vary slightly with the product version.

Step 2 For the local storage system, set **Host Access Mode** to **Asymmetric** and **Preferred Path for HyperMetro** to **Yes**. For the remote storage system, set **Host Access Mode** to **Asymmetric** and **Preferred Path for HyperMetro** to **No**.

Figure 7-61 Settings on the local storage system

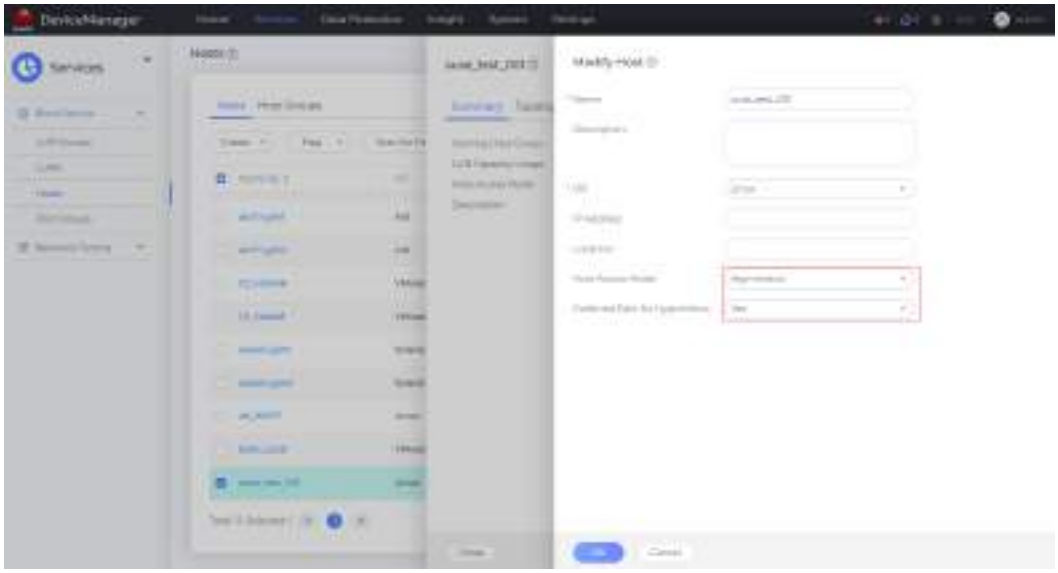
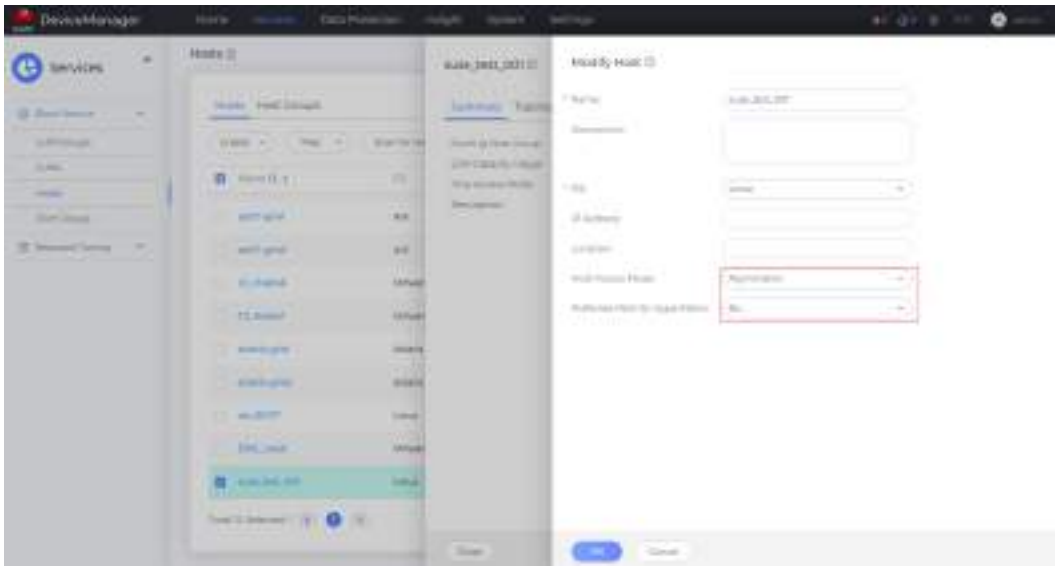


Figure 7-62 Settings on the remote storage system



----End

7.6.5.2 Host Configuration

Installing Multipathing Software

Generally, multipathing software packages in SUSE are rpm packages starting with **device-mapper** or **multipath-tools**, and are installed by default. To install the software manually, upload the software package to the server and use the **rpm** command to install it. The following is an example.

```
linux-x8bt:~ # rpm -qa | grep device-mapper*
device-mapper-1.02.149-8.16.x86_64
device-mapper-32bit-1.02.149-8.16.x86_64
linux-x8bt:~ #
```



```
linux-x8bt:~ # rpm -qa | grep multipath*
multipath-tools-0.7.3+102+suse.fb43a08-1.3.x86_64
```

Modifying the Configuration File

DM-Multipath's most important configuration file is **/etc/multipath.conf**.

Some operating systems have this file by default. If your operating system does not have this file, you can copy the **multipath.conf.synthetic** file to the **/etc** directory to generate one. The following is an example.

```
linux-x8bt:~ # cp /usr/share/doc/packages/multipath-tools/multipath.conf.synthetic /etc/multipath.conf
```

If the system does not have a template, run the **/sbin/mpathconf --enable** command to manually generate **/etc/multipath.conf**.

If **Host Access Mode** is set to **Load balancing** on the storage system, add the following content to the **devices** field in the **/etc/multipath.conf** file:

```
devices {
    device {
        vendor                "HUAWEI"
        product               "XSG1"
        path_grouping_policy    multibus
        path_checker            tur
        prio                  const
        path_selector           "round-robin 0"
        failback              immediate
        dev_loss_tmo            30
        fast_io_fail_tmo        5
        no_path_retry           15
}
}
```

If **Host Access Mode** is set to **Asymmetric** on the storage system, add the following content to the **devices** field in the **/etc/multipath.conf** file:

```
devices {
    device {
        vendor                "HUAWEI"
        product               "XSG1"
        path_grouping_policy    group_by_prio
        path_checker            tur
        prio                  alua
        path_selector           "round-robin 0"
        failback              immediate
        dev_loss_tmo            30
        fast_io_fail_tmo        5
        no_path_retry           15
}
}
```


NOTE

- **dev_loss_tmo** and **fast_io_fail_tmo** specify the retry time and switchover time in the event of a link fault. The preceding example provides recommended values for these two parameters, and you can modify them according to your own requirements.
- You are advised to blacklist the WWID of the host's system disk. Otherwise, the system disk may be taken over by multipathing software, resulting in system startup exceptions. For details about how to blacklist WWIDs, see the following link: **https://documentation.suse.com/sles/12-SP4/html/SLES-all/cha-multipath.html#sec-multipath-blacklist**.
- **no_path_retry** specifies the retry policy if all paths of a LUN are faulty. The preceding retry time is a recommended value and you can modify it according to your own requirements.
- In SLES 12 SP3, SLES 15, and later versions, due to changes to the kernel parameters, the status displayed by the **multipath -ll** command may not be updated in the event of a path fault. You are advised to add **detect_checker no** to the **device** field.
- After modifying **multipath.conf**, run **/etc/init.d/multipathd restart** or **systemctl restart multipathd.service** to restart the multipath service for the modification to take effect.

Starting the Multipathing Software

After configuring the configuration file, run the following command on SLES 11 to start the multipath service:

```
/etc/init.d/multipathd start
```

For SLES 12 and 15, run the following command to start the multipath service:

```
systemctl start multipathd.service
```

Setting the Multipathing Software to Run at System Startup

After enabling the software, you can run the following command on SLES 11 to run the software at system startup:

```
chkconfig multipathd on
```

For SLES 12 and 15, run the following command:

```
systemctl enable multipathd
```

Rebuilding the Boot Image

For SLES 12 and 15, it is required to rebuild the boot image initrd whenever you enable or disable the multipath service. Otherwise, the system may not boot anymore. When enabling the multipath service, run the following command to rebuild the initrd:

```
dracut --force --add multipath
```

When disabling the multipath service, run the following command to rebuild the initrd:

```
dracut --force -o multipath
```


7.6.5.3 Verification

Verifying the Load Balancing Mode

Run the **multipath -ll** command to verify that the configuration has taken effect. In load balancing mode, all paths are active. The following is an example:

```
[root@localhost ~]# multipath -ll
mpathaf (361603041002d0306003e6dc300000009) dm-9 HUAWEI  ,XSG1
size=5.0G features='0' hwhandler='0' wp=rw
`-+- policy='round-robin 0' prio=1 status=active
  |- 2:0:2:4 sde  8:64   active ready running
  |- 9:0:2:4 sdq  65:0   active ready running
  |- 2:0:3:4 sdaw 67:0   active ready running
  |- 9:0:3:4 sdas 66:192 active ready running
  |- 2:0:0:4 sdi  8:128  active ready running
  |- 9:0:0:4 sdak 66:64  active ready running
  |- 2:0:1:4 sdo  8:224  active ready running
  `- 9:0:1:4 sdao 66:128 active ready running
mpathae (361603041002d0306003e549f00000000) dm-3 HUAWEI  ,XSG1
size=50G features='0' hwhandler='0' wp=rw
`-+- policy='round-robin 0' prio=1 status=active
  |- 2:0:2:1 sdb  8:16   active ready running
  |- 9:0:2:1 sdm  8:192  active ready running
  |- 2:0:3:1 sdat 66:208 active ready running
  |- 9:0:3:1 sdap 66:144 active ready running
  |- 2:0:0:1 sdf  8:80   active ready running
  |- 9:0:0:1 sdah 66:16  active ready running
  |- 2:0:1:1 sdj  8:144  active ready running
  `- 9:0:1:1 sdal 66:80  active ready running
```

Verifying the Local Preferred Mode

Run the **multipath -ll** command to verify that the configuration has taken effect. In local preferred mode, **status=active** corresponds to the preferred paths on the local storage system, and **status=enabled** corresponds to the non-preferred paths on the remote storage system. The following command output indicates that the configuration has taken effect. Generally, the **prio** value of preferred paths is **50** and that of non-preferred paths is **10** in Linux systems. The following is an example:

```
[root@localhost ~]# multipath -ll
mpathaf (361603041002d0306003e6dc300000009) dm-9 HUAWEI  ,XSG1
size=5.0G features='0' hwhandler='0' wp=rw
|-+- policy='round-robin 0' prio=50 status=active
| |- 2:0:2:4 sdak 66:64  active ready running
| |- 9:0:2:4 sdba 67:64  active ready running
| |- 2:0:3:4 sdao 66:128 active ready running
| |- 9:0:3:4 sdbe 67:128 active ready running
`-+- policy='round-robin 0' prio=10 status=enabled
  |- 2:0:0:4 sdh  8:112  active ready running
  |- 9:0:0:4 sdi  8:128  active ready running
  |- 2:0:1:4 sdp  8:240  active ready running
  |- 9:0:1:4 sdq  65:0   active ready running
```

7.6.6 VMware ESXi

7.6.6.1 Storage System Configuration

Recommended Storage Configuration

This section provides recommended configurations on HyperMetro storage systems for interconnection with VMware ESXi hosts using VMware NMP.

Table 7-18 Recommended configurations on 6.x series storage systems

HyperMetro Working Mode	Storage System	OS Setting	Host Access Mode	Preferred Path for HyperMetro	Description
Load balancing mode	Local storage	VMware ESXi	Load balancing	N/A	The host uses all paths of a disk with equal priority.
	Remote storage	VMware ESXi	Load balancing	N/A	
Local preferred mode	Local storage	VMware ESXi	Asymmetric	Yes	The host considers the paths from the local storage system as preferred paths, and those from the remote storage system as non-preferred paths.
	Remote storage	VMware ESXi	Asymmetric	No	

NOTICE

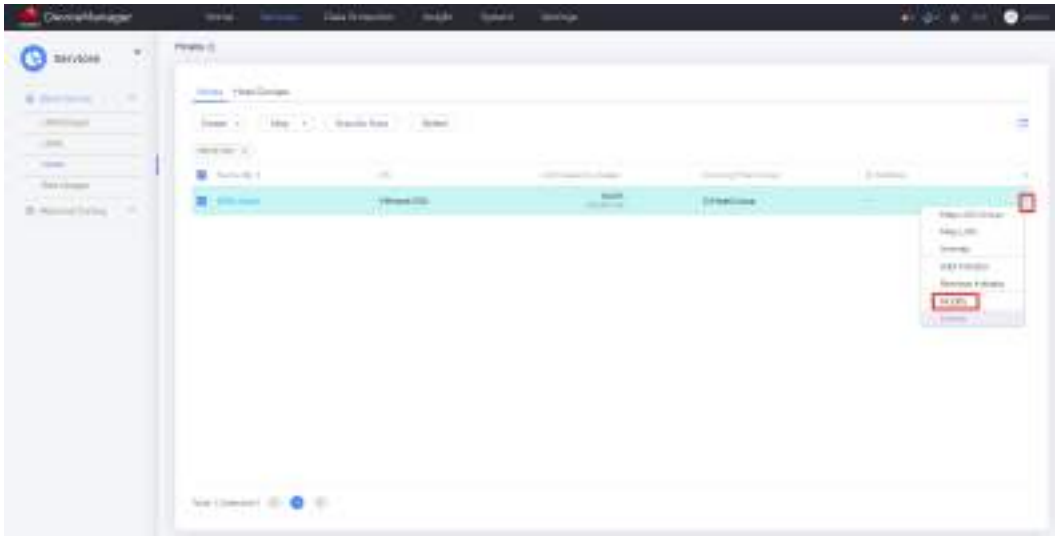
- Use the recommended configurations in **Table 7-18**. Other configurations may cause problems.
- If a LUN has been mapped to a host, you must restart the host for the configuration to take effect after you modify **Host Access Mode**. If you map the LUN for the first time, restart is not needed.
- When data is migrated from other Huawei storage systems (including OceanStor Dorado V3, OceanStor V3, and OceanStor V5) to 6.x series storage systems, configure the storage system by following instructions in "FAQs" in the ***Host Connectivity Guide***.
- When a LUN of a HyperMetro pair is mapped to all ESXi hosts in a cluster, the LUN must have the same host LUN ID on all of the hosts. You are advised to add all ESXi hosts in a cluster that are served by the same storage device to a host group and to the same mapping.

Configuring the Load Balancing Mode

Perform the following operations to configure the load balancing mode:

Step 1 On DeviceManager, choose **Services** > **Hosts**. Select the desired host, click ⋮ on the right, and choose **Modify**.

Figure 7-63 Modifying the host properties

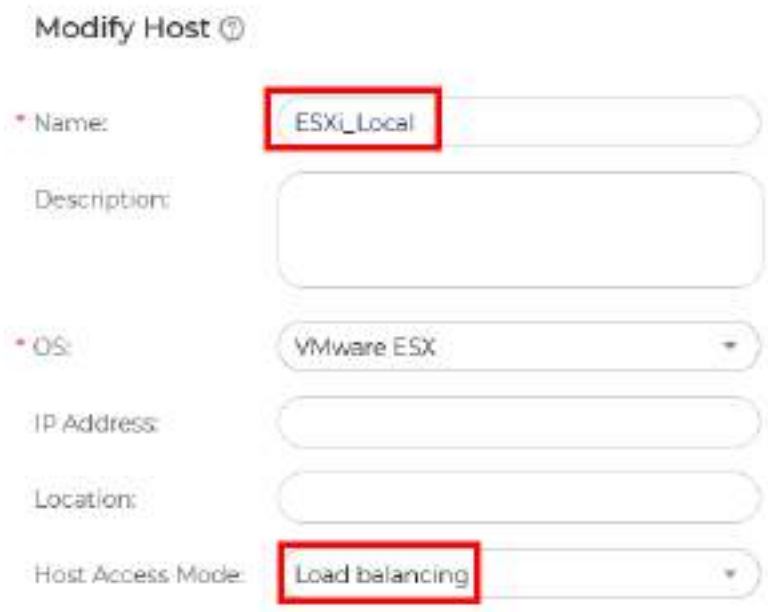


NOTE

- The information displayed on the GUI may vary slightly with the product version.

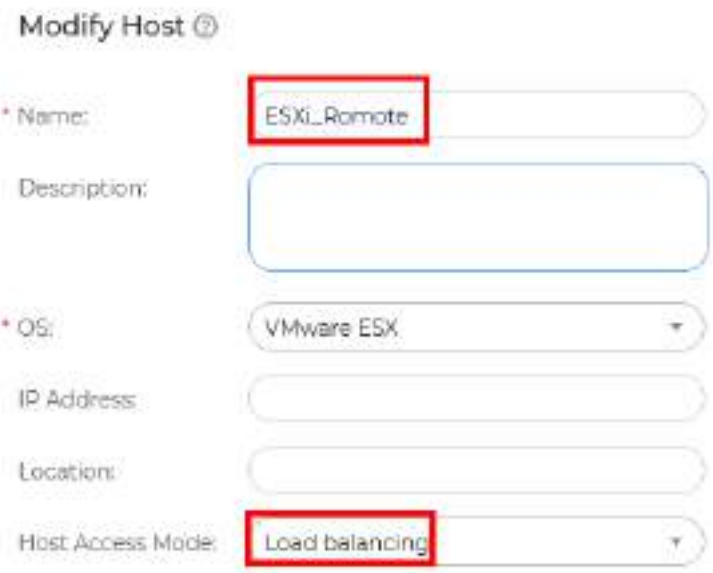
Step 2 On the **Modify Host** page, set **Host Access Mode** to **Load balancing**.

Figure 7-64 Settings on the local storage system



Step 3 Repeat the preceding steps to set **Host Access Mode** of the remote storage system to **Load balancing**.

Figure 7-65 Settings on the remote storage system



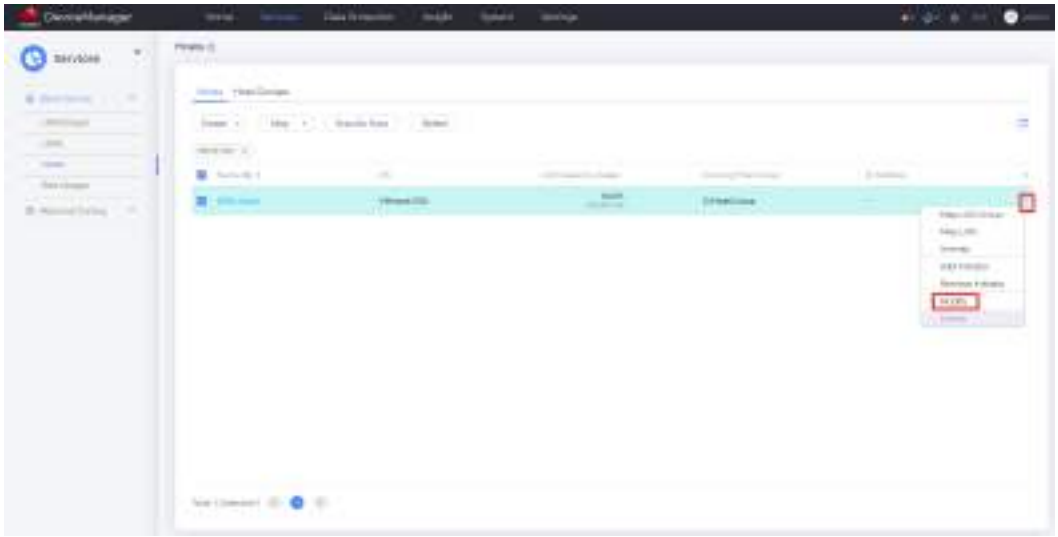
----End

Configuring the Local Preferred Mode

Perform the following operations to configure the local preferred mode:

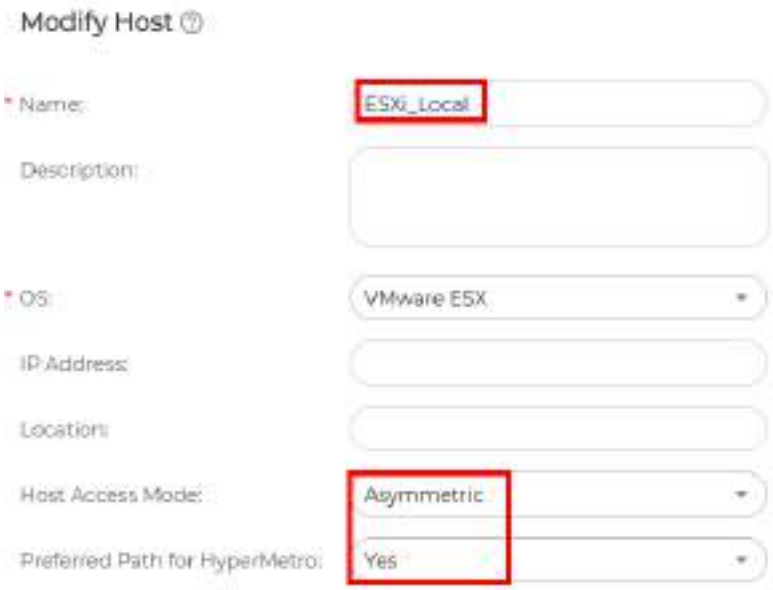
Step 1 On DeviceManager, choose **Services** > **Hosts**. Select the desired host, click ⋮ on the right, and choose **Modify**, as shown in.

Figure 7-66 Modifying the host properties



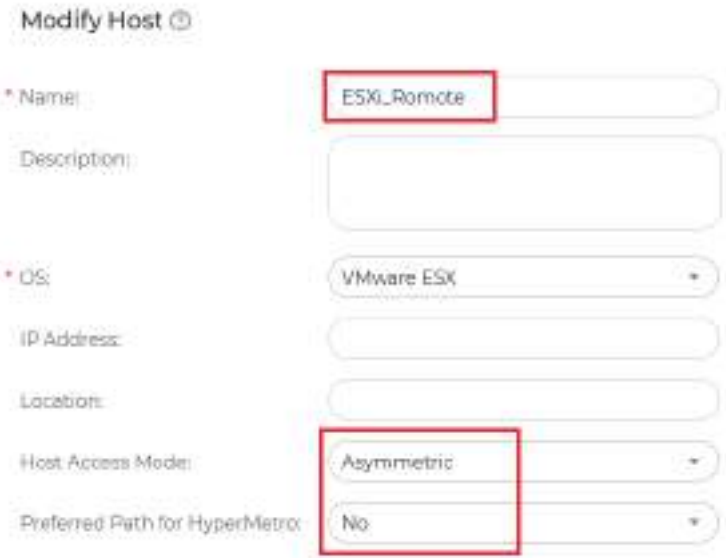
Step 2 For the local storage system, set **Host Access Mode** to **Asymmetric** and **Preferred Path for HyperMetro** to **Yes**.

Figure 7-67 Settings on the local storage system



Step 3 For the remote storage system, set **Host Access Mode** to **Asymmetric** and **Preferred Path for HyperMetro** to **No**.

Figure 7-68 Settings on the remote storage system



----End

NOTE

For details about the VMware ESXi versions, see the **Huawei Storage Interoperability Navigator**.

7.6.6.2 Host Configuration

Requirements on Host LUN IDs

- All path LUN IDs of a LUN are consistent for a host.
- All host LUN IDs of a LUN shared by multiple hosts are consistent across these hosts.

If LUN IDs do not meet the preceding requirements, correct them by referring to "ID Description" in the ***Host Connectivity Guide***.

Recommended VMware NMP Configuration

- VMware NMP is ESXi's native multipathing software and therefore does not need to be installed separately.
- Before mapping LUNs, ensure that Huawei-recommended SATP and PSP rules are configured on the VMware ESXi host. Otherwise, the mapped LUNs can match SATP and PSP rules only after the ESXi host is restarted.
- This section provides the recommended configuration for VMware NMP when it is used for HyperMetro deployment of 6.x series storage systems.

Table 7-19 Recommended VMware NMP configuration for HyperMetro

HyperMetro Working Mode	Storage System	Recommended SATP Rule	Recommended PSP Rule
Load balancing mode	Local storage	VMW_SATP_DEFAULT_AA	VMW_PSP_RR
	Remote storage	VMW_SATP_DEFAULT_AA	VMW_PSP_RR
Local preferred mode	Local storage	VMW_SATP_ALUA	VMW_PSP_RR
	Remote storage	VMW_SATP_ALUA	VMW_PSP_RR

NOTE

- It is advised to set IOPS limit to **1**. For details, see "How Can I Set IOPS Limit for PSP Round Robin to 1?" in the ***Host Connectivity Guide***.
- When employing the HyperMetro solution based on VMware ESXi NMP-inherent multi-pathing, consider compatibility between components (such as storage systems, operating system, HBAs, and switches) and upper-layer software. For details, see the **Huawei Storage Interoperability Navigator**.

- If your VMware ESXi host version is later than or equal to the earliest version in **Table 7-20**, the host has integrated Huawei storage VMW_SATP_ALUA/VMW_PSP_RR and VMW_SATP_DEFAULT_AA/VMW_PSP_RR policies by default and you do not need to manually add them.

Table 7-20 Earliest versions of VMware ESXi hosts that integrate Huawei storage SATP and PSP rules by default

Version	Earliest Version That Integrates VMW_SATP_ALUA and VMW_PSP_RR Policies	Earliest Version That Integrates VMW_SATP_DEFAULT_AA and VMW_PSP_RR Policies
ESXi 6.0	ESXi 6.0 P07 (build number 9239799)	None. You need to manually add the VMW_SATP_DEFAULT_AA and VMW_PSP_RR policies.
ESXi 6.5	ESXi 6.5 Patch 02 (build number 7388607)	ESXi 6.5 Patch 05 (build number 16576891)
ESXi 6.7	ESXi 6.7 GA	ESXi 6.7 Patch 03 (build number 16713306)
ESXi 7.0	ESXi 7.0 GA	ESXi 7.0 U1 (build number 16850804)

NOTE

- For details about the VMware ESXi version release schedule, visit **https://kb.vmware.com/s/article/2143832**.
- VMware ESXi 6.0 U2 and later versions support HyperMetro configuration. Versions earlier than VMware ESXi 6.0 U2 have their defects.

- You can run the following commands to manually add VMW_SATP_ALUA/VMW_PSP_RR and VMW_SATP_DEFAULT_AA/VMW_PSP_RR policies:

  Local preferred mode

  ```
  esxcli storage nmp satp rule add -V HUAWEI -M XSG1 -s VMW_SATP_ALUA -P VMW_PSP_RR -c tpgs_on
  ```

  Load balancing mode

  ```
  esxcli storage nmp satp rule add -V HUAWEI -M XSG1 -s VMW_SATP_DEFAULT_AA -P VMW_PSP_RR -c tpgs_off
  ```

  NOTE

  - In the command, **HUAWEI** is the storage vendor and **XSG1** is the storage model.
  - New SATP rules will immediately take effect for newly mapped LUNs, but will not take effect for previously mapped LUNs until the host is restarted.
  - For details about the parameters in the host commands, see **https://docs.vmware.com/en/VMware-vSphere/6.0/com.vmware.vsphere.storage.doc/GUID-D10F7E66-9DF1-4CB7-AAE8-6F3F1F450B42.html**.

- Set timeout parameters.

  FC networking does not require setting of timeout parameters.

  For iSCSI networking, perform the following operations on ESXi hosts. You must restart the host for the configuration to take effect. Exercise caution when performing this operation.

  a. Obtain the iSCSI adapter name.

  ```
  [root@esxi16113:~] esxcfg-scsidevs -a | grep -i iscsi
  vmhba35 iscsi_vmk       online    iqn.XXXX-XX.com.vmware:esxi16113-xxxxxxxxSCSI Software Adapte
  ```


In the command output, the iSCSI adapter name is **vmhba35**.

b. Query the current timeout parameter settings.

```
[root@esxi16113:~] esxcli iscsi adapter param get -A vmhba35 | egrep 'NoopOutInterval|
NoopOutTimeout|RecoveryTimeout'
NoopOutInterval       15          15          1    60          true    false
NoopOutTimeout        10          10          10   30          true    false
RecoveryTimeout       10          10          1    120         true    false
```

c. Set the timeout parameters.

```
esxcli iscsi adapter param set -A vmhba35 -k NoopOutInterval -v 1
esxcli iscsi adapter param set -A vmhba35 -k NoopOutTimeout -v 10
esxcli iscsi adapter param set -A vmhba35 -k RecoveryTimeout -v 1
```

NOTE

- All the preceding commands are available only in VMware ESXi 5.5, 6.0, 6.5, 6.7, and 7.0. For details on the VMware versions supported in HyperMetro, see the **Huawei Storage Interoperability Navigator**.
- The information in bold is the iSCSI adapter. Change it based on the site requirements. (Run the **esxcfg-scsidevs -a** command to query the iSCSI adapter.)
- You must restart the host for the configuration to take effect.
- The settings shorten the path switchover time to about 11s. In comparison, the default ESXi settings may result in an up-to-35s path switchover time for ESXi 6.0.* and ESXi 6.5.* and an up-to-25s path switchover time for ESXi 6.7.*.

d. Verify the modification.

```
[root@esxi16113:~] esxcli iscsi adapter param get -A vmhba35 | egrep 'NoopOutInterval|
NoopOutTimeout|RecoveryTimeout'
NoopOutInterval       1           15          1    60          true    false
NoopOutTimeout        10          10          10   30          true    false
RecoveryTimeout       1           10          1    120         true    false
```

Host Configuration

- Configuring a VMware cluster

Table 7-21 Cluster configuration

VMware vSphere ESXi Version	Host Parameter	Cluster Parameter (VM Policy for APD and PDL)	Remarks
5.0 U1 5.1	Log in to each ESXi host using SSH, open the **/etc/vmware/settings** file, and add **Disk.terminateVMOnPDL-Default = True** to the file.	Use the vSphere Client to log in to each ESXi host. In the advanced settings, set **das.maskCleanShutdownEnabled = True**.	After configuring host parameters, restart the host for the configuration to take effect.

<table>
<tr><th>VMware vSphere ESXi Version</th><th colspan="2">Host Parameter</th><th>Cluster Parameter (VM Policy for APD and PDL)</th><th>Remarks</th></tr>
<tr><td>5.5.*</td><td>VMkernel.Boot.terminateVMOnPDL=True</td><td>Disk.AutoremoveOnPDL=0</td><td>Select Turn on vSphere HA.</td><td>After configuring host parameters, restart the host for the configuration to take effect.
After configuring cluster parameters, re-enable HA for the configuration to take effect.</td></tr>
<tr><td>6.0 GA
6.0 U1</td><td colspan="4">HyperMetro is not supported if the OS native multipathing software (VMware NMP) is used. You are advised to upgrade the operating system to ESXi 6.0 U2 or later.
NOTE
Storage PDL responses may not trigger path failover in VMware vSphere 6.0 GA and 6.0 U1. For details, see VMware KB.</td></tr>
<tr><td>6.0 U2
6.0 U3
6.5.*
6.7.*</td><td>VMkernel.Boot.terminateVMOnPDL=False (Retain the default value.)</td><td>Disk.AutoremoveOnPDL=1 (Retain the default value.)</td><td>1. Select Turn on vSphere HA.
2. Set Datastore with PDL to Power off and restart VMs.
3. Set Datastore with APD to Power off and restart VMs - Aggressive restart policy.</td><td>Retain the default host parameter settings. You only need to enable HA again in vCenter for the settings to take effect.
On a parallel network, set Datastore with PDL and Datastore with APD to Power off and restart VMs to ensure that VMs can be switched to the peer end in the case of a single point of failure. On a standard network, this setting is optional and you can determine whether to use</td></tr>
</table>

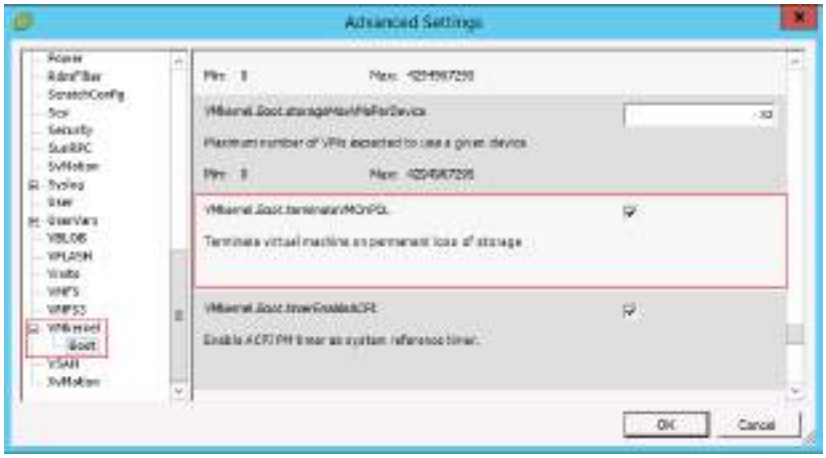
VMware vSphere ESXi Version	Host Parameter		Cluster Parameter (VM Policy for APD and PDL)	Remarks
7.0.*				this setting based on site requirements.

The following configurations are mandatory when you configure a VMware cluster:

- A VM service network requires L2 interworking between data centers so that VM migration between data centers will not affect VM services.
- For VMware vSphere 5.0 u1, later 5.0 versions, and vSphere 5.1:
  - Cluster parameter configuration: Use the vSphere Client to log in to each ESXi host. In the advanced settings, set **das.maskCleanShutdownEnabled = True**.
  - Host parameter configuration: Log in to each ESXi host using SSH and add **Disk.terminateVMOnPDLDefault = True** to the **/etc/vmware/settings** file. After configuring host parameters, restart the host for the configuration to take effect.
- For VMware vSphere 5.5 and its update versions:
  - Cluster parameter configuration: Use vSphere Web Client to connect to vCenter, go to the cluster HA configuration page, and select **Turn on vSphere HA**. After configuring cluster parameters, re-enable HA for the configuration to take effect.
  - Host parameter configuration: Log in to each ESXi host using vSphere Client or vCenter and complete the following advanced settings. After configuring host parameters, restart the host for the configuration to take effect.

    Set **VMkernel.Boot.terminateVMOnPDL = True**. The parameter forcibly powers off VMs on a datastore when the datastore enters the PDL state.

Figure 7-69 Boot parameter settings



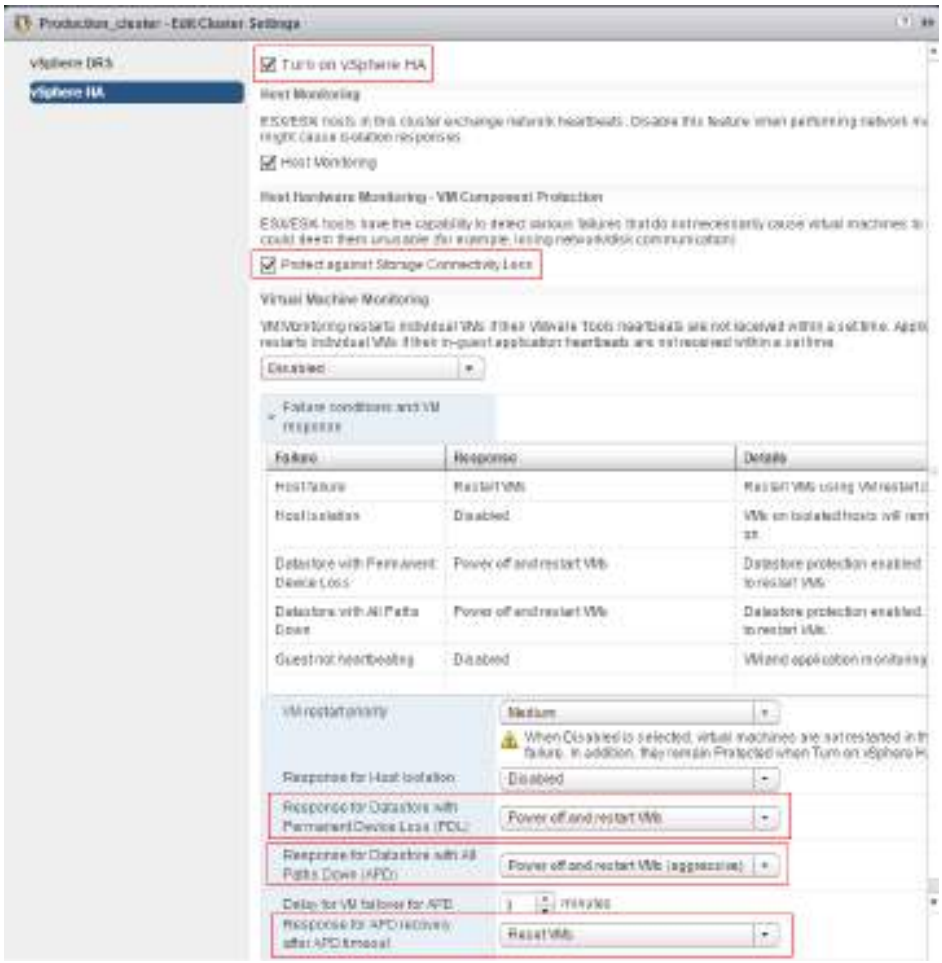
Set **Disk.AutoremoveOnPDL = 0**. This setting ensures that datastores in the PDL state will not be automatically removed.

Figure 7-70 Disk parameter settings

– For VMware vSphere 6.0 u2 and later updates:

  After connecting to vCenter through the vSphere Web Client, enter the cluster HA configuration and set the parameters as follows.

Figure 7-71 vSphere 6.0 cluster configuration



– For VMware vSphere 6.5:

  After connecting to vCenter through the vSphere Web Client, enter the cluster HA configuration and set the parameters as follows.

  Figure 7-72 vSphere 6.5 cluster configuration-1

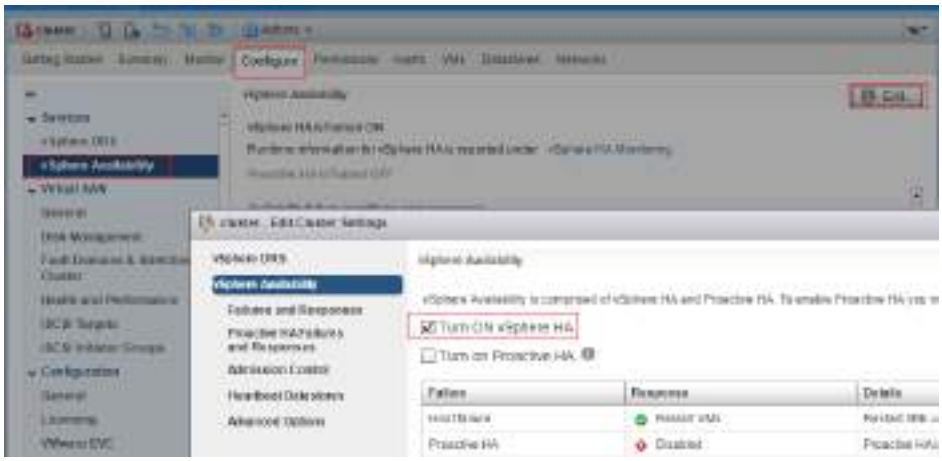
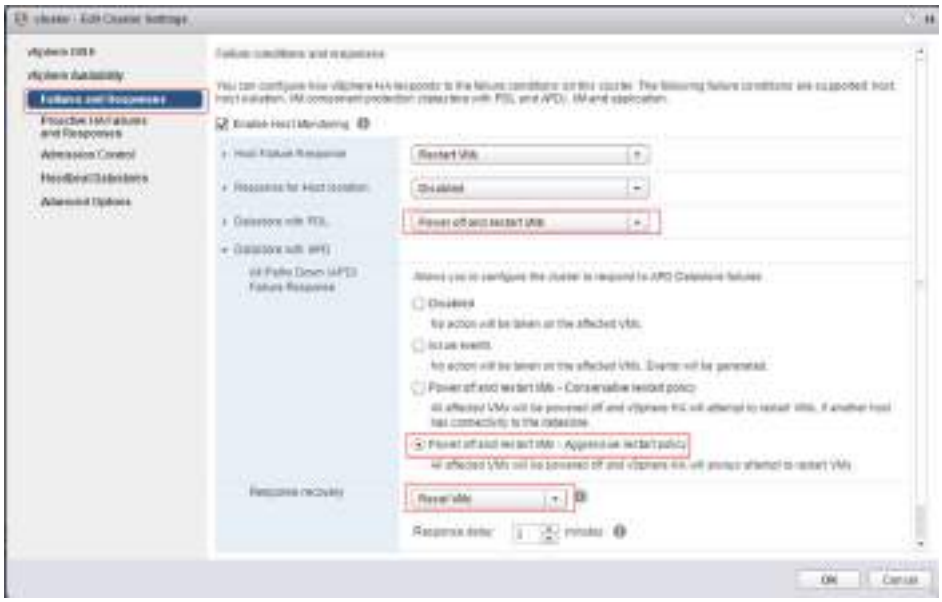


  Figure 7-73 vSphere 6.5 cluster configuration-2

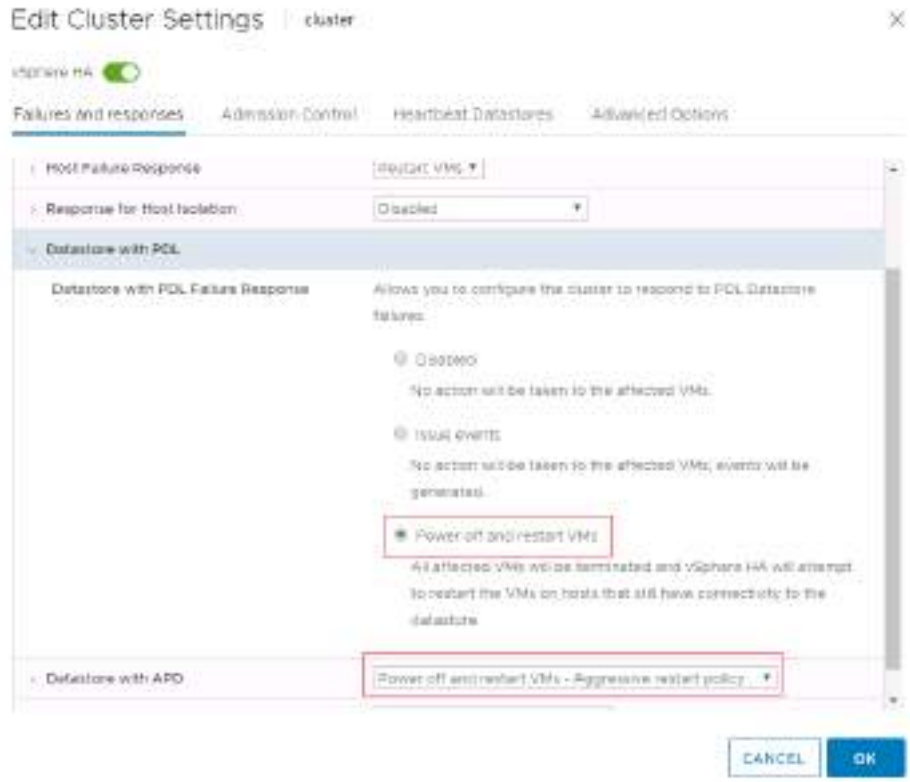


– For VMware vSphere 6.7 and 7.0 and later updates:

  After connecting to vCenter through the vSphere Web Client, enter the cluster HA configuration and set the parameters as follows.

Figure 7-74 vSphere 6.7 and 7.0 cluster configuration-1

Figure 7-75 vSphere 6.7 and 7.0 cluster configuration-2



- Configuring a VMware cluster (optional)
  - Configure the vMotion, service, and management networks with different VLAN IDs to prevent network interference.
  - Configure the management network to include the vCenter Server management node and ESXi hosts. Deny access from external applications.
  - Divide the service network into VLANs to ensure logical isolation and control broadcast domains.
  - Configure a DRS group to ensure that VMs can be recovered first in the local data center in the event of the breakdown of a single host.

7.6.6.3 Verification

Verifying the Load Balancing Mode

Perform the following operations to verify that VMware NMP configurations have taken effect:

Step 1 Run the **esxcli storage nmp satp rule list | grep -i huawei** command to verify that SATP rules are successfully added.

```
[root@localhost:~] esxcli storage nmp satp rule list | grep -i huawei
VMW_SATP_ALUA              HUAWEI   XSG1                                    system
tpgs_on                    VMW_PSP_RR
VMW_SATP_DEFAULT_AA        HUAWEI   XSG1                                    user
tpgs_off                   VMW_PSP_RR
```

The command output includes **VMW_SATP_DEFAULT_AA**, which means that SATP rules have been successfully added. Manually added SATP rules (user-level) have a higher priority than the default ones (system-level).

Step 2 Run the **esxcli storage nmp device list -d=***naa.6xxxxxxx* command to verify that working paths of LUNs are properly configured.

naa.6xxxxxxx indicates the drive letter of a LUN after being mapped to the host.

Working paths are successfully configured if their **Storage Array Type** and **Path Selection Policy** are the same as those configured, and the number of **Working Paths** is equal to the total number of paths in the port group.

Example:

The following SATP rule is configured:

```
esxcli storage nmp satp rule add -V HUAWEI -M XSG1 -s VMW_SATP_DEFAULT_AA -P VMW_PSP_RR -c
tpgs_off
```

The port group has four paths.

Figure 7-76 Checking the working paths of LUNs

In the preceding command output, **Storage Array Type** is **VMW_SATP_DEFAULT_AA**, **Path Selection Policy** is **VMW_PSP_RR**, and there are four **Working Paths**, which are consistent with the configuration. Therefore, working paths are successfully configured.

NOTE

When **Path Selection Policy** is **VMW_PSP_FIXED**, only one working path is available, which may be any path in the port group.

----End

Verifying the Local Preferred Mode

Perform the following operations to verify that VMware NMP configurations have taken effect:

Step 1 Run the **esxcli storage nmp satp rule list | grep -i huawei** command to verify that SATP rules are successfully added.

```
[root@localhost:~] esxcli storage nmp satp rule list | grep -i huawei
VMW_SATP_ALUA                HUAWEI   XSG1                                                system
tpgs_on                      VMW_PSP_RR
VMW_SATP_ALUA          HUAWEI   XSG1                                                user
tpgs_on                      VMW_PSP_RR
```

The command output includes **VMW_SATP_ALUA**, which means that SATP rules have been successfully added. Manually added SATP rules (user-level) have a higher priority than the default ones (system-level).

Step 2 Run the **esxcli storage nmp device list -d=***naa.6xxxxxxx* command to verify that working paths of LUNs are properly configured.

naa.6xxxxxxx indicates the drive letter of a LUN after being mapped to the host.

Working paths are successfully configured if their **Storage Array Type** and **Path Selection Policy** are the same as those configured, and the number of **Working Paths** is equal to the total number of paths in the port group.

Example:

The following SATP rule is configured:

```
esxcli storage nmp satp rule add -V HUAWEI -M XSG1 -s VMW_SATP_ALUA -P VMW_PSP_RR -c tpgs_on
```

The port group has three paths.

Figure 7-77 Checking the working paths of LUNs

In the preceding command output, **Storage Array Type** is **VMW_SATP_ALUA**, **Path Selection Policy** is **VMW_PSP_RR**, and there are three **Working Paths**, which are consistent with the corresponding preferred path parameters. Therefore, working paths are successfully configured.

NOTE

When **Path Selection Policy** is **VMW_PSP_FIXED**, only one working path is available, which may be any path in the port group where preferred paths reside.

----End

7.6.7 Windows

7.6.7.1 Storage System Configuration

If the OS native multipathing software is used, retain the default settings of the initiator and configure **Host Access Mode** and **Preferred Path for HyperMetro** as required. **Table 7-22** lists the detailed settings.

Table 7-22 Storage configurations for interconnection with Windows application servers

HyperMetro Working Mode	Storage System	OS Setting	Host Access Mode	Preferred Path for HyperMetro	Description
Load balancing mode	Local storage	Windows	Asymmetric	Yes	The host uses all paths of a disk with equal priority.
	Remote storage	Windows	Asymmetric	Yes	
Local preferred mode	Local storage	Windows	Asymmetric	Yes	The host considers the paths from the local storage system as preferred paths, and those from the remote storage system as non-preferred paths.
	Remote storage	Windows	Asymmetric	No	

Configuring the Load Balancing Mode

Perform the following operations to configure the load balancing mode:

Step 1 On DeviceManager, choose **Services** > **Hosts**. Select the desired host, click ⋮ on the right, and choose **Modify**.

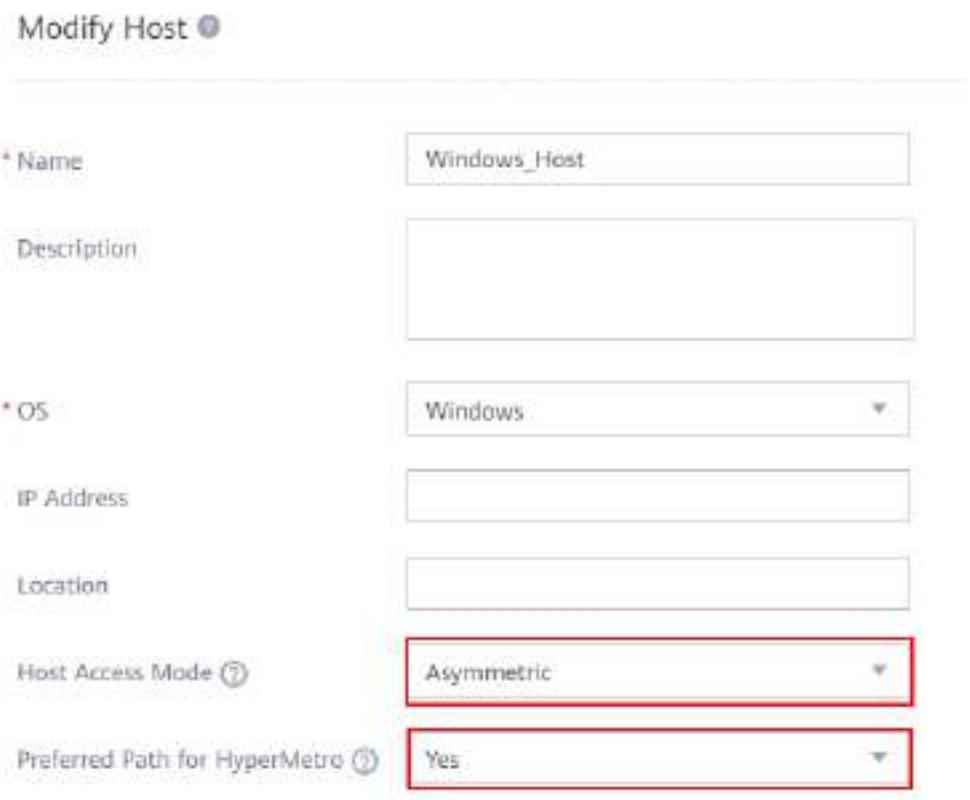
Figure 7-78 Modifying the host properties

NOTE

- The information displayed on the GUI may vary slightly with the product version.

Step 2 On the **Modify Host** page, set **Host Access Mode** of the local storage system to **Asymmetric** and **Preferred Path for HyperMetro** to **Yes**.

Figure 7-79 Settings on the local storage system



Step 3 Repeat the preceding steps to set **Host Access Mode** of the remote storage system to **Asymmetric** and **Preferred Path for HyperMetro** to **Yes**.

----End

Configuring the Local Preferred Mode

Perform the following operations to configure the local preferred mode:

Step 1 On DeviceManager, choose **Services** > **Hosts**. Select the desired host, click ⋮ on the right, and choose **Modify**.

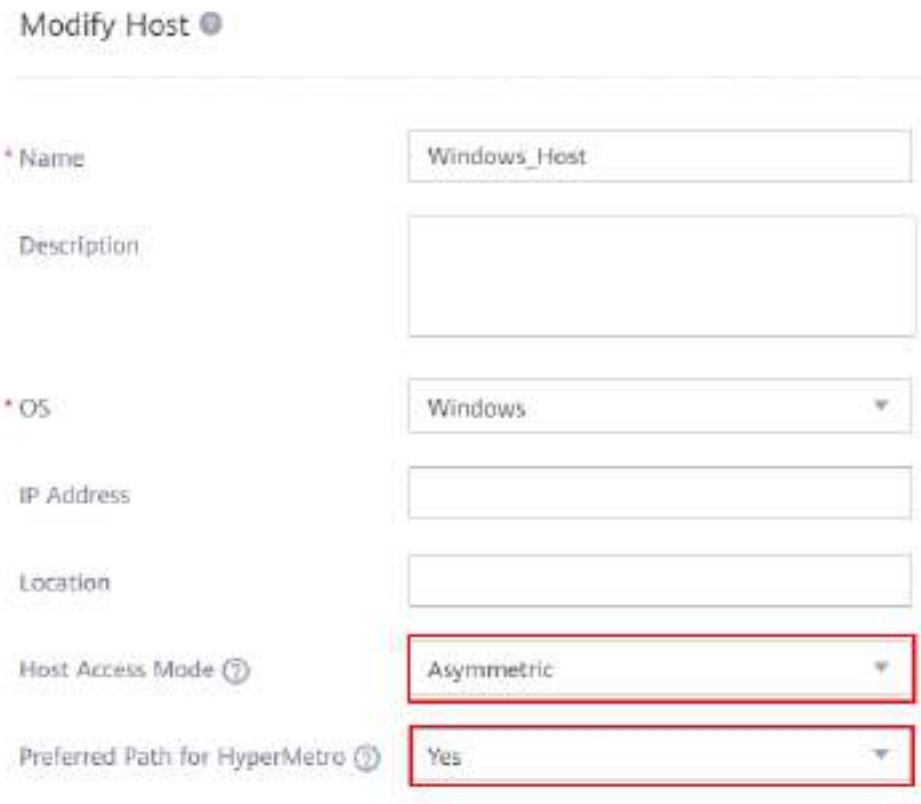
Figure 7-80 Modifying the host properties

NOTE

- The information displayed on the GUI may vary slightly with the product version.

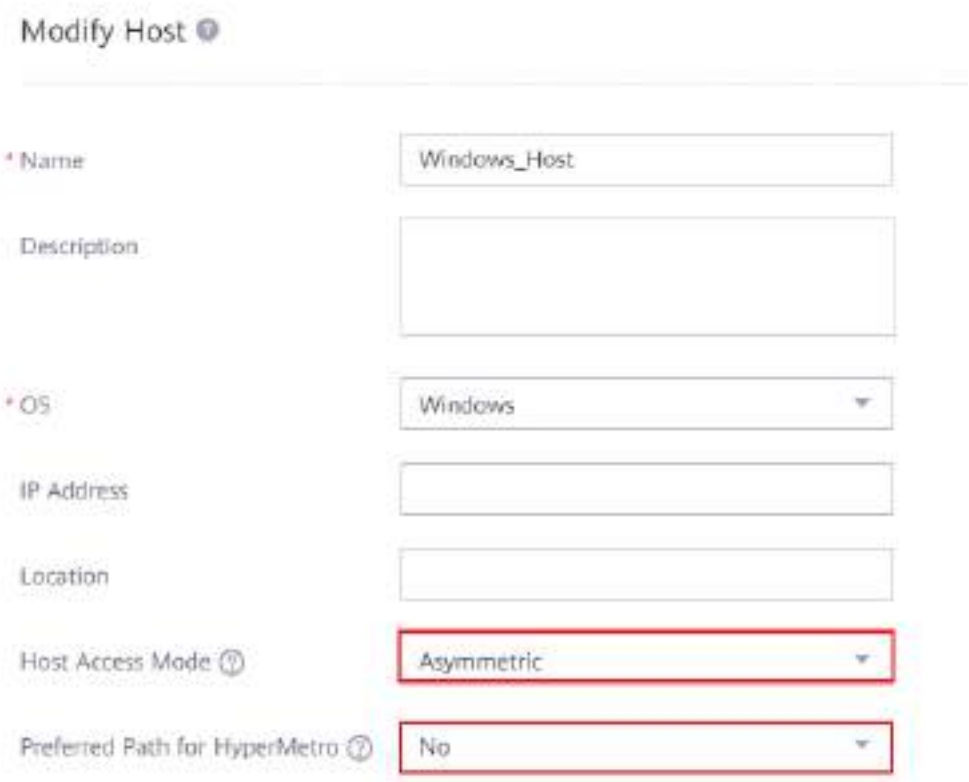
Step 2 For the local storage system, set **Host Access Mode** to **Asymmetric** and **Preferred Path for HyperMetro** to **Yes**.

Figure 7-81 Settings on the local storage system



Step 3 For the remote storage system, set **Host Access Mode** to **Asymmetric** and **Preferred Path for HyperMetro** to **No**.

Figure 7-82 Settings on the remote storage system



----End

NOTICE

- For details about the Windows versions, see the **Huawei Storage Interoperability Navigator**.
- If a LUN has been mapped to a host, you must restart the host for the configuration to take effect after you modify **Host Access Mode** or **Preferred Path for HyperMetro**. If you map the LUN for the first time, restart is not needed.
- When data is migrated from other Huawei storage systems (including OceanStor Dorado V3, OceanStor V3, and OceanStor V5) to 6.x series storage systems, configure the storage system by following instructions in "FAQs" in the ***Host Connectivity Guide***.

7.6.7.2 Host Configuration

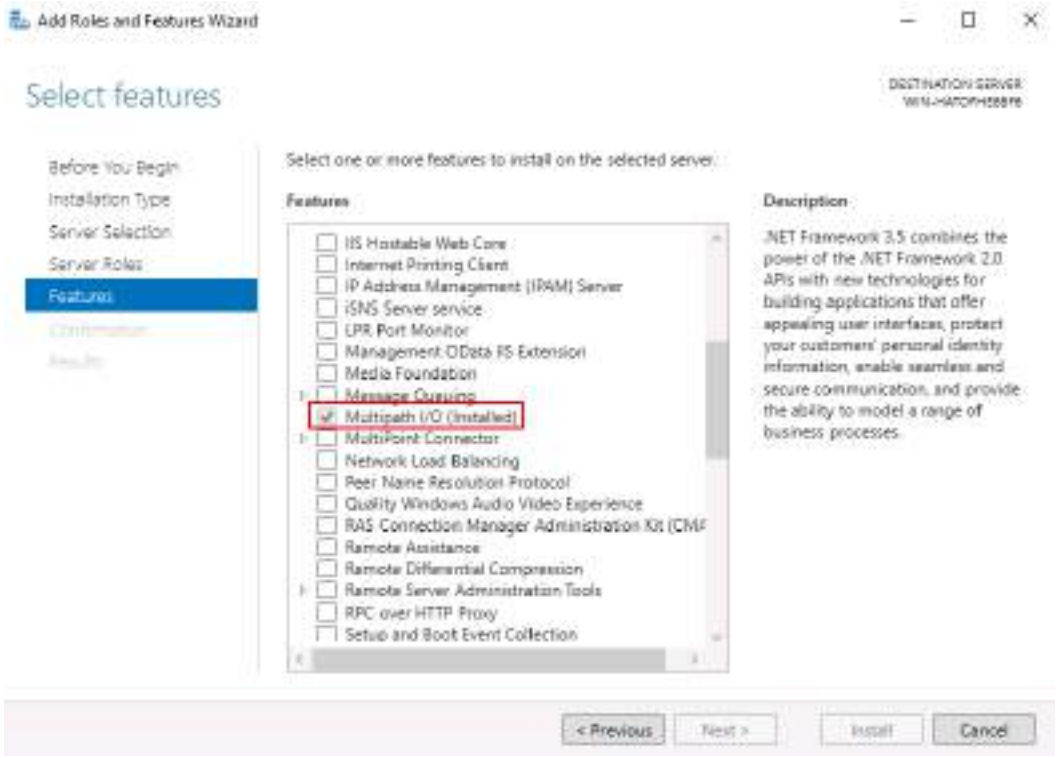
In Windows, MPIO is disabled by default. You must manually enable it.

This section uses Windows Server 2016 as an example to describe how to install and configure MPIO. The MPIO installation and configuration procedures in other Windows Server releases are similar. For more details, see the Microsoft official documentation.

Step 1 Add **Multipath I/O**.

Start **Server Manager**, choose **Manage** > **Add Roles and Features**, and select **Multipath I/O**.

Figure 7-83 Adding Multipath I/O



Step 2 Query the device's VID and PID.

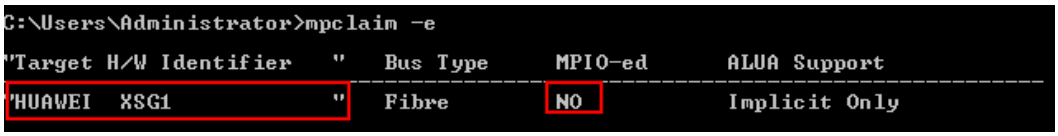
VID indicates the vendor ID, for example, **HUAWEI**.

PID indicates the product ID, for example, **S5500T**, **S5600T**, or **XSG1**.

If MPIO is installed on Windows Server 2008 to 2019, you can use multipathing command **mpclaim** to query disk information.

If **Host Access Mode** is set to **Asymmetric** on the storage system, use the command in **Figure 7-84** to query disk information.

Figure 7-84 Querying disk information



In the preceding figures, the VID is **HUAWEI** and the PID is **XSG1**. **MPIO-ed** is **NO**, indicating that the LUN is not taken over by MPIO.

NOTE

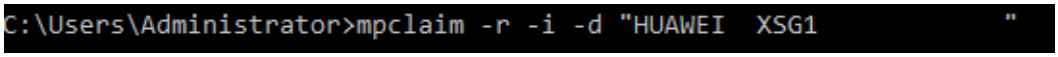
The PID and VID in this section are examples only.

Step 3 Configure MPIO to take over the storage system.

You can add the target storage system on the MPIO console or run a command in Command Prompt to take over the storage. In this example, a command is run in Command Prompt.

On the Windows server, open Command Prompt and run the **mpclaim -r -i -d "HUAWEI XSG1 "** command. Note that the VID must contain eight characters and the PID must contain 16 characters. If the characters are insufficient, add spaces. You can copy the VID and PID from the output of the **mpclaim -e** command.

Figure 7-85 Taking over Huawei storage



NOTICE

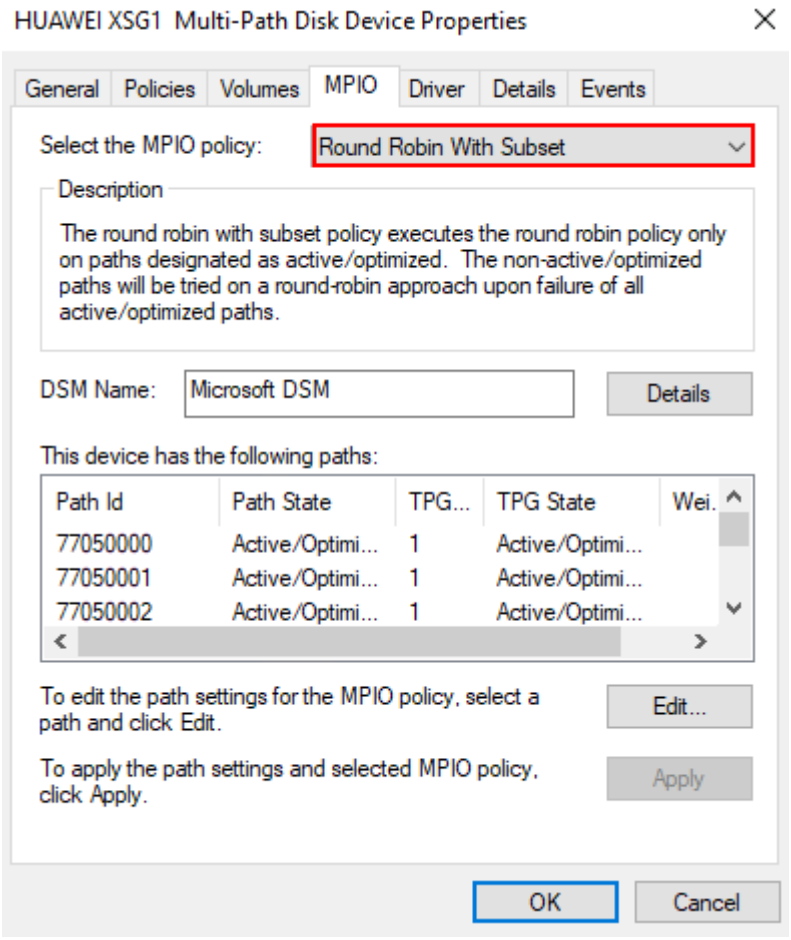
After the command is executed, the host restarts automatically. If the host does not restart automatically, restart it manually.

Step 4 View MPIO policies.

Rescan for disks after restarting the host. Ensure that the number of discovered disks is consistent with that of LUNs mapped to the host. Right-click a disk and choose **Properties** from the shortcut menu. You can view the policies on the **MPIO** tab page.

If **Host Access Mode** is set to **Asymmetric** on the storage system, the default MPIO policy of the OS is **Round Robin With Subset**.

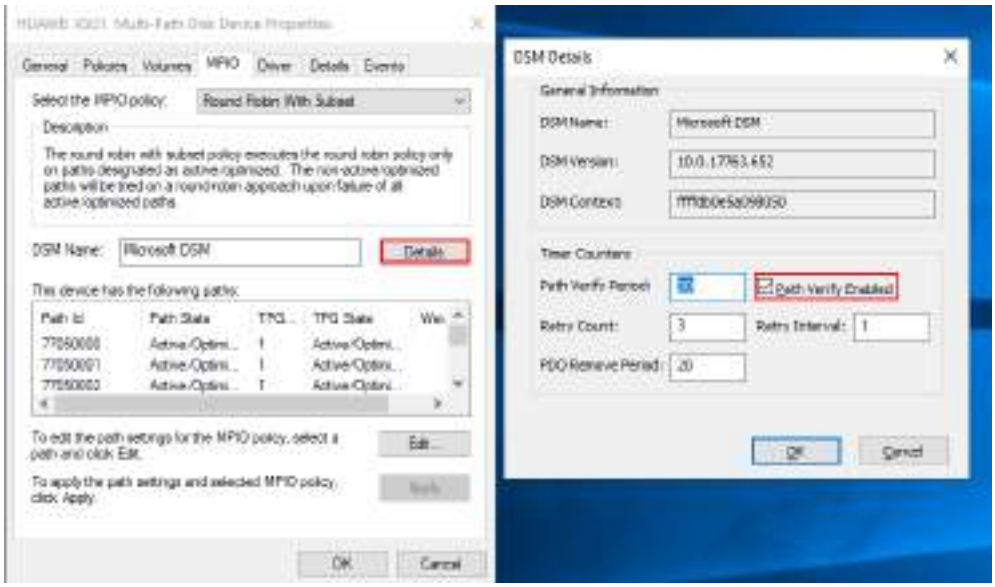
Figure 7-86 MPIO policy management page



Step 5 Enable path verification.

On the **MPIO** tab, click **Details**. In the dialog box that is displayed, select **Path Verify Enabled** and click **OK**. Then restart the host for the configuration to take effect.

Figure 7-87 Enabling path verification



----End

NOTICE

- If a path switchover takes a long period of time, you can modify the timeout time for a driver by following instructions in "How Do I Modify the Timeout Time for the FC HBA Port Driver", "How Do I Modify the iSCSI Initiator's Driver Timeout Time", and "How Do I Change the Number of TCP Data Retransmission Times" in the *OceanStor Dorado Host Connectivity Guide for Windows* to shorten I/O interruption.
- If the underlying physical signals between the storage system and Cisco switch are poor, the Cisco switch resets the link. There is a low probability that the Cisco switch does not detect the port status change and does not send RSCN messages. In this case, Windows MPIO cannot detect the port status change, and host services are interrupted due to I/O retry timeout on an abnormal link. Huawei UltraPath can be used to avoid this risk.

7.6.7.3 Verification

Verifying the Load Balancing Mode

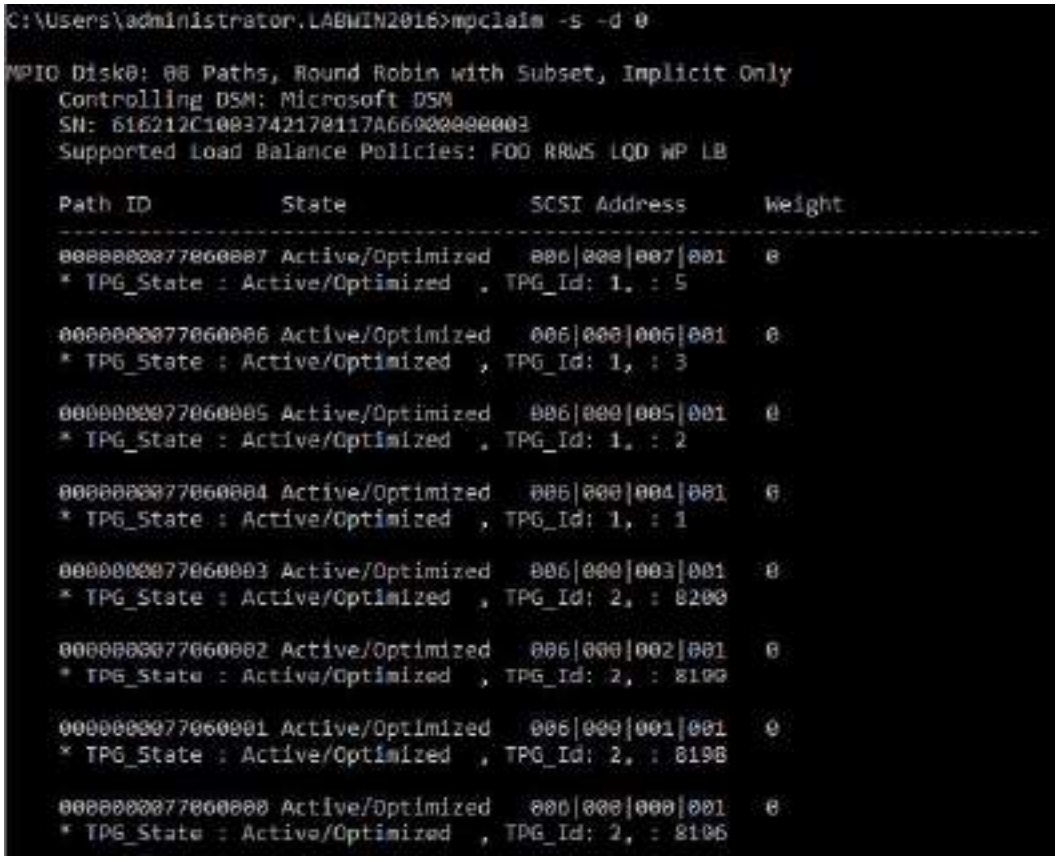
If HyperMetro works in load balancing mode, run the **mpclaim -s -d** command to verify that the configuration has taken effect.

Figure 7-88 Verifying the MPIO disk information

```
C:\Users\Administrator.LABWIN2016>mpclaim -s -d

For more information about a particular disk, use 'mpclaim -s -d #' where # is the MPIO disk number.

MPIO Disk    System Disk  LB Policy    DSM Name
-------------------------------------------------------------------------------
MPIO Disk1   Disk 2       RRWS         Microsoft DSM
MPIO Disk0   Disk 1       RRWS         Microsoft DSM
```


Run the **mpclaim -s -d** *MPIO Disk No.* command to verify path information about an MPIO disk.

Figure 7-89 Verifying path information about an MPIO disk

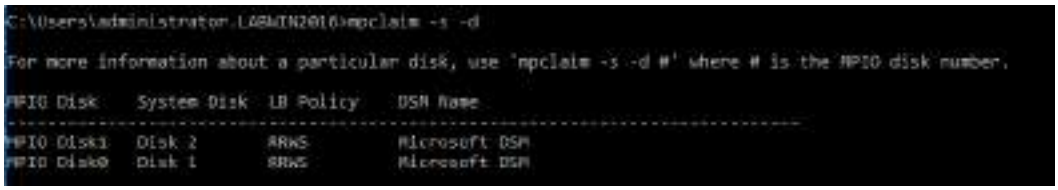


In the preceding figure, the MPIO policy is **Round Robin**, and the paths whose **TPG_State** is **Active/Optimized** are preferred paths.

Verifying the Local Preferred Mode

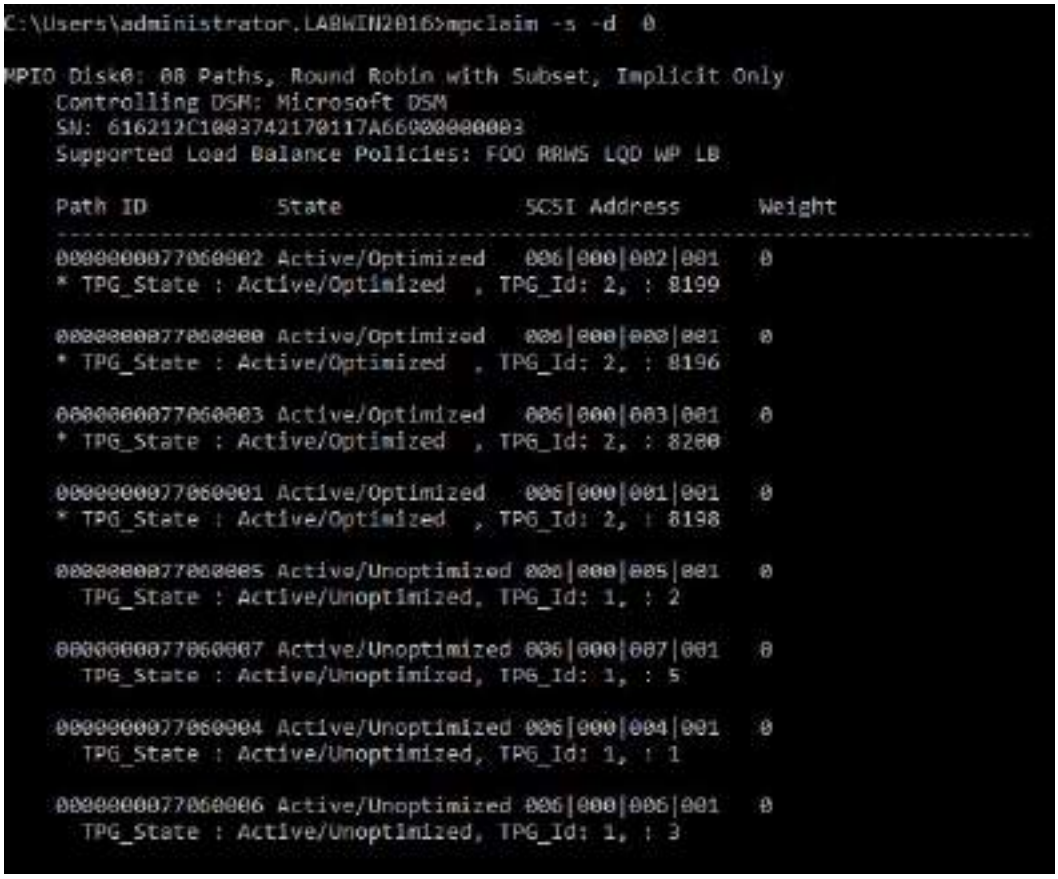
If HyperMetro works in local preferred mode, run the **mpclaim -s -d** command to verify that the configuration has taken effect.

Figure 7-90 Verifying the MPIO disk information



Run the **mpclaim -s -d** *MPIO Disk No.* command to verify path information about an MPIO disk.

Figure 7-91 Verifying path information about an MPIO disk



In the preceding figure, the MPIO policy is **Round Robin with Subset**. The paths whose **TPG_State** is **Active/Optimized** are preferred path, and the paths whose **TPG_State** is **Active/Unoptimized** are non-preferred paths.

7.7 Configuring Veritas/Symantec DMP

7.7.1 AIX

7.7.1.1 Storage System Configuration

If DMP is used, retain the default settings of the initiator and configure **Host Access Mode** and **Preferred Path for HyperMetro** as required. **Table 7-23** lists the detailed settings.

Table 7-23 Storage configurations for interconnection with AIX application servers

DMP	HyperMetro Working Mode	Storage System	OS Setting	Host Access Mode	Preferred Path for HyperMetro	Description
DMP 6.0.x to DMP 7.0	Load balancing mode	Local storage	AIX	Load balancing	N/A	The host uses all paths of a disk with equal priority.
		Remote storage	AIX	Load balancing	N/A	
DMP 7.1 or later	Load balancing mode	Local storage	AIX	Load balancing	N/A	
		Remote storage	AIX	Load balancing	N/A	
	Local preferred mode	Local storage	AIX	Asymmetric	Yes	The host considers the paths from the local storage system as preferred paths, and those from the remote storage system as non-preferred paths.
		Remote storage	AIX	Asymmetric	No	

NOTE

- Use **Huawei Storage Interoperability Navigator** to query the combinations supported by DMP.
- DMP earlier than 7.1 does not support the local preferred mode or asymmetric mode.
- If a LUN has been mapped to a host, you must restart the host for the configuration to take effect after you modify **Host Access Mode** or **Preferred Path for HyperMetro**. If the host is running services, stop the services and export the disk group before restarting the host. If you configure the initiator for the first time, restart is not needed.
- To change the LUN mapping on the storage system, including but not limited to changing the host LUN ID, changing the port online, and removing and adding a LUN, follow the instructions in "How Can I Change LUN Mappings When Non-Huawei Multipathing Software Is Used?" in the ***Host Connectivity Guide*** *for AIX* to correctly change the LUN mapping. Otherwise, services may be interrupted.
- If you do not use the recommended configurations, DMP may fail to identify and process paths properly.
- If DMP 7.x is used and **Host Access Mode** is set to **Asymmetric**, the maximum number of online FC and Ethernet ports supported by a single storage system or two HyperMetro storage systems is limited because the default RTPG buffer length of Veritas VxVM (DMP) is 255. If the number of online ports is greater than the allowed value, paths may not be properly identified. For details, contact Huawei engineers.

Configuring the Load Balancing Mode

The method for configuring the load balancing mode when DMP is used is the same as that when the OS native multipathing software is used.

Configuring the Local Preferred Mode

The method for configuring the local preferred mode when DMP is used is the same as that when the OS native multipathing software is used.

7.7.1.2 Host Configuration

Pre-installation Check

Before installing the Veritas DMP multipathing software, ensure that the operating system's native multipathing software has not taken over Huawei storage. In the following example, there are 16 sub-paths between a LUN and a host. The host OS identifies 16 hdisks of the **Other FC SCSI Disk Drive** type, indicating that the OS native multipathing software has not taken over Huawei storage.

```
bash-3.2# lsdev -Cc disk
hdisk0  Available 0D-00-00 SAS Disk Drive
hdisk1  Defined   06-00-02 N/A
hdisk2  Defined   06-00-02 N/A
hdisk3  Available 0J-00-02 Other FC SCSI Disk Drive
hdisk4  Available 0J-00-02 Other FC SCSI Disk Drive
hdisk5  Available 0J-00-02 Other FC SCSI Disk Drive
hdisk6  Available 0J-00-02 Other FC SCSI Disk Drive
hdisk7  Available 0J-01-02 Other FC SCSI Disk Drive
hdisk8  Available 0J-01-02 Other FC SCSI Disk Drive
hdisk9  Available 0J-01-02 Other FC SCSI Disk Drive
hdisk10 Available 0J-01-02 Other FC SCSI Disk Drive
hdisk11 Available 0J-00-02 Other FC SCSI Disk Drive
hdisk12 Available 0J-00-02 Other FC SCSI Disk Drive
hdisk13 Available 0J-00-02 Other FC SCSI Disk Drive
hdisk14 Available 0J-00-02 Other FC SCSI Disk Drive
hdisk15 Available 0J-01-02 Other FC SCSI Disk Drive
hdisk16 Available 0J-01-02 Other FC SCSI Disk Drive
hdisk17 Available 0J-01-02 Other FC SCSI Disk Drive
hdisk18 Available 0J-01-02 Other FC SCSI Disk Drive
bash-3.2#
```

NOTICE

If any hdisk is of the **Huawei MPIO FC Disk Drive** type, you must stop services and uninstall ODM. For details on how to uninstall ODM, see the *AIX ODM for MPIO User Guide*.

Installing ASL

DMP is generally integrated in the Veritas Storage Foundation/InfoScale software package and is used together with the Veritas Volume Manager (VxVM) and Veritas File System (VxFS).

In this document, installing Veritas InfoScale 7.4.1 in AIX 7.2 TL1 is used as an example. For details about how to install Veritas InfoScale 7.4.1, see **Veritas Storage Foundation Installation Guide**.

After installing Veritas InfoScale, install Array Support Library (ASL), which provides array-specific support for DMP. ASL is a shared library that can be dynamically loaded. When discovering devices, ASL implements hardware-specific logic to discover device properties.

You are advised to install the latest version of ASL. You can obtain the ASL installation package for Huawei storage from **https://sort.veritas.com/asl**. ASL can be installed online or offline. Install ASL by following instructions in the **Readme** file on the official download page. The default path selection policy is MinimumQ.

NOTE

- Veritas AVID does not support Huawei storage.
- After installing the Veritas software, modify the **dyntrk** and **fc_err_recov** parameters of the AIX FC HBA. For details, see "How Can I Modify the dyntrk and fc_err_recov Parameters for FC HBAs?" in the ***Host Connectivity Guide***.
- DMP provides the **MinimumQ** and **Round-Robin** path selection algorithms, which can be modified based on customer service configurations. You can run the **vxdmpadm setattr ENCLR_NAME iopolicy=***xxx* command to modify the path selection algorithm. *xxx* indicates the path selection algorithm, which can be **MinimumQ** or **Round-Robin**.

7.7.1.3 Verification

Verifying the Load Balancing Mode

Step 1 Run the **vxddladm listsupport all | grep huawei** command to verify the ASL installation. In the following example, the multipathing software has correctly identified **XSG1**.

```
bash-3.2# vxddladm listsupport all | grep huawei
libvxhuawei.so      HUAWEI, HUASY       S5100, S5300, S5500, S5600, S6800E, S8000, S8000-I, VIS6000, S5500T, S5600T, S5800T, S6800T, S2600T, V1500, V1800, S2100, S2200T, S2300, S2300E, S2600, S3900-M100, S3900-M200, S3900-M300, S5900-M100, S5900-M200, S6900-M100, Dorado2100, Dorado2100 G2, Dorado5100, HVS85T, HVS88T, XSG1
bash-3.2#
```

CAUTION

If **XSG1** does not exist, upgrade the VRTSaslapm ASL online to a version that supports Huawei storage. You can obtain the ASL installation package for Huawei storage from **https://sort.veritas.com/asl**. Install ASL by following instructions in the **Readme** file on the official download page.

Step 2 Run the **cfgmgr -v** and **vxdisk scandisks** commands at the OS and DMP layers respectively to scan for LUNs. Then run the **vxddladm list devices** command to check whether the disk corresponding to each sub-path is claimed by Veritas. In the following example, one LUN is mapped and has 16 sub-paths. **libvxhuawei.so** has identified 16 devices.

```
bash-3.2# vxddladm list devices
DEVICE            TARGET-ID    STATE   DDL-STATUS (ASL)
============================================================
hdisk17           -            Online  CLAIMED (libvxhuawei.so)
hdisk6            -            Online  CLAIMED (libvxhuawei.so)
hdisk12           -            Online  CLAIMED (libvxhuawei.so)
hdisk18           -            Online  CLAIMED (libvxhuawei.so)
```



```
hdisk7          -          Online  CLAIMED (libvxhuawei.so)
hdisk13         -          Online  CLAIMED (libvxhuawei.so)
hdisk8          -          Online  CLAIMED (libvxhuawei.so)
hdisk14         -          Online  CLAIMED (libvxhuawei.so)
hdisk3          -          Online  CLAIMED (libvxhuawei.so)
hdisk9          -          Online  CLAIMED (libvxhuawei.so)
hdisk15         -          Online  CLAIMED (libvxhuawei.so)
hdisk4          -          Online  CLAIMED (libvxhuawei.so)
hdisk10         -          Online  CLAIMED (libvxhuawei.so)
hdisk16         -          Online  CLAIMED (libvxhuawei.so)
hdisk5          -          Online  CLAIMED (libvxhuawei.so)
hdisk11         -          Online  CLAIMED (libvxhuawei.so)
hdisk0          -          Online  CLAIMED (Disk)
```

Step 3 Run the **vxdisk list** command to check whether HyperMetro LUNs on the host have been aggregated. The aggregated device can be identified as **huawei-xxx**. In the following example, DMP identifies an aggregated LUN as **huawei-xsg11_#**.

```
bash-3.2# vxdisk list
DEVICE          TYPE          DISK        GROUP        STATUS
aix_disk_0 auto:LVM        -           -            LVM
huawei-xsg11_8 auto:cdsdisk    -           -            online thinrclm
bash-3.2#
```

Step 4 Run the **vxdisk list** *device* command and check whether the number of paths and path status are correct (consistent with the actual configuration). In the following example, there are 16 paths (**hdisk3** to **hdisk18**) to the aggregated LUN, and all paths are enabled.

```
bash-3.2# vxdisk list huawei-xsg11_8
Device:    huawei-xsg11_8
devicetag: huawei-xsg11_8
type:      auto
hostid:
disk:      name= id=1293226805.9.aix
group:     name= id=
info:      format=cdsdisk,privoffset=256
flags:     online ready private autoconfig autoimport thinrclm
pubpaths:  block=/dev/vx/dmp/huawei-xsg11_8 char=/dev/vx/rdmp/huawei-xsg11_8
guid:      {5ee70f22-0fa6-11e0-9fc9-1772d74b5b9a}
udid:      HUAWEI%5FXSG1%5F2100238256791322%5F623825610079132200216l2B00000000
site:      -
version:   3.1
iosize:    min=512 (bytes) max=512 (blocks)
public:    slice=0 offset=65792 len=209639920 disk_offset=0
private:   slice=0 offset=256 len=65536 disk_offset=0
update:    time=1293226805 seqno=0.2
ssb:       actual_seqno=0.0
headers:   0 240
configs:   count=1 len=48144
logs:      count=1 len=7296
Defined regions:
 config   priv 000048-000239[000192]: copy=01 offset=000000 disabled
 config   priv 000256-048207[047952]: copy=01 offset=000192 disabled
 log      priv 048208-055503[007296]: copy=01 offset=000000 disabled
 lockrgn  priv 055504-055647[000144]: part=00 offset=000000
Multipathing information:
numpaths:  16
hdisk10         state=enabled
hdisk7          state=enabled
hdisk8          state=enabled
hdisk9          state=enabled
hdisk6          state=enabled
hdisk5          state=enabled
hdisk3          state=enabled
hdisk4          state=enabled
hdisk12         state=enabled
hdisk11         state=enabled
hdisk13         state=enabled
hdisk14         state=enabled
```



```
hdisk15      state=enabled
hdisk16      state=enabled
hdisk17      state=enabled
hdisk18      state=enabled
bash-3.2#
```

Step 5 Run the **vxdmpadm listenclosure all** command. The command output shows that **ENCLR_NAME** of the HyperMetro storage systems is correctly aggregated and **ARRAY_TYPE** is correctly identified. In the following example, **ARRAY_TYPE** is **AA**, and the HyperMetro storage systems are correctly aggregated into **huawei-xsg11**.

```
bash-3.2# vxdmpadm listenclosure all
ENCLR_NAME        ENCLR_TYPE     ENCLR_SNO      STATUS       ARRAY_TYPE     LUN_COUNT     FIRMWARE
=============================================================================================
=============
disk              Disk           DISKS              CONNECTED    Disk       1         610A
huawei-xsg11      HUAWEI-XSG1    2100238256791322     CONNECTED    A/A        1         6000
bash-3.2#
```

----End

Verifying the Local Preferred Mode

Step 1 Run the **vxddladm listsupport all | grep huawei** command to verify the ASL installation. In the following example, the multipathing software has correctly identified **XSG1**.

```
bash-3.2# vxddladm listsupport all | grep huawei
libvxhuawei.so      HUAWEI, HUASY       S5100, S5300, S5500, S5600, S6800E, S8000, S8000-I, VIS6000,
S5500T, S5600T, S5800T, S6800T, S2600T, V1500, V1800, S2100, S2200T, S2300, S2300E, S2600, S3900-
M100, S3900-M200, S3900-M300, S5900-M100, S5900-M200, S6900-M100, Dorado2100, Dorado2100 G2,
Dorado5100, HVS85T, HVS88T, XSG1
bash-3.2#
```

Step 2 Run the **cfgmgr -v** and **vxdisk scandisks** commands at the OS and DMP layers respectively to scan for LUNs. Then run the **vxddladm list devices** command to check whether the disk corresponding to each sub-path is claimed by Veritas. In the following example, one LUN is mapped and has 16 sub-paths. **libvxhuawei.so** has identified 16 devices.

```
bash-3.2# vxddladm list devices
DEVICE            TARGET-ID    STATE   DDL-STATUS (ASL)
============================================================
hdisk3            -            Online  CLAIMED (libvxhuawei.so)
hdisk4            -            Online  CLAIMED (libvxhuawei.so)
hdisk5            -            Online  CLAIMED (libvxhuawei.so)
hdisk6            -            Online  CLAIMED (libvxhuawei.so)
hdisk7            -            Online  CLAIMED (libvxhuawei.so)
hdisk8            -            Online  CLAIMED (libvxhuawei.so)
hdisk9            -            Online  CLAIMED (libvxhuawei.so)
hdisk10           -            Online  CLAIMED (libvxhuawei.so)
hdisk11           -            Online  CLAIMED (libvxhuawei.so)
hdisk12           -            Online  CLAIMED (libvxhuawei.so)
hdisk13           -            Online  CLAIMED (libvxhuawei.so)
hdisk14           -            Online  CLAIMED (libvxhuawei.so)
hdisk15           -            Online  CLAIMED (libvxhuawei.so)
hdisk16           -            Online  CLAIMED (libvxhuawei.so)
hdisk17           -            Online  CLAIMED (libvxhuawei.so)
hdisk18           -            Online  CLAIMED (libvxhuawei.so)
hdisk0            -            Online  CLAIMED (Disk)
bash-3.2#
```

Step 3 Run the **vxdisk list** command to check whether HyperMetro LUNs on the host have been aggregated. The aggregated device can be identified as **huawei-xxx**. In the following example, DMP identifies an aggregated LUN as **huawei-xsg11_#**.

```
bash-3.2# vxdisk list
DEVICE       TYPE          DISK        GROUP       STATUS
```



```
aix_disk_0 auto:LVM       -          -          LVM
huawei-xsg11_8 auto:cdsdisk    -          -          online thinrclm
bash-3.2#
```

Step 4 Run the **vxdisk list** *device* command and check whether the number of paths and path status are correct (consistent with the actual configuration). The asymmetric mode involves preferred and non-preferred paths. You must check whether the status and number of both preferred and non-preferred paths are correct. In the following example, there are 16 paths (**hdisk3** to **hdisk18**) to the aggregated LUN, and all paths are enabled. The type of eight preferred paths is **active/optimized**, and that of eight non-preferred paths is **active/non-optimized**.

```
bash-3.2# vxdisk list huawei-xsg11_8
Device:    huawei-xsg11_8
devicetag: huawei-xsg11_8
type:      auto
hostid:
disk:      name= id=1293226805.9.aix722zj
group:     name= id=
info:      format=cdsdisk,privoffset=256
flags:     online ready private autoconfig autoimport thinrclm
pubpaths:  block=/dev/vx/dmp/huawei-xsg11_8 char=/dev/vx/rdmp/huawei-xsg11_8
guid:      {5ee70f22-0fa6-11e0-9fc9-1772d74b5b9a}
udid:      HUAWEI%5FXSG1%5F2100238256791322%5F623825610079132200216 12B00000000
site:      -
version:   3.1
iosize:    min=512 (bytes) max=512 (blocks)
public:    slice=0 offset=65792 len=209639920 disk_offset=0
private:   slice=0 offset=256 len=65536 disk_offset=0
update:    time=1293226805 seqno=0.2
ssb:       actual_seqno=0.0
headers:   0 240
configs:   count=1 len=48144
logs:      count=1 len=7296
Defined regions:
 config   priv 000048-000239[000192]: copy=01 offset=000000 disabled
 config   priv 000256-048207[047952]: copy=01 offset=000192 disabled
 log      priv 048208-055503[007296]: copy=01 offset=000000 disabled
 lockrgn  priv 055504-055647[000144]: part=00 offset=000000
Multipathing information:
numpaths:  16
hdisk18        state=enabled   type=active/non-optimized
hdisk16        state=enabled   type=active/non-optimized
hdisk17        state=enabled   type=active/non-optimized
hdisk14        state=enabled   type=active/optimized(p)
hdisk15        state=enabled   type=active/non-optimized
hdisk13        state=enabled   type=active/optimized(p)
hdisk11        state=enabled   type=active/optimized(p)
hdisk12        state=enabled   type=active/optimized(p)
hdisk10        state=enabled   type=active/non-optimized
hdisk9         state=enabled   type=active/non-optimized
hdisk7         state=enabled   type=active/non-optimized
hdisk8         state=enabled   type=active/non-optimized
hdisk4         state=enabled   type=active/optimized(p)
hdisk5         state=enabled   type=active/optimized(p)
hdisk3         state=enabled   type=active/optimized(p)
hdisk6         state=enabled   type=active/optimized(p)
bash-3.2#
```

Step 5 Run the **vxdmpadm listenclosure all** command. The command output shows that **ENCLR_NAME** of the HyperMetro storage systems is correctly aggregated and **ARRAY_TYPE** is correctly identified. In the following example, **ARRAY_TYPE** is **ALUA**, and the HyperMetro storage systems are correctly aggregated into **huawei-xsg11**.

```
bash-3.2# vxdmpadm listenclosure all
ENCLR_NAME       ENCLR_TYPE     ENCLR_SNO      STATUS       ARRAY_TYPE     LUN_COUNT    FIRMWARE
================================================================================
```



```
=============
disk          Disk        DISKS             CONNECTED    Disk      1       610A
huawei-xsg11  HUAWEI-XSG1  2100238256791322  CONNECTED    ALUA      1       6000
bash-3.2#
```

----End

7.7.2 Red Hat

7.7.2.1 Storage System Configuration

If DMP is used, retain the default settings of the initiator and configure **Host Access Mode** and **Preferred Path for HyperMetro** as required. **Table 7-24** lists the detailed settings.

Table 7-24 Storage configurations for interconnection with Red Hat application servers

DMP	HyperMetro Working Mode	Storage System	OS Setting	Host Access Mode	Preferred Path for HyperMetro	Description
DMP 6.0.x to DMP 7.0	Load balancing mode	Local storage	Linux	Load balancing	N/A	The host uses all paths of a disk with equal priority.
		Remote storage	Linux	Load balancing	N/A	
DMP 7.1 or later	Load balancing mode	Local storage	Linux	Load balancing	N/A	
		Remote storage	Linux	Load balancing	N/A	
	Local preferred mode	Local storage	Linux	Asymmetric	Yes	The host considers the paths from the local storage system as preferred paths, and those from the remote storage system as non-preferred paths.
		Remote storage	Linux	Asymmetric	No	

NOTE

- Use **Huawei Storage Interoperability Navigator** to query the combinations supported by DMP.
- If a LUN has been mapped to a host, you must restart the host for the configuration to take effect after you modify **Host Access Mode** or **Preferred Path for HyperMetro**. If the host is running services, stop the services and export the disk group before restarting the host. If you configure the initiator for the first time, restart is not needed.
- To change the LUN mapping on the storage system, including but not limited to changing the host LUN ID, changing the port online, and removing and adding a LUN, follow the instructions in "LUN Information Fails to Be Updated After LUN Replacement" in the ***Host Connectivity Guide*** to correctly change the LUN mapping. Otherwise, services may be interrupted.
- If you do not use the recommended configurations, DMP may fail to identify and process paths properly.
- If DMP 7.x is used and **Host Access Mode** is set to **Asymmetric**, the maximum number of online FC and Ethernet ports supported by a single storage system or two HyperMetro storage systems is limited because the default RTPG buffer length of Veritas VxVM (DMP) is 255. If the number of online ports is greater than the allowed value, paths may not be properly identified. For details, contact Huawei engineers.

Configuring the Load Balancing Mode

The method for configuring the load balancing mode when DMP is used is the same as that when the OS native multipathing software is used.

Configuring the Local Preferred Mode

The method for configuring the local preferred mode when DMP is used is the same as that when the OS native multipathing software is used.

7.7.2.2 Host Configuration

Pre-installation Check

DMP cannot coexist with the operating system's native multipathing software. Before installing DMP, you must disable the OS native multipathing software. You can use the following methods to check whether the native multipathing software of Red Hat has been disabled.

For RHEL 6 and earlier versions, run the following command on the host:

```
[root@rhel6u91 ~]# /etc/init.d/multipathd status
multipathd (pid  6831) is running...
```

NOTICE

The preceding command output indicates that the native multipathing software has been enabled. You must stop services and run the **/etc/init.d/multipathd stop** command to disable it.

If the status of **multipathd** is **stopped**, the native multipathing software has been disabled.


```
[root@rhel6u91 ~]# /etc/init.d/multipathd stop
Stopping multipathd daemon:                                [  OK  ]
[root@rhel6u91 ~]# /etc/init.d/multipathd status
multipathd is stopped
```

After disabling the native multipathing software, forbid it to run automatically at system startup using the following command:

```
chkconfig multipathd off
```

For RHEL 7, run the following command on the host:

```
[root@rhel76 ~]# systemctl status multipathd
  multipathd.service - Device-Mapper Multipath Device Controller
  Loaded: loaded (/usr/lib/systemd/system/multipathd.service; enabled; vendor preset: enabled)
  Active: inactive (dead)
Condition: start condition failed at Wed 2015-09-16 00:27:29 CST; 3s ago
       ConditionPathExists=/etc/multipath.conf was not met
[root@rhel76 ~]#
```

NOTICE

In the preceding command output, **inactive** indicates that the native multipathing software has been disabled. If it is enabled, you must stop services and run the **systemctl stop multipathd.service** command to disable it.

After disabling the native multipathing software, forbid it to run automatically at system startup using the following command:

```
systemctl disable multipathd.service
```

Installing ASL

DMP is generally integrated in the Veritas Storage Foundation/InfoScale software package and is used together with the Veritas Volume Manager (VxVM) and Veritas File System (VxFS).

In this document, installing Veritas Storage Foundation 7.3.1 in RHEL 7.4 is used as an example. For details on how to install Veritas Storage Foundation 7.3.1, see the **Veritas Storage Foundation Installation Guide**.

After installing Veritas Storage Foundation, install Array Support Library (ASL), which provides array-specific support for DMP. ASL is a shared library that can be dynamically loaded. When discovering devices, ASL implements hardware-specific logic to discover device properties.

You are advised to install the latest version of ASL. You can obtain the ASL installation package for Huawei storage from **https://sort.veritas.com/asl**. ASL can be installed online or offline. Install ASL by following instructions in the **Readme** file on the official download page. The default path selection policy is MinimumQ.

NOTE

- Veritas AVID does not support Huawei storage.
- DMP provides the **MinimumQ** and **Round-Robin** path selection algorithms, which can be modified based on customer service configurations. You can run the **vxdmpadm setattr ENCLR_NAME iopolicy=*xxx*** command to modify the path selection algorithm. *xxx* indicates the path selection algorithm, which can be **MinimumQ** or **Round-Robin**.

7.7.2.3 Verification

Verifying the Load Balancing Mode

Step 1 Run the **vxddladm listsupport all | grep huawei** command to verify the ASL installation. In the following example, the multipathing software has correctly identified **XSG1**.

```
[root@localhost ~]# vxddladm listsupport all | grep huawei
libvxhuawei.so       HUAWEI, HUASY       S5100, S5300, S5500, S5600, S6800E, S8000, S8000-I, VIS6000, S5500T, S5600T, S5800T, S6800T, S2600T, V1500, V1800, S2100, S2200T, S2300, S2300E, S2600, S3900-M100, S3900-M200, S3900-M300, S5900-M100, S5900-M200, S6900-M100, Dorado2100, Dorado2100 G2, Dorado5100, HVS85T, HVS88T, XSG1
[root@localhost ~]#
```

Step 2 Scan for LUNs at the OS layer and run the **vxdisk scandisks** command to scan for LUNs at the DMP layer. Then run the **vxddladm list devices** command to check whether the disk corresponding to each sub-path is claimed by Veritas. In the following example, one LUN is mapped and has 16 sub-paths. **libvxhuawei.so** has identified 16 online claimed devices.

```
[root@localhost ~]# vxddladm list devices
DEVICE              TARGET-ID    STATE   DDL-STATUS (ASL)
============================================================
sda                 -            Online  CLAIMED (Disk)
sde                 c14_p8_t0    Online  CLAIMED (libvxhuawei.so)
sdb                 c14_p7_t0    Online  CLAIMED (libvxhuawei.so)
sdg                 c14_p6_t0    Online  CLAIMED (libvxhuawei.so)
sdi                 c14_p5_t0    Online  CLAIMED (libvxhuawei.so)
sdn                 c14_p4_t0    Online  CLAIMED (libvxhuawei.so)
sdo                 c14_p3_t0    Online  CLAIMED (libvxhuawei.so)
sdq                 c14_p2_t0    Online  CLAIMED (libvxhuawei.so)
sdp                 c14_p1_t0    Online  CLAIMED (libvxhuawei.so)
sdj                 c13_p8_t0    Online  CLAIMED (libvxhuawei.so)
sdl                 c13_p7_t0    Online  CLAIMED (libvxhuawei.so)
sdk                 c13_p6_t0    Online  CLAIMED (libvxhuawei.so)
sdm                 c13_p5_t0    Online  CLAIMED (libvxhuawei.so)
sdc                 c13_p4_t0    Online  CLAIMED (libvxhuawei.so)
sdh                 c13_p3_t0    Online  CLAIMED (libvxhuawei.so)
sdd                 c13_p2_t0    Online  CLAIMED (libvxhuawei.so)
sdf                 c13_p1_t0    Online  CLAIMED (libvxhuawei.so)
```

Step 3 Run the **vxdisk list** command to check whether HyperMetro LUNs on the host have been aggregated. The aggregated device can be identified as **huawei-xxx**. In the following example, DMP identifies an aggregated LUN as **huawei-xsg10_#**.

```
[root@localhost ~]# vxdisk list
DEVICE          TYPE           DISK         GROUP        STATUS
huawei-xsg10_6 auto:cdsdisk    -            -            online thinrclm
rhel74_disk_0 auto:LVM         -            -            LVM
```

Step 4 Run the **vxdisk list** *device* command and check whether the number of paths and path status are correct (consistent with the actual configuration). In the following example, there are 16 paths to the aggregated LUN, and all paths are enabled.

```
[root@localhost ~]# vxdisk list huawei-xsg10_6
Device:    huawei-xsg10_6
devicetag: huawei-xsg10_6
type:      auto
hostid:
disk:      name= id=1577437518.9.rhel74
group:     name= id=
info:      format=cdsdisk,privoffset=256,pubslice=3,privslice=3
flags:     online ready private autoconfig autoimport thinrclm
pubpaths:  block=/dev/vx/dmp/huawei-xsg10_6s3 char=/dev/vx/rdmp/huawei-xsg10_6s3
guid:      {00ad10d2-2888-11ea-a4e8-5cbfb51fcbab}
udid:      HUAWEI%5FXSG1%5F2100238256791322%5F6238256100791322000FAA840000001C
```



```
site:      -
version:   3.1
iosize:    min=512 (bytes) max=1024 (blocks)
public:    slice=3 offset=65792 len=209639920 disk_offset=0
private:   slice=3 offset=256 len=65536 disk_offset=0
update:    time=1577437518 seqno=0.2
ssb:       actual_seqno=0.0
headers:   0 240
configs:   count=1 len=51360
logs:      count=1 len=4096
Defined regions:
 config    priv 000048-000239[000192]: copy=01 offset=000000 disabled
 config    priv 000256-051423[051168]: copy=01 offset=000192 disabled
 log       priv 051424-055519[004096]: copy=01 offset=000000 disabled
 lockrgn   priv 055520-055663[000144]: part=00 offset=000000
Multipathing information:
numpaths:  16
sdh          state=enabled
sdf          state=enabled
sdd          state=enabled
sdc          state=enabled
sdb          state=enabled
sdg          state=enabled
sde          state=enabled
sdi          state=enabled
sdn          state=enabled
sdp          state=enabled
sdo          state=enabled
sdj          state=enabled
sdk          state=enabled
sdl          state=enabled
sdm          state=enabled
sdq          state=enabled
[root@localhost ~]#
```

Step 5 Run the **vxdmpadm listenclosure all** command. The command output shows that **ENCLR_NAME** of the HyperMetro storage systems is correctly aggregated and **ARRAY_TYPE** is correctly identified. In the following example, **ARRAY_TYPE** is **AA**, and the HyperMetro storage systems are correctly aggregated into **huawei-xsg10**.

```
[root@localhost ~]# vxdmpadm listenclosure all
ENCLR_NAME        ENCLR_TYPE     ENCLR_SNO      STATUS       ARRAY_TYPE     LUN_COUNT     FIRMWARE
================================================================================================
=============
disk              Disk           DISKS              CONNECTED    Disk       1         4.21
huawei-xsg10      HUAWEI-XSG1    2100238256791322     CONNECTED    A/A        1         6000
[root@localhost ~]#
```

----End

Verifying the Local Preferred Mode

Step 1 Run the **vxddladm listsupport all | grep huawei** command to verify the ASL installation. In the following example, the multipathing software has correctly identified **XSG1**.

```
[root@localhost ~]# vxddladm listsupport all | grep huawei
libvxhuawei.so       HUAWEI, HUASY        S5100, S5300, S5500, S5600, S6800E, S8000, S8000-I, VIS6000,
S5500T, S5600T, S5800T, S6800T, S2600T, V1500, V1800, S2100, S2200T, S2300, S2300E, S2600, S3900-
M100, S3900-M200, S3900-M300, S5900-M100, S5900-M200, S6900-M100, Dorado2100, Dorado2100 G2,
Dorado5100, HVS85T, HVS88T, XSG1
[root@localhost ~]#
```

Step 2 Scan for LUNs at the OS layer and run the **vxdisk scandisks** command to scan for LUNs at the DMP layer. Then run the **vxddladm list devices** command to check whether the disk corresponding to each sub-path is claimed by Veritas. In the

following example, one LUN is mapped and has 16 sub-paths. **libvxhuawei.so** has identified 16 devices.

```
[root@localhost ~]# vxddladm list devices
DEVICE              TARGET-ID    STATE   DDL-STATUS (ASL)
============================================================
sda                 -            Online  CLAIMED (Disk)
sdo                 c14_p8_t0    Online  CLAIMED (libvxhuawei.so)
sdp                 c14_p7_t0    Online  CLAIMED (libvxhuawei.so)
sdn                 c14_p6_t0    Online  CLAIMED (libvxhuawei.so)
sde                 c14_p5_t0    Online  CLAIMED (libvxhuawei.so)
sdb                 c14_p4_t0    Online  CLAIMED (libvxhuawei.so)
sdq                 c14_p3_t0    Online  CLAIMED (libvxhuawei.so)
sdg                 c14_p2_t0    Online  CLAIMED (libvxhuawei.so)
sdi                 c14_p1_t0    Online  CLAIMED (libvxhuawei.so)
sdh                 c13_p8_t0    Online  CLAIMED (libvxhuawei.so)
sdd                 c13_p7_t0    Online  CLAIMED (libvxhuawei.so)
sdf                 c13_p6_t0    Online  CLAIMED (libvxhuawei.so)
sdj                 c13_p5_t0    Online  CLAIMED (libvxhuawei.so)
sdc                 c13_p4_t0    Online  CLAIMED (libvxhuawei.so)
sdl                 c13_p3_t0    Online  CLAIMED (libvxhuawei.so)
sdk                 c13_p2_t0    Online  CLAIMED (libvxhuawei.so)
sdm                 c13_p1_t0    Online  CLAIMED (libvxhuawei.so)
[root@localhost ~]#
```

Step 3 Run the **vxdisk list** command to check whether HyperMetro LUNs on the host have been aggregated. The aggregated device can be identified as **huawei-xxx**. In the following example, DMP identifies an aggregated LUN as **huawei-xsg10_#**.

```
[root@localhost ~]# vxdisk list
DEVICE          TYPE            DISK         GROUP        STATUS
huawei-xsg10_6 auto:cdsdisk    -            -            online thinrclm
rhel74_disk_0 auto:LVM         -            -            LVM
```

Step 4 Run the **vxdisk list** *device* command and check whether the number of paths and path status are correct (consistent with the actual configuration). The asymmetric mode involves preferred and non-preferred paths. You must check whether the status and number of both preferred and non-preferred paths are correct. In the following example, there are 16 paths to the aggregated LUN, and all paths are enabled. The type of eight preferred paths is **active/optimized**, and that of eight non-preferred paths is **active/non-optimized**.

```
[root@localhost ~]# vxdisk list huawei-xsg10_6
Device:    huawei-xsg10_6
devicetag: huawei-xsg10_6
type:      auto
hostid:
disk:      name= id=1577437518.9.rhel74
group:     name= id=
info:      format=cdsdisk,privoffset=256,pubslice=3,privslice=3
flags:     online ready private autoconfig autoimport thinrclm
pubpaths:  block=/dev/vx/dmp/huawei-xsg10_6s3 char=/dev/vx/rdmp/huawei-xsg10_6s3
guid:      {00ad10d2-2888-11ea-a4e8-5cbfb51fcbab}
udid:      HUAWEI%5FXSG1%5F2100238256791322%5F623825610079132200 0FAA840000001C
site:      -
version:   3.1
iosize:    min=512 (bytes) max=1024 (blocks)
public:    slice=3 offset=65792 len=209639920 disk_offset=0
private:   slice=3 offset=256 len=65536 disk_offset=0
update:    time=1577437518 seqno=0.2
ssb:       actual_seqno=0.0
headers:   0 240
configs:   count=1 len=51360
logs:      count=1 len=4096
Defined regions:
 config   priv 000048-000239[000192]: copy=01 offset=000000 disabled
 config   priv 000256-051423[051168]: copy=01 offset=000192 disabled
 log      priv 051424-055519[004096]: copy=01 offset=000000 disabled
 lockrgn  priv 055520-055663[000144]: part=00 offset=000000
```



```
Multipathing information:
numpaths:  16
sdq         state=enabled    type=active/non-optimized
sdar        state=enabled    type=active/non-optimized
sdc         state=enabled    type=active/non-optimized
sdal        state=enabled    type=active/non-optimized
sdn         state=enabled    type=active/non-optimized
sdas        state=enabled    type=active/non-optimized
sde         state=enabled    type=active/non-optimized
sdam        state=enabled    type=active/non-optimized
sdw         state=enabled    type=active/optimized(p)
sdo         state=enabled    type=active/optimized(p)
sdac        state=enabled    type=active/optimized(p)
sdd         state=enabled    type=active/optimized(p)
sdb         state=enabled    type=active/optimized(p)
sdv         state=enabled    type=active/optimized(p)
sdp         state=enabled    type=active/optimized(p)
sdab        state=enabled    type=active/optimized(p)
[root@localhost ~]#
```

Step 5 Run the **vxdmpadm listenclosure all** command. The command output shows that **ENCLR_NAME** of the HyperMetro storage systems is correctly aggregated and **ARRAY_TYPE** is correctly identified. In the following example, **ARRAY_TYPE** is **ALUA**, and the HyperMetro storage systems are correctly aggregated into **huawei-xsg10**.

```
[root@localhost ~]# vxdmpadm listenclosure all
ENCLR_NAME        ENCLR_TYPE     ENCLR_SNO      STATUS       ARRAY_TYPE     LUN_COUNT     FIRMWARE
=============================================================================================
=============
disk              Disk           DISKS              CONNECTED    Disk       1         4.21
huawei-xsg10      HUAWEI-XSG1    2100238256791322   CONNECTED    ALUA       1         6000
[root@localhost ~]#
```

----End

7.7.3 Solaris

7.7.3.1 Storage System Configuration

If DMP is used, retain the default settings of the initiator and configure **Host Access Mode** and **Preferred Path for HyperMetro** as required. **Table 7-25** lists the detailed settings.

Table 7-25 Configurations of storage systems earlier than 6.1.3 for interconnection with Solaris application servers

DMP	HyperMetro Working Mode	Storage System	OS Setting	Host Access Mode	Preferred Path for HyperMetro	Description
DMP 7.1 or later	Load balancing mode	Local storage	Solaris	Asymmetric	Yes	The host uses all paths of a disk with equal priority.
		Remote storage	Solaris	Asymmetric	Yes	
	Local preferred mode	Local storage	Solaris	Asymmetric	Yes	The host considers the paths from the

DMP	HyperMetro Working Mode	Storage System	OS Setting	Host Access Mode	Preferred Path for HyperMetro	Description
		Remote storage	Solaris	Asymmetric	No	local storage system as preferred paths, and those from the remote storage system as non-preferred paths.

Table 7-26 Configurations of storage systems 6.1.3 or later for interconnection with Solaris application servers

DMP	HyperMetro Working Mode	Storage System	OS Setting	Host Access Mode	Preferred Path for HyperMetro	Description
DMP 7.1 or later	Load balancing mode	Local storage	Solaris	Load balancing	N/A	The host uses all paths of a disk with equal priority.
		Remote storage	Solaris	Load balancing	N/A	
	Local preferred mode	Local storage	Solaris	Asymmetric	Yes	The host considers the paths from the local storage system as preferred paths, and those from the remote storage system as non-preferred paths.
		Remote storage	Solaris	Asymmetric	No	

NOTE

- Use **Huawei Storage Interoperability Navigator** to query the combinations supported by DMP.
- DMP earlier than 7.1 does not support HyperMetro.
- In asymmetric mode, HyperMetro does not support VCS clusters.
- If a LUN has been mapped to a host, you must restart the host for the configuration to take effect after you modify **Host Access Mode** or **Preferred Path for HyperMetro**. If the host is running services, stop the services and export the disk group before restarting the host. If you configure the initiator for the first time, restart is not needed.
- If you do not use the recommended configurations, DMP may fail to identify and process paths properly.
- If DMP 7.x is used and **Host Access Mode** is set to **Asymmetric**, the maximum number of online FC and Ethernet ports supported by a single storage system or two HyperMetro storage systems is limited because the default RTPG buffer length of Veritas VxVM (DMP) is 255. If the number of online ports is greater than the allowed value, paths may not be properly identified. For details, contact Huawei engineers.

Configuring the Load Balancing Mode

The method for configuring the load balancing mode when DMP is used is the same as that when the OS native multipathing software is used.

Configuring the Local Preferred Mode

The method for configuring the local preferred mode when DMP is used is the same as that when the OS native multipathing software is used.

7.7.3.2 Host Configuration

Pre-installation Check

DMP cannot coexist with the operating system's native multipathing software MPxIO. Before installing DMP, run the **stmsboot -L** command to check whether MPxIO (STMS) is disabled.

```
-bash-4.1#  stmsboot -L
stmsboot: MPXIO disabled
```

NOTICE

If MPxIO is not disabled, open the **/kernel/drv/fp.conf** configuration file and change **mpxio-disable** to **yes**. Then run the **stmsboot -d** command to disable STMS. When running **stmsboot**, choose **reboot** for the settings to take effect.

Installing ASL

DMP is generally integrated in the Veritas Storage Foundation/InfoScale software package and is used together with the Veritas Volume Manager (VxVM) and Veritas File System (VxFS).

In this document, installing Veritas InfoScale 7.3.1 in Solaris 11.3 for SPARC is used as an example. For details about how to install Veritas InfoScale 7.3.1, see **Veritas InfoScale Installation Guide**.

After installing Veritas InfoScale, install Array Support Library (ASL), which provides array-specific support for DMP. ASL is a shared library that can be dynamically loaded. When discovering devices, ASL implements hardware-specific logic to discover device properties.

You are advised to install the latest version of ASL. You can obtain the ASL installation package for Huawei storage from **https://sort.veritas.com/asl**. ASL can be installed online or offline. Install ASL by following instructions in the **Readme** file on the official download page. The default path selection policy is MinimumQ.

NOTE

- Veritas AVID does not support Huawei storage.
- After installing Veritas software, you need to modify **fp_offline_ticker** and **fcp_offline_delay** for **fp** and **fcp** drivers. The two parameters affect the I/O suspension time when a link fault occurs. You are advised to set both **fp_offline_ticker** and **fcp_offline_delay** to **10** based on the value ranges provided by Oracle. You can also set the two parameters based on service configurations. For details, see "How Can I Set the fp and fcp Drivers' Time Parameters That Determine How Long a Host Will Wait Before Offlining Disks Upon a Link Failure" in the ***Host Connectivity Guide***.
- ZFS file systems are not supported.
- DMP provides the **MinimumQ** and **Round-Robin** path selection algorithms, which can be modified based on customer service configurations. You can run the **vxdmpadm setattr ENCLR_NAME iopolicy=***xxx* command to modify the path selection algorithm. *xxx* indicates the path selection algorithm, which can be **MinimumQ** or **Round-Robin**.

7.7.3.3 Verification

Verifying the Load Balancing Mode

Step 1 Run the **vxddladm listsupport all | grep huawei** command to verify the ASL installation. In the following example, the multipathing software has correctly identified **XSG1**.

```
-bash-4.1# vxddladm listsupport all | grep huawei
libvxhuawei.so      HUAWEI, HUASY       S5100, S5300, S5500, S5600, S6800E, S8000, S8000-I, VIS6000, S5500T, S5600T, S5800T, S6800T, S2600T, V1500, V1800, S2100, S2200T, S2300, S2300E, S2600, S3900-M100, S3900-M200, S3900-M300, S5900-M100, S5900-M200, S6900-M100, Dorado2100, Dorado2100 G2, Dorado5100, HVS85T, HVS88T, XSG1
-bash-4.1#
```

Step 2 Run the **cfgadm -al** and **vxdisk scandisks** commands at the OS and DMP layers respectively to scan for LUNs. Then run the **vxddladm list devices** command to check whether the disk corresponding to each sub-path is claimed by Veritas. In the following example, one LUN is mapped and has 16 sub-paths. **libvxhuawei.so** has identified 16 devices.

```
-bash-4.1# vxddladm list devices
DEVICE            TARGET-ID    STATE   DDL-STATUS (ASL)
============================================================
c2t3d0s2          -            Online  CLAIMED (Disk)
c9t28011603042D0306d1s2 c9_p8_t0     Online  CLAIMED (libvxhuawei.so)
c9t28001603042D0306d1s2 c9_p7_t0     Online  CLAIMED (libvxhuawei.so)
c9t28F11603042D0306d1s2 c9_p6_t0     Online  CLAIMED (libvxhuawei.so)
c9t28F01603042D0306d1s2 c9_p5_t0     Online  CLAIMED (libvxhuawei.so)
```



```
c9t2211238256791322d1s2 c9_p4_t0     Online  CLAIMED (libvxhuawei.so)
c9t2210238256791322d1s2 c9_p3_t0     Online  CLAIMED (libvxhuawei.so)
c9t2001238256791322d1s2 c9_p2_t0     Online  CLAIMED (libvxhuawei.so)
c9t2000238256791322d1s2 c9_p1_t0     Online  CLAIMED (libvxhuawei.so)
c8t28011603042D0306d1s2 c8_p8_t0     Online  CLAIMED (libvxhuawei.so)
c8t28001603042D0306d1s2 c8_p7_t0     Online  CLAIMED (libvxhuawei.so)
c8t28F11603042D0306d1s2 c8_p6_t0     Online  CLAIMED (libvxhuawei.so)
c8t28F01603042D0306d1s2 c8_p5_t0     Online  CLAIMED (libvxhuawei.so)
c8t2211238256791322d1s2 c8_p4_t0     Online  CLAIMED (libvxhuawei.so)
c8t2210238256791322d1s2 c8_p3_t0     Online  CLAIMED (libvxhuawei.so)
c8t2001238256791322d1s2 c8_p2_t0     Online  CLAIMED (libvxhuawei.so)
c8t2000238256791322d1s2 c8_p1_t0     Online  CLAIMED (libvxhuawei.so)
-bash-4.1#
```

Step 3 Run the **vxdisk list** command to check whether HyperMetro LUNs on the host have been aggregated. The aggregated device can be identified as **huawei-xxx**. In the following example, DMP identifies an aggregated LUN as **huawei-xsg11_#**.

```
-bash-4.1# vxdisk list
DEVICE          TYPE          DISK        GROUP       STATUS
huawei-xsg11_0 auto:cdsdisk    -           -           online thinrclm
s113_disk_0  auto:ZFS       -           -           ZFS
```

Step 4 Run the **vxdisk list** *device* command and check whether the number of paths and path status are correct (consistent with the actual configuration). The following is an example when the storage version is earlier than 6.1.3. There are 16 paths (**cXtXdXsX**) to the aggregated LUN, and all paths are enabled.

```
-bash-4.1# vxdisk list huawei-xsg11_0
Device:    huawei-xsg11_0
devicetag: huawei-xsg11_0
type:      auto
hostid:
disk:      name= id=1577290545.6.S113
group:     name= id=
info:      format=cdsdisk,privoffset=256,pubslice=2,privslice=2
flags:     online ready private autoconfig autoimport thinrclm
pubpaths:  block=/dev/vx/dmp/huawei-xsg11_0s2 char=/dev/vx/rdmp/huawei-xsg11_0s2
guid:      {cdf68062-2731-11ea-bd1f-00144fec1884}
udid:      HUAWEI%5FXSG1%5F21001603042d0306%5F61603041002D030604F9505C0000000F
site:      -
version:   3.1
iosize:    min=512 (bytes) max=2048 (blocks)
public:    slice=2 offset=65792 len=209619712 disk_offset=0
private:   slice=2 offset=256 len=65536 disk_offset=0
update:    time=1577290545 seqno=0.2
ssb:       actual_seqno=0.0
headers:   0 240
configs:   count=1 len=48144
logs:      count=1 len=7296
Defined regions:
 config   priv 000048-000239[000192]: copy=01 offset=000000 disabled
 config   priv 000256-048207[047952]: copy=01 offset=000192 disabled
 log      priv 048208-055503[007296]: copy=01 offset=000000 disabled
 lockrgn  priv 055504-055647[000144]: part=00 offset=000000
Multipathing information:
numpaths:  16
c8t2000238256791322d1s2 state=enabled   type=active/optimized(p)
c8t2211238256791322d1s2 state=enabled   type=active/optimized(p)
c8t2001238256791322d1s2 state=enabled   type=active/optimized(p)
c8t2210238256791322d1s2 state=enabled   type=active/optimized(p)
c8t28001603042D0306d1s2 state=enabled   type=active/optimized(p)
c8t28011603042D0306d1s2 state=enabled   type=active/optimized(p)
c8t28F01603042D0306d1s2 state=enabled   type=active/optimized(p)
c8t28F11603042D0306d1s2 state=enabled   type=active/optimized(p)
c9t2210238256791322d1s2 state=enabled   type=active/optimized(p)
c9t2211238256791322d1s2 state=enabled   type=active/optimized(p)
c9t28F01603042D0306d1s2 state=enabled   type=active/optimized(p)
c9t28001603042D0306d1s2 state=enabled   type=active/optimized(p)
c9t2000238256791322d1s2 state=enabled   type=active/optimized(p)
```



```
c9t28F11603042D0306d1s2 state=enabled   type=active/optimized(p)
c9t28011603042D0306d1s2 state=enabled   type=active/optimized(p)
c9t2001238256791322d1s2 state=enabled   type=active/optimized(p)
-bash-4.1#
```

The following is an example when the storage version is 6.1.3 or later. There are 16 paths (**cXtXdXsX**) to the aggregated LUN, and all paths are enabled.

```
bash-3.2# vxdisk list huawei-xsg11_3
Device:    huawei-xsg11_3
devicetag: huawei-xsg11_3
type:      auto
hostid:
disk:      name= id=1652444225.5.sol10u11b
group:     name= id=
info:      format=cdsdisk,privoffset=256,pubslice=2,privslice=2
flags:     online ready private autoconfig autoimport thinrclm
pubpaths:  block=/dev/vx/dmp/huawei-xsg11_3s2 char=/dev/vx/rdmp/huawei-xsg11_3s2
guid:      {9a580090-d2b6-11ec-a86b-0010e0584fb2}
udid:      HUAWEI%5FXSG1%5F2100cc64a68314d3%5F6CC64A61008314D3099097B1000001DD
site:      -
version:   3.1
iosize:    min=512 (bytes) max=2048 (blocks)
public:    slice=2 offset=65792 len=209616640 disk_offset=0
private:   slice=2 offset=256 len=65536 disk_offset=0
update:    time=1652444270 seqno=0.2
ssb:       actual_seqno=0.0
headers:   0 240
configs:   count=1 len=48144
logs:      count=1 len=7296
Defined regions:
 config   priv 000048-000239[000192]: copy=01 offset=000000 disabled
 config   priv 000256-048207[047952]: copy=01 offset=000192 disabled
 log      priv 048208-055503[007296]: copy=01 offset=000000 disabled
 lockrgn  priv 055504-055647[000144]: part=00 offset=000000
Multipathing information:
numpaths:  16
c6t2018CC64A68314D3d4s2 state=enabled
c6t28F20A2B304438A8d4s2 state=enabled
c6t2019CC64A68314D3d4s2 state=enabled
c6t28130A2B304438A8d4s2 state=enabled
c6t28120A2B304438A8d4s2 state=enabled
c6t2008CC64A68314D3d4s2 state=enabled
c6t28F30A2B304438A8d4s2 state=enabled
c6t2009CC64A68314D3d4s2 state=enabled
c7t28120A2B304438A8d4s2 state=enabled
c7t28130A2B304438A8d4s2 state=enabled
c7t2008CC64A68314D3d4s2 state=enabled
c7t28F30A2B304438A8d4s2 state=enabled
c7t2018CC64A68314D3d4s2 state=enabled
c7t28F20A2B304438A8d4s2 state=enabled
c7t2019CC64A68314D3d4s2 state=enabled
c7t2009CC64A68314D3d4s2 state=enabled
```

----End

Verifying the Local Preferred Mode

Step 1 Run the **vxddladm listsupport all | grep huawei** command to verify the ASL installation. In the following example, the multipathing software has correctly identified **XSG1**.

```
-bash-4.1# vxddladm listsupport all | grep huawei
libvxhuawei.so       HUAWEI, HUASY       S5100, S5300, S5500, S5600, S6800E, S8000, S8000-I, VIS6000, S5500T, S5600T, S5800T, S6800T, S2600T, V1500, V1800, S2100, S2200T, S2300, S2300E, S2600, S3900-M100, S3900-M200, S3900-M300, S5900-M100, S5900-M200, S6900-M100, Dorado2100, Dorado2100 G2, Dorado5100, HVS85T, HVS88T, XSG1
-bash-4.1#
```


Step 2 Run the **cfgadm -al** and **vxdisk scandisks** commands at the OS and DMP layers respectively to scan for LUNs. Then run the **vxddladm list devices** command to check whether the disk corresponding to each sub-path is claimed by Veritas. In the following example, one LUN is mapped and has 16 sub-paths. **libvxhuawei.so** has identified 16 devices.

```
-bash-4.1# vxddladm list devices
DEVICE              TARGET-ID    STATE   DDL-STATUS (ASL)
============================================================
c2t3d0s2            -            Online  CLAIMED (Disk)
c9t28011603042D0306d1s2 c9_p8_t0     Online  CLAIMED (libvxhuawei.so)
c9t28001603042D0306d1s2 c9_p7_t0     Online  CLAIMED (libvxhuawei.so)
c9t28F11603042D0306d1s2 c9_p6_t0     Online  CLAIMED (libvxhuawei.so)
c9t28F01603042D0306d1s2 c9_p5_t0     Online  CLAIMED (libvxhuawei.so)
c9t2211238256791322d1s2 c9_p4_t0     Online  CLAIMED (libvxhuawei.so)
c9t2210238256791322d1s2 c9_p3_t0     Online  CLAIMED (libvxhuawei.so)
c9t2001238256791322d1s2 c9_p2_t0     Online  CLAIMED (libvxhuawei.so)
c9t2000238256791322d1s2 c9_p1_t0     Online  CLAIMED (libvxhuawei.so)
c8t28011603042D0306d1s2 c8_p8_t0     Online  CLAIMED (libvxhuawei.so)
c8t28001603042D0306d1s2 c8_p7_t0     Online  CLAIMED (libvxhuawei.so)
c8t28F11603042D0306d1s2 c8_p6_t0     Online  CLAIMED (libvxhuawei.so)
c8t28F01603042D0306d1s2 c8_p5_t0     Online  CLAIMED (libvxhuawei.so)
c8t2211238256791322d1s2 c8_p4_t0     Online  CLAIMED (libvxhuawei.so)
c8t2210238256791322d1s2 c8_p3_t0     Online  CLAIMED (libvxhuawei.so)
c8t2001238256791322d1s2 c8_p2_t0     Online  CLAIMED (libvxhuawei.so)
c8t2000238256791322d1s2 c8_p1_t0     Online  CLAIMED (libvxhuawei.so)
-bash-4.1#
```

Step 3 Run the **vxdisk list** command to check whether HyperMetro LUNs on the host have been aggregated. The aggregated device can be identified as **huawei-xxx**. In the following example, DMP identifies an aggregated LUN as **huawei-xsg11_#**.

```
-bash-4.1# vxdisk list
DEVICE          TYPE           DISK         GROUP        STATUS
huawei-xsg11_0 auto:cdsdisk    -            -            online thinrclm
s113_disk_0  auto:ZFS        -            -           ZFS
```

Step 4 Run the **vxdisk list** *device* command and check whether the number of paths and path status are correct (consistent with the actual configuration). The asymmetric mode involves preferred and non-preferred paths. You must check whether the status and number of both preferred and non-preferred paths are correct. In the following example, there are 16 paths to the aggregated LUN, and all paths are enabled. The type of eight preferred paths is **active/optimized**, and that of eight non-preferred paths is **active/non-optimized**.

```
-bash-4.1# vxdisk list huawei-xsg11_0
Device:    huawei-xsg11_0
devicetag: huawei-xsg11_0
type:      auto
hostid:
disk:      name= id=1577290545.6.S113
group:     name= id=
info:      format=cdsdisk,privoffset=256,pubslice=2,privslice=2
flags:     online ready private autoconfig autoimport thinrclm
pubpaths:  block=/dev/vx/dmp/huawei-xsg11_0s2 char=/dev/vx/rdmp/huawei-xsg11_0s2
guid:      {cdf68062-2731-11ea-bd1f-00144fec1884}
udid:      HUAWEI%5FXSG1%5F21001603042d0306%5F61603041002D030604F9505C0000000F
site:      -
version:   3.1
iosize:    min=512 (bytes) max=2048 (blocks)
public:    slice=2 offset=65792 len=209619712 disk_offset=0
private:   slice=2 offset=256 len=65536 disk_offset=0
update:    time=1577290545 seqno=0.2
ssb:       actual_seqno=0.0
headers:   0 240
configs:   count=1 len=48144
logs:      count=1 len=7296
Defined regions:
```



```
 config   priv 000048-000239[000192]: copy=01 offset=000000 disabled
 config   priv 000256-048207[047952]: copy=01 offset=000192 disabled
 log      priv 048208-055503[007296]: copy=01 offset=000000 disabled
 lockrgn  priv 055504-055647[000144]: part=00 offset=000000
Multipathing information:
numpaths:  16
c8t2000238256791322d1s2 state=enabled   type=active/non-optimized
c8t2211238256791322d1s2 state=enabled   type=active/non-optimized
c8t2001238256791322d1s2 state=enabled   type=active/non-optimized
c8t2210238256791322d1s2 state=enabled   type=active/non-optimized
c8t28001603042D0306d1s2 state=enabled   type=active/optimized(p)
c8t28011603042D0306d1s2 state=enabled   type=active/optimized(p)
c8t28F01603042D0306d1s2 state=enabled   type=active/optimized(p)
c8t28F11603042D0306d1s2 state=enabled   type=active/optimized(p)
c9t2210238256791322d1s2 state=enabled   type=active/non-optimized
c9t2211238256791322d1s2 state=enabled   type=active/non-optimized
c9t28F01603042D0306d1s2 state=enabled   type=active/optimized(p)
c9t28001603042D0306d1s2 state=enabled   type=active/optimized(p)
c9t2000238256791322d1s2 state=enabled   type=active/non-optimized
c9t28F11603042D0306d1s2 state=enabled   type=active/optimized(p)
c9t28011603042D0306d1s2 state=enabled   type=active/optimized(p)
c9t2001238256791322d1s2 state=enabled   type=active/non-optimized
```

Step 5 Run the **vxdmpadm listenclosure all** command. The command output shows that **ENCLR_NAME** of the HyperMetro storage systems is correctly aggregated and **ARRAY_TYPE** is correctly identified. In the following example, **ARRAY_TYPE** is **ALUA**, and the HyperMetro storage systems are correctly aggregated into **huawei-xsg11**.

```
-bash-4.1# vxdmpadm listenclosure all
ENCLR_NAME       ENCLR_TYPE     ENCLR_SNO      STATUS       ARRAY_TYPE     LUN_COUNT     FIRMWARE
================================================================================================
=============
disk             Disk           DISKS              CONNECTED    Disk       1        0603
huawei-xsg11     HUAWEI-XSG1    21001603042d0306     CONNECTED    ALUA       1        6000
```

----End

7.7.4 Windows

7.7.4.1 Storage System Configuration

If DMP is used, retain the default settings of the initiator and configure **Host Access Mode** and **Preferred Path for HyperMetro** as required. **Table 7-27** lists the detailed settings.

Table 7-27 Storage configurations for interconnection with Windows application servers

HyperMetro Working Mode	Storage System	OS Setting	Host Access Mode	Preferred Path for HyperMetro	Description
Load balancing mode	Local storage	Windows	Asymmetric	Yes	The host uses all paths of a disk with equal priority.
	Remote storage	Windows	Asymmetric	Yes	
Local preferred mode	Local storage	Windows	Asymmetric	Yes	The host considers the paths from the local storage system as

HyperMetro Working Mode	Storage System	OS Setting	Host Access Mode	Preferred Path for HyperMetro	Description
	Remote storage	Windows	Asymmetric	No	preferred paths, and those from the remote storage system as non-preferred paths.

NOTE

- Use **Huawei Storage Interoperability Navigator** to query the combinations supported by DMP.
- If a LUN has been mapped to a host, you must restart the host for the configuration to take effect after you modify the initiator parameters. If the host is running services, stop the services and export the disk group before restarting the host. If you configure the initiator for the first time, restart is not needed.
- If you do not use the recommended configurations, DMP may fail to identify and process paths properly.

Configuring the Load Balancing Mode

The method for configuring the load balancing mode when DMP is used is the same as that when the OS native multipathing software is used.

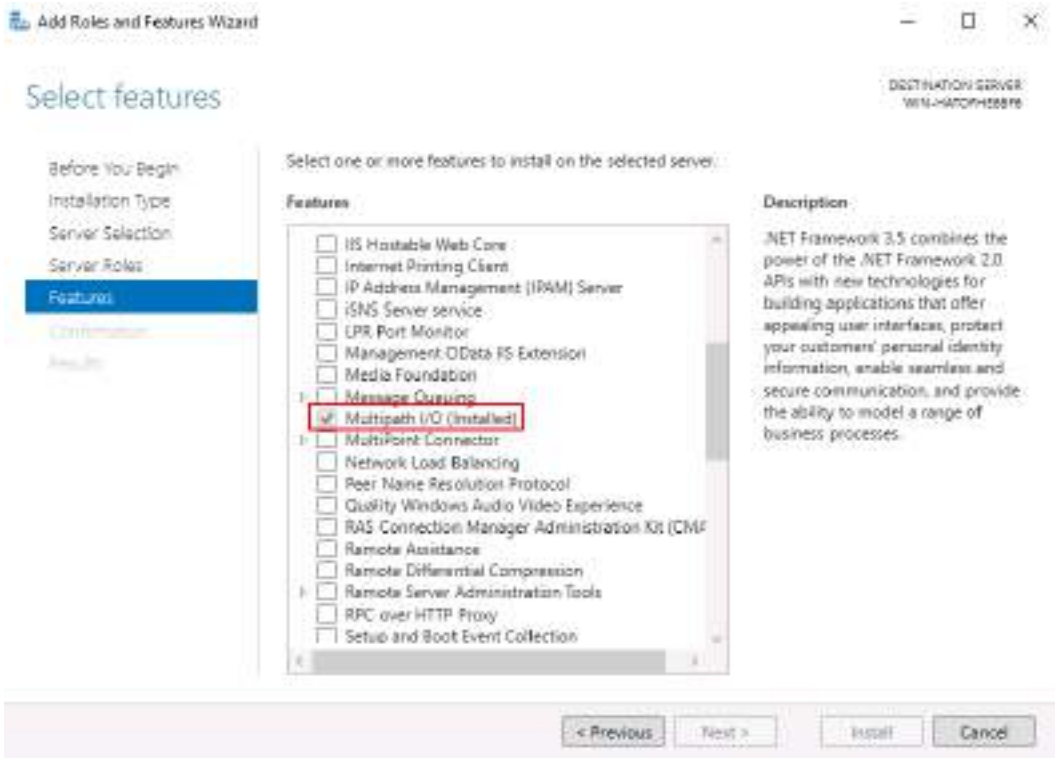
Configuring the Local Preferred Mode

The method for configuring the local preferred mode when DMP is used is the same as that when the OS native multipathing software is used.

7.7.4.2 Host Configuration

Install **Multipath I/O**.

Figure 7-92 Adding Multipath I/O



Then, install Veritas InfoScale. In this document, installing Veritas InfoScale 7.3.1 on Windows Server 2016 is used as an example. For details about the prerequisites and method for installing Veritas InfoScale 7.3.1, see **Veritas InfoScale Installation and Upgrade Guide**.

NOTICE

- After installing Storage Foundation/InfoScale, install Device Driver Installers (DDIs) for versions earlier than InfoScale 7.1. It is recommended that you install the latest version of DDIs. You can obtain the DDIs installation package from https://sort.veritas.com/asl. For InfoScale 7.1 and later versions, you do not need to install DDIs.
- After installing Storage Foundation/InfoScale and DDIs, install the DMP patches corresponding to the Storage Foundation/InfoScale version. **Table 7-28** provides the links for the patches.

Table 7-28 Links for DMP patches

Storage Foundation/ InfoScale Version	Applicable Windows Version	Patch Link	Remarks
Storage Foundation 6.0	Windows Server 2008 R2	**http://svlvault.veritas.com/cgi-bin/patch_central?archive=14248**	This patch is released on Veritas's internal website. You can obtain the patch from Veritas technical support engineers.
Storage Foundation 6.0.1	Windows Server 2008 R2	**http://svlvault.veritas.com/cgi-bin/patch_central?archive=14247**	This patch is released on Veritas's internal website. You can obtain the patch from Veritas technical support engineers.
Storage Foundation 6.0.2	Windows Server 2012	**https://sort.veritas.com/patch/detail/14246**	-
Storage Foundation 6.1	Windows Server 2008 R2 Windows Server 2012 Windows Server 2012 R2	**https://sort.veritas.com/patch/detail/14227**	-
InfoScale 7.0	Windows Server 2008 R2 Windows Server 2012 Windows Server 2012 R2	**https://sort.veritas.com/patch/detail/14201** **https://sort.veritas.com/patch/detail/14202**	-

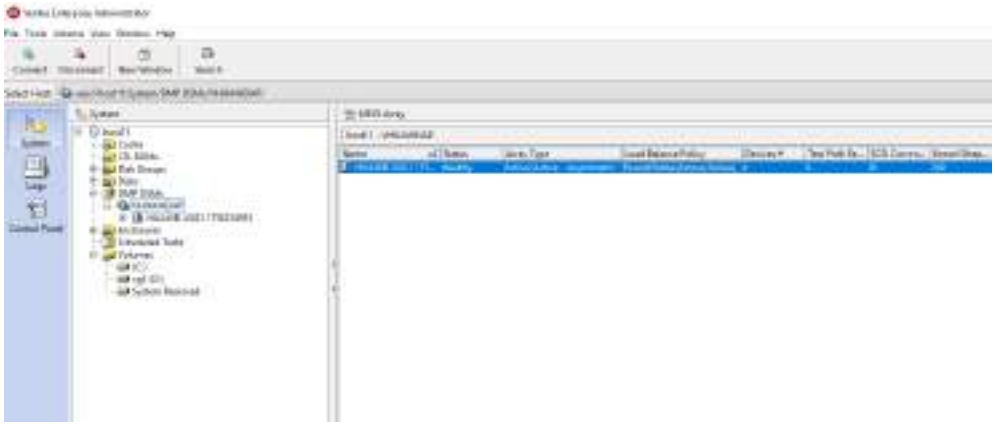
Storage Foundation/ InfoScale Version	Applicable Windows Version	Patch Link	Remarks
InfoScale 7.1	Windows Server 2008 R2 Windows Server 2012 Windows Server 2012 R2	**https://sort.veritas.com/patch/detail/14191**	-
InfoScale 7.2	Windows Server 2012 Windows Server 2012 R2 Windows Server 2016	**https://sort.veritas.com/patch/detail/14203**	-
InfoScale 7.3	Windows Server 2012 Windows Server 2012 R2 Windows Server 2016	**https://sort.veritas.com/patch/detail/14216**	-
InfoScale 7.3.1	Windows Server 2012 Windows Server 2012 R2 Windows Server 2016	**https://sort.veritas.com/patch/detail/14218**	-

7.7.4.3 Verification

Verifying the Load Balancing Mode

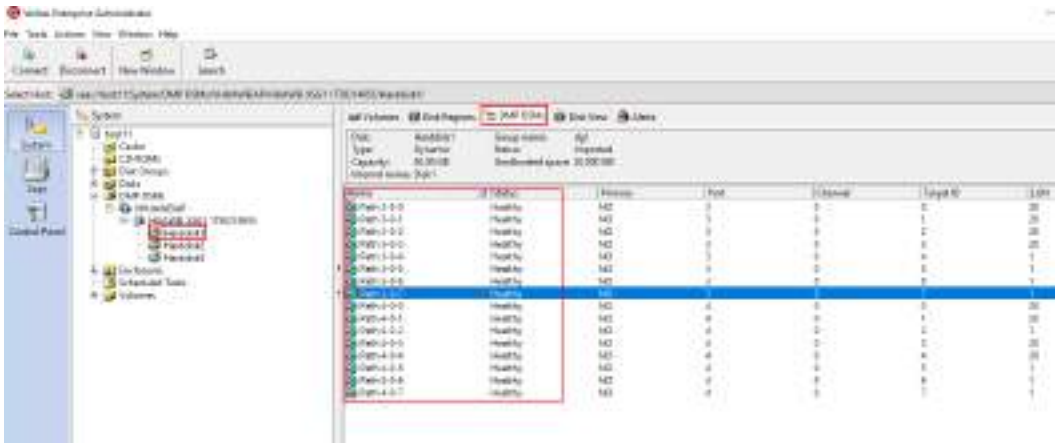
Step 1 After installing DDIs and patches, verify that **VHUAWEIAP** is displayed under **DMP DSMs**, **Array Type** is **Active/Active-Asymmetric**, and **Load Balance Policy** is **Round Robin(Active/Active)** on Veritas Enterprise Administrator.

Figure 7-93 Verifying that Huawei storage systems have been properly identified by DMP



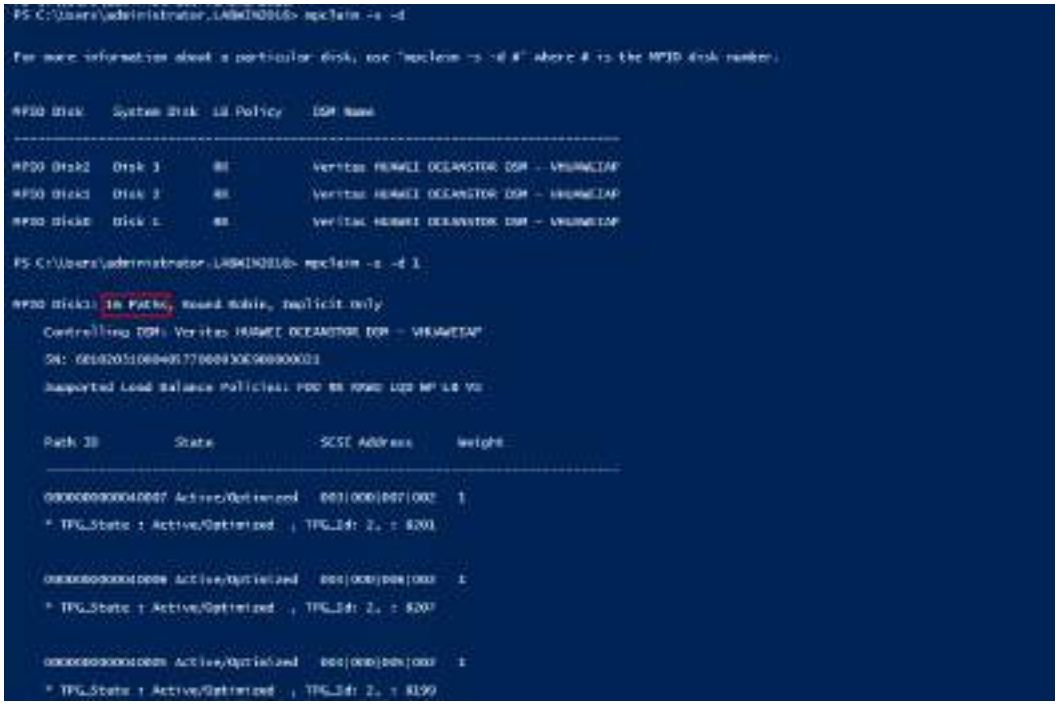
Step 2 Verify that HyperMetro LUNs have been aggregated on the host. As shown in Figure 7-94, HyperMetro LUNs have been aggregated into the **Harddisk1** disk. There are 16 paths in total for this aggregated disk, each of which is marked with a green dot. This indicates that I/Os can be delivered to all of these paths, implementing load balancing.

Figure 7-94 Querying path information about the aggregated disk on Veritas Enterprise Administrator



Alternatively, run the **mpclaim -s -d** command to check the path quantity and status.

Figure 7-95 Querying path information about the aggregated disk using the CLI



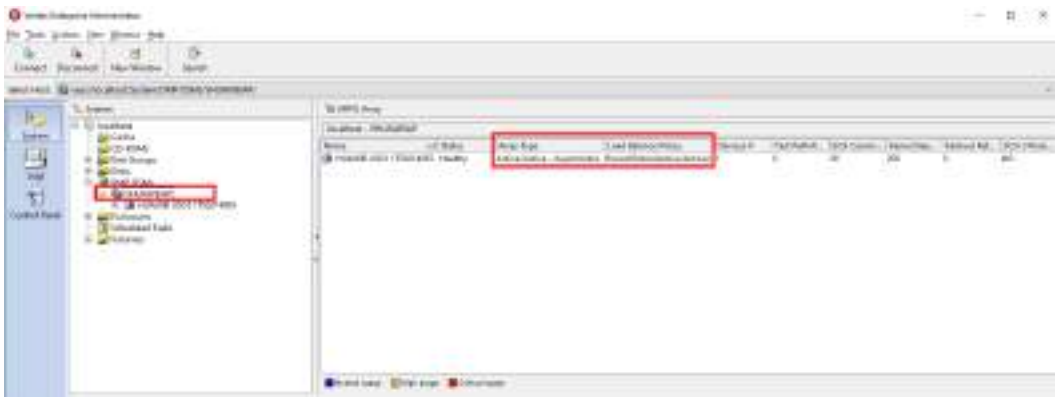
In the preceding command output, **LB Policy** is **Round Robin** and **State** of all paths is **Active/Optimized**, indicating that I/Os will be distributed on all of these paths for load balancing.

----End

Verifying the Local Preferred Mode

Step 1 After installing DDIs and patches, verify that **VHUAWEIAP** is displayed under **DMP DSMs**, **Array Type** is **Active/Active-Asymmetric**, and **Load Balance Policy** is **Round Robin(Active/Active)** on Veritas Enterprise Administrator.

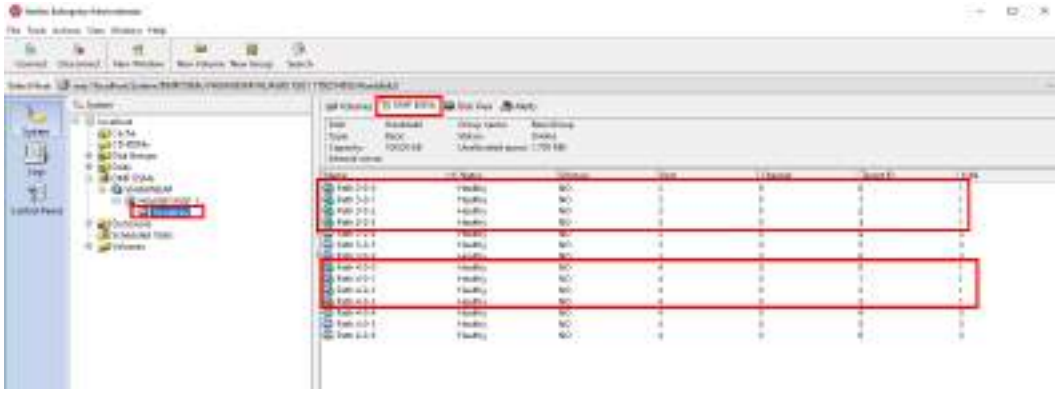
Figure 7-96 Verifying that Huawei storage systems have been properly identified by DMP



Step 2 Verify that HyperMetro LUNs have been aggregated on the host. As shown in Figure 7-97, HyperMetro LUNs have been aggregated into the **Harddisk2** disk. There are 14 paths in total for this aggregated disk, eight of which are marked

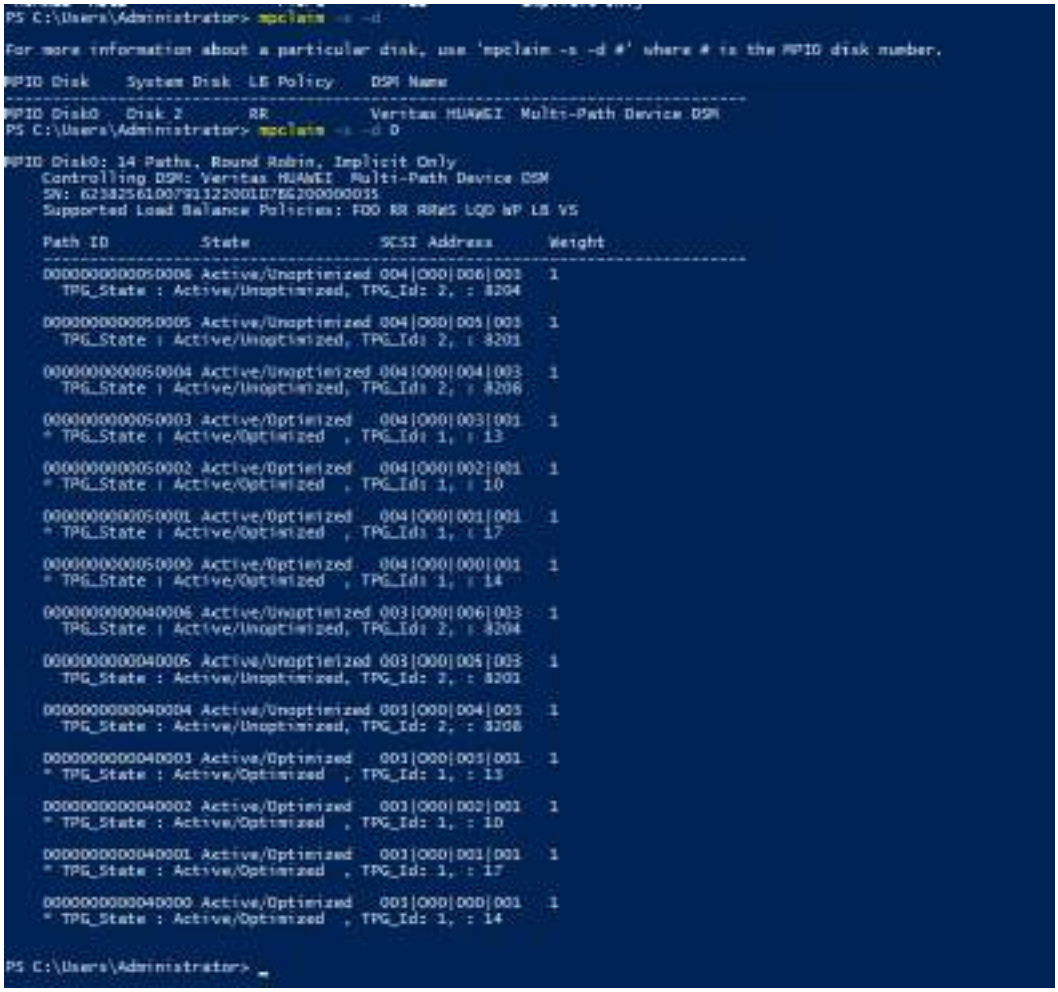
with green dots. This indicates that I/Os can be delivered to these eight paths, implementing load balancing. The six paths from the non-preferred storage system are not marked with green dots. They are non-preferred paths.

Figure 7-97 Querying path information about the aggregated disk on Veritas Enterprise Administrator



Alternatively, run the **mpclaim -s -d** command to check the path quantity and status.

Figure 7-98 Querying path information about the aggregated disk using the CLI



In the preceding command output, eight preferred paths (whose **LB Policy** is **Round Robin** and **TPG_State** is **Active/Optimized**) and six non-preferred paths (whose **TPG_State** is **Active/Unoptimized**) are displayed, indicating that the configuration has taken effect.

----End

8 Configuring the Replication Network

This section describes how to configure the switches to connect the HyperMetro replication network.

8.1 Configuring Fibre Channel Switches (Applicable to Fibre Channel Connections)

Fibre Channel switch configuration includes setting domain IDs, configuring the long-distance mode for links, and creating zones.

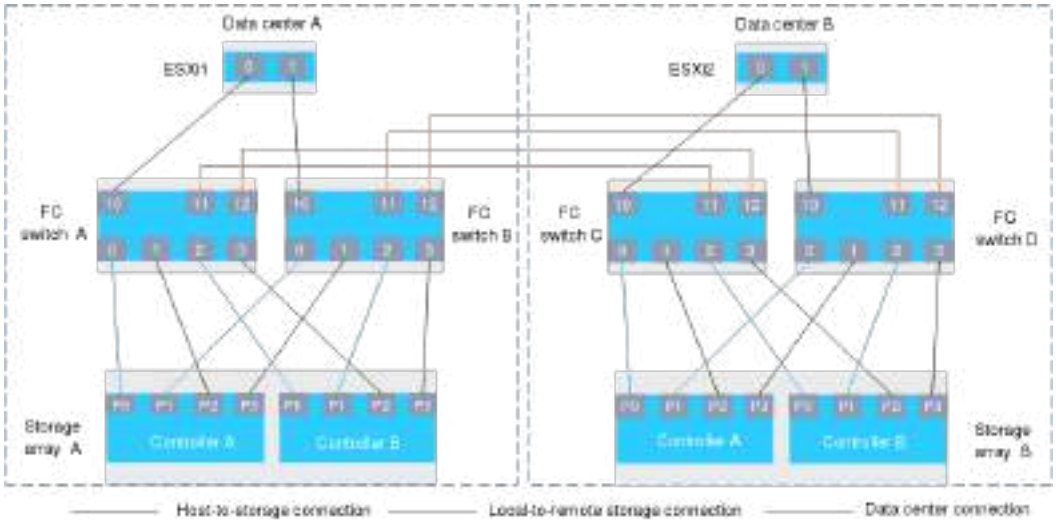
Prerequisites

The user names and passwords used to log in to Fibre Channel switches have been obtained.

Configurations for Entry-Level and Mid-Range Storage Models (Two Controllers)

Figure 8-1 shows the link planning.

Figure 8-1 Link planning



Four Fibre Channel switches are cascaded across active-active data centers, building a mirroring relationship between the storage arrays in the two data centers.

As shown in **Figure 8-1**, Fibre Channel switches A and C are cascaded across data centers through ports 11 and 12 on them. Fibre Channel switches B and D are cascaded across data centers through ports 11 and 12 on them.

Domain ID planning

If Fibre Channel switches are cascaded, domain IDs must be set to prevent ID conflicts on a network. A domain ID is the unique identifier of a Fibre Channel switch. **Table 8-1** describes the domain ID planning.

Table 8-1 Domain ID planning

Fibre Channel Switch (Example)	Domain ID (Example)
Fibre Channel switch A	1
Fibre Channel switch B	2
Fibre Channel switch C	3
Fibre Channel switch D	4

Zone planning

A zone allows specific switches and devices to communicate with each other. On two cascaded Fibre Channel switches, the ports of each link form a zone. Zone planning complies with the following principles:

- Each application host is connected to all the controllers of active-active storage arrays.
- Each controller on one storage array is physically and logically connected to each controller on the other storage array.

NOTE

If a port of the application host has multiple WWNs, plan zones based on WWNs.

Table 8-2 uses **Fibre Channel switches A and C as an example** to describe the zone planning.

Table 8-2 Service zones

Zone (Example)[a]	Zone Member[b]	Used To
ESXi1_0_StorageA_A_P2	(1, 10; 1, 1)	Connect controller A or B of storage array A to ESXi host 1.
ESXi1_0_StorageA_B_P2	(1, 10; 1, 3)	
ESXi1_0_StorageB_A_P2	(1, 10; 3, 1)	Connect controller A or B of storage array B to ESXi host 1.
ESXi1_0_StorageB_B_P2	(1, 10; 3, 3)	
ESXi2_0_StorageA_A_P2	(3, 10; 1, 1)	Connect controller A or B of storage array A to ESXi host 2.
ESXi2_0_StorageA_B_P2	(3, 10; 1, 3)	
ESXi2_0_StorageB_A_P2	(3, 10; 3, 1)	Connect controller A or B of storage array B to ESXi host 2.
ESXi2_0_StorageB_B_P2	(3, 10; 3, 3)	
a: The zone name **ESXi1_0_StorageA_A_P2** means the zone connects port 0 on ESXi host 1 to port P2 on controller A of storage array A. b: Zone members are expressed in the format of domain ID of Fibre Channel switch, port ID. For example, 1, 1 indicates port 1 on Fibre Channel switch 1.		

Table 8-3 uses **Fibre Channel switches A and C as an example** to describe the zone planning for the replication network.

Table 8-3 Replication zones

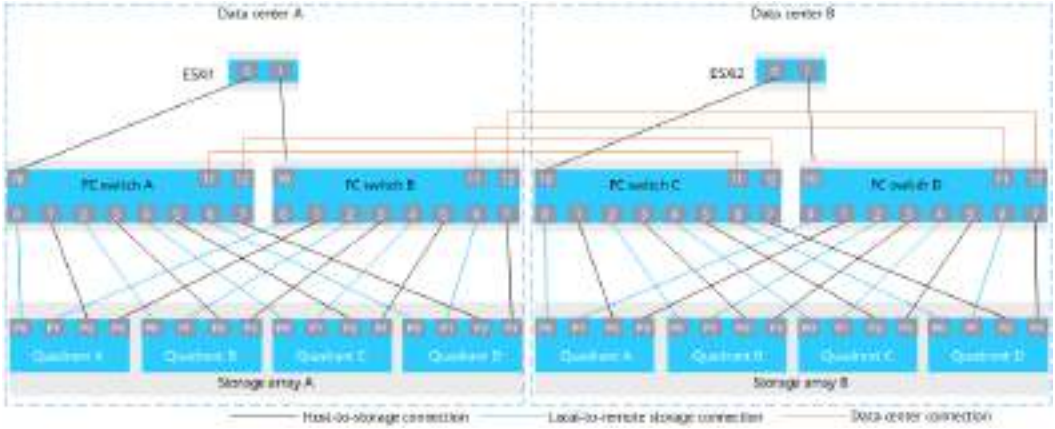
Zone (Example)[a]	Zone Member[b]	Used To
StorageA_A_P0_StorageB_A_P0	(1, 0; 3, 0)	Connect controller A of storage array A to controller A of storage array B.
StorageA_A_P0_StorageB_B_P0	(1, 0; 3, 2)	Connect controller A of storage array A to controller B of storage array B.
StorageA_B_P0_StorageB_B_P0	(1, 2; 3, 2)	Connect controller B of storage array A to controller B of storage array B.

Zone (Example)[a]	Zone Member[b]	Used To
StorageA_B_P0_StorageB_A_P0	(1, 2; 3, 0)	Connect controller B of storage array A to controller A of storage array B.
a: The zone name **StorageA_A_P0_StorageB_A_P0** means the zone connects port P0 on controller A of storage array A to port P0 on controller A of storage array B. b: Zone members are expressed in the format of domain ID of Fibre Channel switch, port ID. For example, 1, 1 indicates port 1 on Fibre Channel switch 1.		

Configurations for High-End Storage Models (Four Controllers)

Figure 8-2 shows the link planning.

Figure 8-2 Link planning



Four Fibre Channel switches are cascaded across active-active data centers, building a mirroring relationship between the storage arrays in the two data centers.

As shown in **Figure 8-2**, Fibre Channel switches A and C are cascaded across data centers through ports 11 and 12 on them. Fibre Channel switches B and D are cascaded across data centers through ports 11 and 12 on them.

Domain ID planning

If Fibre Channel switches are cascaded, domain IDs must be set to prevent ID conflicts on a network. A domain ID is the unique identifier of a Fibre Channel switch. **Table 8-4** describes the domain ID planning.

Table 8-4 Domain ID planning

Fibre Channel Switch (Example)	Domain ID (Example)
Fibre Channel Switch A	1

Fibre Channel Switch (Example)	Domain ID (Example)
Fibre Channel Switch B	2
Fibre Channel Switch C	3
Fibre Channel Switch D	4

Zone planning

A zone allows specific switches and devices to communicate with each other. On two cascaded Fibre Channel switches, the ports of each link form a zone. Zone planning complies with the following principles:

- Each application host is connected to all the quadrants of active-active storage systems.
- Every quadrant on each local controller enclosure is physically or logically connected to the same quadrant on each remote controller enclosure. For example, quadrant A on the local controller enclosure 0 must have links to quadrant A on every remote controller enclosure.

NOTE

If a port of the application host has multiple WWNs, plan zones based on WWNs.

Table 8-5 uses **Fibre Channel switches A and C as an example** to describe the zone planning.

Table 8-5 Service zone

Zone (Example)[a]	Zone Member[b]	Used To
ESXi1_0_StorageA_A_P2	(1, 10; 1, 1)	Connect quadrant A, B, C, or D of storage array A to ESXi host 1.
ESXi1_0_StorageA_B_P2	(1, 10; 1, 3)	
ESXi1_0_StorageA_C_P2	(1, 10; 1, 5)	
ESXi1_0_StorageA_D_P2	(1, 10; 1, 7)	
ESXi1_0_StorageB_A_P2	(1, 10; 3, 1)	Connect quadrant A, B, C, or D of storage array B to ESXi host 1.
ESXi1_0_StorageB_B_P2	(1, 10; 3, 3)	
ESXi1_0_StorageB_C_P2	(1, 10; 3, 5)	
ESXi1_0_StorageB_D_P2	(1, 10; 3, 7)	
ESXi2_0_StorageA_A_P2	(3, 10; 1, 1)	Connect quadrant A, B, C, or D of storage array A to ESXi host 2.
ESXi2_0_StorageA_B_P2	(3, 10; 1, 3)	
ESXi2_0_StorageA_C_P2	(3, 10; 1, 5)	
ESXi2_0_StorageA_D_P2	(3, 10; 1, 7)	

Zone (Example)[a]	Zone Member[b]	Used To
ESXi2_0_StorageB_A_P2	(3, 10; 3, 1)	Connect quadrant A, B, C, or D of storage array B to ESXi host 2.
ESXi2_0_StorageB_B_P2	(3, 10; 3, 3)	
ESXi2_0_StorageB_C_P2	(3, 10; 3, 5)	
ESXi2_0_StorageB_D_P2	(3, 10; 3, 7)	
a: The zone name **ESXi1_0_StorageA_A_P2** means the zone connects port 0 on ESXi host 1 to port P2 in quadrant A of storage array A. b: Zone members are expressed in the format of domain ID of Fibre Channel switch, port ID. For example, 1, 1 indicates port 1 on Fibre Channel switch 1.		

Table 8-6 uses **Fibre Channel switches A and C as an example** to describe the zone planning for the replication network.

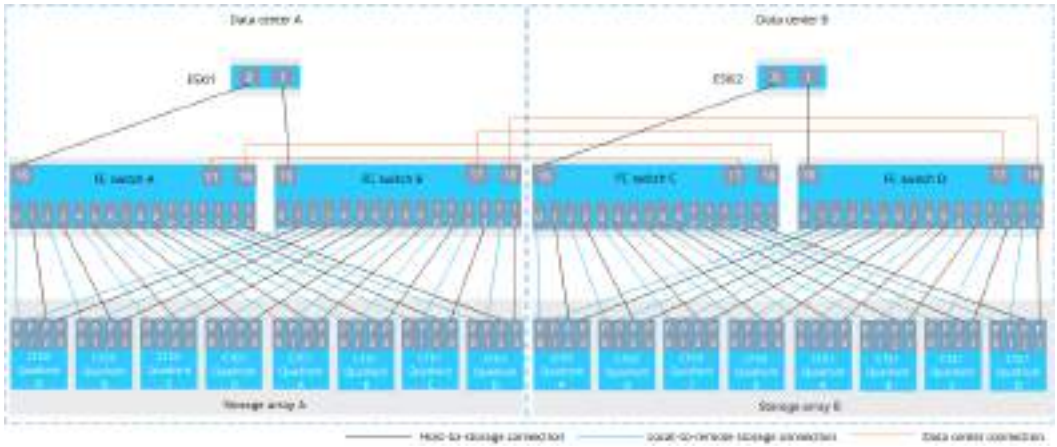
Table 8-6 Replication zones

Zone (Example)[a]	Zone Member[b]	Used To
StorageA_A_P0_StorageB_A_P0	(1, 0; 3, 0)	Connect quadrant A of storage array A to quadrant A of storage array B.
StorageA_B_P0_StorageB_B_P0	(1, 2; 3, 2)	Connect quadrant B of storage array A to quadrant B of storage array B.
StorageA_C_P0_StorageB_C_P0	(1, 4; 3, 4)	Connect quadrant C of storage array A to quadrant C of storage array B.
StorageA_D_P0_StorageB_D_P0	(1, 6; 3, 6)	Connect quadrant D of storage array A to quadrant D of storage array B.
a: The zone name **StorageA_A_P0_StorageB_A_P0** means the zone connects port P0 in quadrant A of storage array A to port P0 in quadrant A of storage array B. b: Zone members are expressed in the format of domain ID of Fibre Channel switch, port ID. For example, 1, 1 indicates port 1 on Fibre Channel switch 1.		

Configurations for High-End Storage Models (Eight Controllers)

Figure 8-3 shows the link planning.

Figure 8-3 Link planning



Four Fibre Channel switches are cascaded across active-active data centers, building a mirroring relationship between the storage arrays in the two data centers.

As shown in **Figure 8-3**, Fibre Channel switches A and C are cascaded across data centers through ports 17 and 18 on them. Fibre Channel switches B and D are cascaded across data centers through ports 17 and 18 on them.

Domain ID planning

If Fibre Channel switches are cascaded, domain IDs must be set to prevent ID conflicts on a network. A domain ID is the unique identifier of a Fibre Channel switch. **Table 8-7** describes the domain ID planning.

Table 8-7 Domain ID planning

Fibre Channel Switch (Example)	Domain ID (Example)
Fibre Channel switch A	1
Fibre Channel switch B	2
Fibre Channel switch C	3
Fibre Channel switch D	4

Zone planning

A zone allows specific switches and devices to communicate with each other. On two cascaded Fibre Channel switches, the ports of each link form a zone. Zone planning complies with the following principles:

- Each application host is connected to all the quadrants of active-active storage systems.
- Every quadrant on each local controller enclosure is physically or logically connected to the same quadrant on each remote controller enclosure. For example, quadrant A on the local controller enclosure 0 must have links to quadrant A on every remote controller enclosure; quadrant B on the local

controller enclosure 0 must have links to quadrant B on every remote controller enclosure; quadrant C on the local controller enclosure 0 must have links to quadrant C on every remote controller enclosure; quadrant D on the local controller enclosure 0 must have links to quadrant D on every remote controller enclosure; quadrant A on the local controller enclosure 1 must have links to quadrant A on every remote controller enclosure; quadrant B on the local controller enclosure 1 must have links to quadrant B on every remote controller enclosure; quadrant C on the local controller enclosure 1 must have links to quadrant C on every remote controller enclosure; quadrant D on the local controller enclosure 1 must have links to quadrant D on every remote controller enclosure.

NOTE

If a port of the application host has multiple WWNs, plan zones based on WWNs.

Table 8-8 uses **Fibre Channel switches A and C as an example** to describe the zone planning.

Table 8-8 Service zones

Zone (Example)[a]	Zone Member[b]	Used To
ESXi1_0_StorageA_Engine0_A_P2	(1, 16; 1, 1)	Connect quadrant A, B, C, or D on controller enclosure 0 of storage array A to ESXi host 1.
ESXi1_0_StorageA_Engine0_B_P2	(1, 16; 1, 3)	
ESXi1_0_StorageA_Engine0_C_P2	(1, 16; 1, 5)	
ESXi1_0_StorageA_Engine0_D_P2	(1, 16; 1, 7)	
ESXi1_0_StorageA_Engine1_A_P2	(1, 16; 1, 9)	Connect quadrant A, B, C, or D on controller enclosure 1 of storage array A to ESXi host 1.
ESXi1_0_StorageA_Engine1_B_P2	(1, 16; 1, 11)	
ESXi1_0_StorageA_Engine1_C_P2	(1, 16; 1, 13)	
ESXi1_0_StorageA_Engine1_D_P2	(1, 16; 1, 15)	
ESXi1_0_StorageB_Engine0_A_P2	(1, 16; 3, 1)	Connect quadrant A, B, C, or D on controller enclosure 0 of storage array B to ESXi host 1.
ESXi1_0_StorageB_Engine0_B_P2	(1, 16; 3, 3)	
ESXi1_0_StorageB_Engine0_C_P2	(1, 16; 3, 5)	

Zone (Example)[a]	Zone Member[b]	Used To
ESXi1_0_StorageB_Engine0_D_P2	(1, 16; 3, 7)	
ESXi1_0_StorageB_Engine1_A_P2	(1, 16; 3, 9)	Connect quadrant A, B, C, or D on controller enclosure 1 of storage array B to ESXi host 1.
ESXi1_0_StorageB_Engine1_B_P2	(1, 16; 3, 11)	
ESXi1_0_StorageB_Engine1_C_P2	(1, 16; 3, 13)	
ESXi1_0_StorageB_Engine1_D_P2	(1, 16; 3, 15)	
ESXi2_0_StorageA_Engine0_A_P2	(3, 16; 1, 1)	Connect quadrant A, B, C, or D on controller enclosure 0 of storage array A to ESXi host 2.
ESXi2_0_StorageA_Engine0_B_P2	(3, 16; 1, 3)	
ESXi2_0_StorageA_Engine0_C_P2	(3, 16; 1, 5)	
ESXi2_0_StorageA_Engine0_D_P2	(3, 16; 1, 7)	
ESXi2_0_StorageA_Engine1_A_P2	(3, 16; 1, 9)	Connect quadrant A, B, C, or D on controller enclosure 1 of storage array A to ESXi host 2.
ESXi2_0_StorageA_Engine1_B_P2	(3, 16; 1, 11)	
ESXi2_0_StorageA_Engine1_C_P2	(3, 16; 1, 13)	
ESXi2_0_StorageA_Engine1_D_P2	(3, 16; 1, 15)	
ESXi2_0_StorageB_Engine0_A_P2	(3, 16; 3, 1)	Connect quadrant A, B, C, or D on controller enclosure 0 of storage array B to ESXi host 2.
ESXi2_0_StorageB_Engine0_B_P2	(3, 16; 3, 3)	
ESXi2_0_StorageB_Engine0_C_P2	(3, 16; 3, 5)	
ESXi2_0_StorageB_Engine0_D_P2	(3, 16; 3, 7)	
ESXi2_0_StorageB_Engine1_A_P2	(3, 16; 3, 9)	Connect quadrant A, B, C, or D on controller enclosure 1 of storage array B to ESXi host 2.
ESXi2_0_StorageB_Engine1_B_P2	(3, 16; 3, 11)	

Zone (Example)[a]	Zone Member[b]	Used To
ESXi2_0_StorageB_Engine1_C_P2	(3, 16; 3, 13)	
ESXi2_0_StorageB_Engine1_D_P2	(3, 16; 3, 15)	
a: The zone name **ESXi1_0_StorageA_Engine0_A_P2** means the zone connects port 0 on ESXi host 1 to port P2 in quadrant A on controller enclosure 0 of storage array A. b: Zone members are expressed in the format of domain ID of Fibre Channel switch, port ID. For example, 1, 1 indicates port 1 on Fibre Channel switch 1.		

Table 8-9 uses **Fibre Channel switches A and C as an example** to describe the zone planning for the replication network.

Table 8-9 Replication zones

Zone (Example)[a]	Zone Member[b]	Used To
StorageA_Engine0_A_P0_StorageB_Engine0_A_P0	(1, 0; 3, 0)	Connect quadrant A on controller enclosure 0 of storage array A to quadrant A on controller enclosure 0 of storage array B.
StorageA_Engine0_A_P0_StorageB_Engine1_A_P0	(1, 0; 3, 8)	Connect quadrant A on controller enclosure 0 of storage array A to quadrant A on controller enclosure 1 of storage array B.
StorageA_Engine0_B_P0_StorageB_Engine0_B_P0	(1, 2; 3, 2)	Connect quadrant B on controller enclosure 0 of storage array A to quadrant B on controller enclosure 0 of storage array B.
StorageA_Engine0_B_P0_StorageB_Engine1_B_P0	(1, 2; 3, 10)	Connect quadrant B on controller enclosure 0 of storage array A to quadrant B on controller enclosure 1 of storage array B.
StorageA_Engine0_C_P0_StorageB_Engine0_C_P0	(1, 4; 3, 4)	Connect quadrant C on controller enclosure 0 of storage array A to quadrant C on controller enclosure 0 of storage array B.

Zone (Example)[a]	Zone Member[b]	Used To
StorageA_Engine0_C_P0_ StorageB_Engine1_C_P0	(1, 4; 3, 12)	Connect quadrant C on controller enclosure 0 of storage array A to quadrant C on controller enclosure 1 of storage array B.
StorageA_Engine0_D_P0_ StorageB_Engine0_D_P0	(1, 6; 3, 6)	Connect quadrant D on controller enclosure 0 of storage array A to quadrant D on controller enclosure 0 of storage array B.
StorageA_Engine0_D_P0_ StorageB_Engine1_D_P0	(1, 6; 3, 14)	Connect quadrant D on controller enclosure 0 of storage array A to quadrant D on controller enclosure 1 of storage array B.
StorageA_Engine1_A_P0_ StorageB_Engine0_A_P0	(1, 8; 3, 0)	Connect quadrant A on controller enclosure 1 of storage array A to quadrant A on controller enclosure 0 of storage array B.
StorageA_Engine1_A_P0_ StorageB_Engine1_A_P0	(1, 8; 3, 8)	Connect quadrant A on controller enclosure 1 of storage array A to quadrant A on controller enclosure 1 of storage array B.
StorageA_Engine1_B_P0_ StorageB_Engine0_B_P0	(1, 10; 3, 2)	Connect quadrant B on controller enclosure 1 of storage array A to quadrant B on controller enclosure 0 of storage array B.
StorageA_Engine1_B_P0_ StorageB_Engine1_B_P0	(1, 10; 3, 10)	Connect quadrant B on controller enclosure 1 of storage array A to quadrant B on controller enclosure 1 of storage array B.
StorageA_Engine1_C_P0_ StorageB_Engine0_C_P0	(1, 12; 3, 4)	Connect quadrant C on controller enclosure 1 of storage array A to quadrant C on controller enclosure 0 of storage array B.
StorageA_Engine1_C_P0_ StorageB_Engine1_C_P0	(1, 12; 3, 12)	Connect quadrant C on controller enclosure 1 of storage array A to quadrant C on controller enclosure 1 of storage array B.

Zone (Example)[a]	Zone Member[b]	Used To
StorageA_Engine1_D_P0_ StorageB_Engine0_D_P0	(1, 14; 3, 6)	Connect quadrant D on controller enclosure 1 of storage array A to quadrant D on controller enclosure 0 of storage array B.
StorageA_Engine1_D_P0_ StorageB_Engine1_D_P0	(1, 14; 3, 14)	Connect quadrant D on controller enclosure 1 of storage array A to quadrant D on controller enclosure 1 of storage array B.
a: The zone name **StorageA_Engine0_A_P0_StorageB_Engine0_A_P0** means the zone connects port P0 in quadrant A on controller enclosure 0 of storage array A to port P0 in quadrant A on controller enclosure 0 of storage array B. b: Zone members are expressed in the format of domain ID of Fibre Channel switch, port ID. For example, 1, 1 indicates port 1 on Fibre Channel switch 1.		

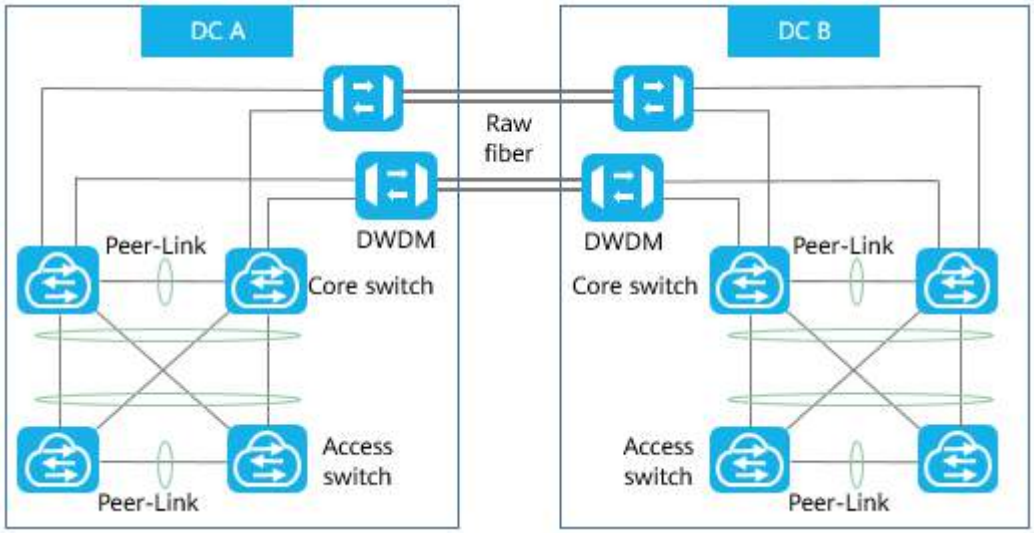
8.2 Configuring Ethernet Switches (Applicable to IP Connections)

Ethernet switches are used as access and core switches in the two DCs. This section describes how to configure Ethernet switches to exchange information in and between the two DCs.

Ethernet Planning

Figure 8-4 shows the Ethernet planning in and between the two DCs in the active-active DC solution.

Figure 8-4 Ethernet planning



For details, see "Spine-Leaf Interconnection Through Multi-level M-LAGs" in the *Best Practices of CloudEngine 16800, 12800, 8800, and 6800 Series Switches for DCN Storage Scenarios*.

NOTE

To obtain the *Best Practices of CloudEngine 16800, 12800, 8800, and 6800 Series Switches for DCN Storage Scenarios*, log in to **http://support.huawei.com/enterprise/**. If you do not have an account, apply for one on the website. Then search for the document by document name.

Configuration Requirements

- Cross-DC L2 interconnection by core switches
  - When the distance between the DCs is 80 km or greater, DWDM devices are used for interconnection.
  - When the distance between the DCs is within 80 km, single-mode optical fibers are used for interconnection. Single-mode optical modules must be configured on the core switches for long-distance transmission. Multiple pairs of single-mode optical fibers must be configured. Each service link is carried by a pair of single-mode optical fibers.

    NOTE

    Ensure that the switches that you use support the single-mode optical modules and the maximum transmission distance supported by the optical modules is greater than the actual distance between the switches.
- VLAN-based service isolation

NOTE

In this solution, you are advised to use Huawei CloudEngine 12800 series and Huawei CloudEngine 5800 or 6800 series as core switches and access switches respectively. You are advised to use Huawei CloudEngine 6800 series as Ethernet switches.

Refer to the switch documentation for the recommended networks of the switches. You can obtain the documents from the following paths:

- **CE12800**
- **CE6800**
- **CE5800**

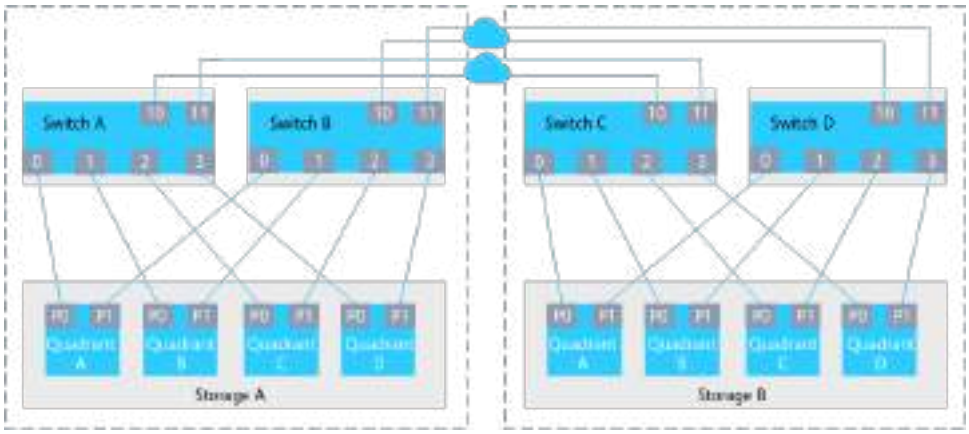
8.3 Configuring Ethernet Switches (for RoCE Connections)

Standard Networking for RoCE Replication Links

- Connect replication links to two switches.
- For a 4 U storage system, every quadrant on each controller enclosure provides two ports to connect to two switches. For a 2 U storage system, every controller on each controller enclosure provides two ports to connect to two switches. For example, **8.3 Configuring Ethernet Switches (for RoCE Connections)** shows the replication network between 4 U storage systems with four controllers.

- The IP addresses of the storage ports connected to switches A and C must be on the same network segment (same VLAN). The IP addresses of the storage ports connected to switches B and D must be on another network segment (same VLAN).

  Figure 8-5 Standard networking for RoCE replication links



RoCE Replication Network Requirements

RoCE has high requirements on the network. Switches must support lossless Ethernet and priority-based flow control (PFC) deadlock detection, suppression, and isolation.

- PFC

  Set the PFC priority to 3, enable PFC on all switch ports to be used, and configure hardware-based PFC deadlock detection.
- Network-based Proactive Congestion Control (NPCC) for lossless queues

  Before configuring NPCC for lossless queues, configure PFC. A queue corresponding to the internal priority for which PFC is enabled is known as a lossless queue.
- (Optional, recommended) AI-ECN

  Configure the low-latency fabric, disable dynamic ECN, and then enable and activate AI-ECN.
- VLAN

  Configure VLANs based on the network plan.
- (Optional) iNOF (quick detection of link faults)

  To quickly detect replication link faults, the SNSD function must be enabled on the storage side and iNOF must be enabled for switches. For details, see **iNOF Configuration** in the product documentation of the switches.
- The RoCE replication network supports a maximum distance of 100 km between two storage systems.
  - For deployment within a data center, use Huawei CloudEngine series switches, such as CE6865 and CE8850.
  - For deployment across data centers, ensure that the switches support long-distance transmission. You are advised to use switches with an optimized congestion control algorithm for long-distance transmission.

For details, see the switch specifications. Huawei CloudEngine 6866-48S8CQ-P (CloudEngine 6860-SAN) and CloudEngine 8851-32CQ8DQ-P (CloudEngine 8850-SAN) switches of V300R020C10 or later support the preceding functions. They are referred to as CE6866 and CE8851 in this document.

NOTICE

The configuration method varies with the switch model and vendor. For details, see the configuration guide released by the switch vendor.

PFC Configuration

The following describes how to configure PFC for CE6866 V300R020C10. The operations must be performed on both sides of the switches.

Step 1 Enable PFC priority. This example configures priority 3.

```
<CE6866-48S8CQ-P>system-view
Enter system view, return user view with return command.
Warning: The current device is single master board. Exercise caution when performing this operation.
[~CE6866-48S8CQ-P]dcb pfc
[~CE6866-48S8CQ-P-dcb-pfc-default]priority 3
[*CE6866-48S8CQ-P-dcb-pfc-default]commit
[~CE6866-48S8CQ-P-dcb-pfc-default]quit
[~CE6866-48S8CQ-P]
```

Run the following command to verify that the PFC priority configuration has taken effect:

```
[~CE6866-48S8CQ-P]display dcb pfc-profile default
------------------------------------------------------------------------------
PFC-profile Name                    Priority
------------------------------------------------------------------------------
default                             3
------------------------------------------------------------------------------
[~CE6866-48S8CQ-P]
```

Step 2 Enable PFC on the switch ports.

The following uses port 25GE1/0/26 as an example. Run the **dcb pfc enable mode manual** command to enable PFC on the port.

```
<CE6866-48S8CQ-P>system-view
Enter system view, return user view with return command.
Warning: The current device is single master board. Exercise caution when performing this operation.
[~CE6866-48S8CQ-P]interface 25GE1/0/26
[~CE6866-48S8CQ-P-25GE1/0/26]dcb pfc enable mode manual
[*CE6866-48S8CQ-P-25GE1/0/26]commit
[~CE6866-48S8CQ-P-25GE1/0/26]quit
[~CE6866-48S8CQ-P]
```

Run the following command to verify that PFC has been enabled on the 25GE1/0/26 port:

```
[~CE6866-48S8CQ-P]display dcb
M:Manual;    A:Auto
------------------------------------------------------------------------------
Interface        PFC Name     PFC Status  ETS Name    ETS Status App-Profile
------------------------------------------------------------------------------
25GE1/0/26       default      ENABLE(M)   -           -          -
------------------------------------------------------------------------------
[~CE6866-48S8CQ-P]
```


> **NOTE**
>
> Repeat this operation on all switch ports to be used, including the ports between switches and between switches and storage systems.

Step 3 Configure PFC deadlock detection.

Set the detection period to 15 ms and recovery period to 15 ms.

```
<CE6866-48S8CQ-P>system-view
Enter system view, return user view with return command.
Warning: The current device is single master board. Exercise caution when performing this operation.
[~CE6866-48S8CQ-P]dcb pfc deadlock-detect timer 15
[*CE6866-48S8CQ-P]dcb pfc deadlock-recovery timer 15
```

Verify the configuration result.

```
[~CE6866-48S8CQ-P]display this | include dcb
dcb pfc deadlock-detect timer 15
dcb pfc deadlock-recovery timer 15
[~CE6866-48S8CQ-P]
```

> **NOTE**
>
> The configuration commands may vary with the versions of the switches. For details, see the product documentation of the specific switch model. For example, in CE6865 V200R019C00, the default PFC deadlock detection period accuracy is 100 ms. After the **dcb pfc deadlock-detect timer 15** and **dcb pfc deadlock-recovery timer 15** commands are executed, the detection period is 1500 ms and the recovery period is 1500 ms.

Step 4 Set the threshold for disabling PFC on a port to 20 deadlocks in 1 minute.

```
<CE6866-48S8CQ-P>system-view
Enter system view, return user view with return command.
Warning: The current device is single master board. Exercise caution when performing this operation.
[~CE6866-48S8CQ-P]dcb pfc

[*CE6866-48S8CQ-P-dcb-pfc-default]priority 3 turn-off threshold 20
[*CE6866-48S8CQ-P-dcb-pfc-default]commit
[~CE6866-48S8CQ-P-dcb-pfc-default]quit
[~CE6866-48S8CQ-P]
```

Verify the configuration result.

```
<CE6866-48S8CQ-P>system-view
Enter system view, return user view with return command.
Warning: The current device is single master board. Exercise caution when performing this operation.
[~CE6866-48S8CQ-P]dcb pfc
[~CE6866-48S8CQ-P-dcb-pfc-default]display this
#
dcb pfc

 priority 3 turn-off threshold 20
#
return
[~CE6866-48S8CQ-P-dcb-pfc-default]quit
[~CE6866-48S8CQ-P]
```

Step 5 (Optional) Run the **dcb pfc deadlock recovery-behavior forwarding slot** *slot-id* command to configure the device forwarding behavior during hardware deadlock recovery.

```
<CE6866-48S8CQ-P>system-view
[~CE6866-48S8CQ-P]dcb pfc deadlock recovery-behavior forwarding slot 1
```


NOTE

- Huawei CE6866 and CE8851 (V300R020C10 and later versions) support long-distance transmission. By default, the devices discard packets during hardware deadlock recovery. In this case, this operation is needed.
- For deployment within a data center, if the software version of Huawei switches (such as CE6865) is earlier than V300R020C10, the devices forward packets during hardware deadlock recovery by default. Therefore, you do not need to perform this operation.

----End

NPCC Configuration

NPCC supports the high-throughput and low-latency modes. The high-throughput mode improves the throughput of RoCEv2 traffic, and the low-latency mode reduces the latency of RoCEv2 traffic. The high-throughput mode is recommended in storage scenarios.

Step 1 Enter the system view.

```
<CE6866-48S8CQ-P>system-view
Enter system view, return user view with return command.
Warning: The current device is single master board. Exercise caution when performing this operation.
```

Step 2 Enable the AI service and enter the AI service view. By default, the AI service is disabled.

```
[~CE6866-48S8CQ-P] ai-service
[*CE6866-48S8CQ-P-ai-service]
```

Step 3 Enter the NPCC view and enable NPCC. By default, NPCC is disabled.

```
[*CE6866-48S8CQ-P-ai-service] npcc
[*CE6866-48S8CQ-P-ai-service-npcc]
```

Step 4 Run the **assign queue** *queue-id* command to specify a lossless queue for which NPCC is enabled. By default, no lossless queue is specified for NPCC.

```
[*CE6866-48S8CQ-P-ai-service-npcc] assign queue 3
```

Step 5 Run the **npcc mode { high-throughput | low-latency }** command to set NPCC to high-throughput or low-latency mode. By default, NPCC works in high-throughput mode.

```
[*CE6866-48S8CQ-P-ai-service-npcc] npcc mode low-latency
```

Step 6 Run the **quit** command to exit the NPCC view.

Step 7 Run the **quit** command to exit the AI service view.

Step 8 Run the **interface** *interface-type interface-number* command to enter the interface view.

```
[~CE6866-48S8CQ-P]interface 25GE 1/0/26
```

Step 9 Enable NPCC on the interface. By default, NPCC is disabled on the interface.

```
[~CE6866-48S8CQ-P-25GE1/0/26] npcc enable
```

Step 10 Run the **quit** command to exit the interface view.

Step 11 Run the **commit** command to commit the configuration.

----End

(Optional, Recommended) AI-ECN Configuration

You are advised to configure AI-ECN to dynamically and intelligently set the threshold based on the network traffic.

Step 1 Before the configuration, check whether the switch has the AI-ECN license.

If the value of **CE-LIC-AFRD** is **YES**, the switch has the AI-ECN license. Otherwise, you must load the license.

```
[~CE6866-48S8CQ-P]display license
MainBoard:
 Active License    : flash:/LICCloudEngine6800_V300R020_20200819SDQG5M.xml
 License state     : Demo
 Revoke ticket     : No ticket
 License mode      : common

 RD of Huawei Technologies Co., Ltd.

 Product name      : CloudEngine 6800
 Product version   : V300R020
 License Serial No : LIC20200819SDQG5M
 Creator           : Huawei Technologies Co., Ltd.
 Created Time      : 2020-08-19 16:01:01
 ------------------------------------------------------------
 Feature name      : Trial0
 Authorize type    : demo
 Expired date      : 2020-11-12
 Trial days        : --

 Item name          Item type      Value      Description
 ------------------------------------------------------------
 N1-CE68LIC-AKA     --             1          N1-AK Advanced SW License for CloudEngine 6800
  CE-LIC-NSH        Function       YES        CE-LIC-NSH
  CE-LIC-TLM        Function       YES        CE-LIC-TLM
  CE-LIC-BASE       Function       YES        CE-LIC-BASE
 CE68-LIC-AFRD      --             1          CloudEngine 6800 RDMA AI Fabric Application Acceleration Basic
Function
  CE-LIC-AFRD       Function       YES        CE-LIC-AFRD
 N1-CE68LIC-iNOF    --             1          N1-CloudEngine 6800 AI Fabric Value-added Package for the iNOF
Storage Scenarios
  CE-LIC-AFRD       Function       YES        CE-LIC-AFRD
  CE-LIC-iNOF       Function       YES        CE-LIC-iNOF
 CE68-LIC-AFV       --             1          CE6800 Anyflow Visibility Function
  CE-LIC-AFV        Function       YES        CE-LIC-AFV
 CE68-LIC-TLM       --             1          CE6800 Telemetry Function
  CE-LIC-TLM        Function       YES        CE-LIC-TLM
 N1-CE68LIC-PLLV    --             1          N1-CloudEngine 6800 Packet Loss and Latency Visibility Function
  CE-LIC-PLLV       Function       YES        CE-LIC-PLLV
 CE68-LIC-iNOF      --             1          CloudEngine 6800 for AI Fabric iNOF storage
  CE-LIC-iNOF       Function       YES        CE-LIC-iNOF
 N1-CE68LIC-AFV     --             1          N1-CloudEngine 6800 Anyflow Visibility Function
  CE-LIC-AFV        Function       YES        CE-LIC-AFV
 N1-CE68LIC-CFAD    --             1          N1-CloudFabric Advanced SW License for CloudEngine 6800
  CE-LIC-NSH        Function       YES        CE-LIC-NSH
  CE-LIC-TLM        Function       YES        CE-LIC-TLM
  CE-LIC-PTP        Function       YES        CE-LIC-PTP
  CE-LIC-BASE       Function       YES        CE-LIC-BASE
 N1-CE68UPG-M-A     --             1          N1-CloudEngine 6800 Upgrade SW License:Management to
Advanced
  CE-LIC-NSH        Function       YES        CE-LIC-NSH
  CE-LIC-TLM        Function       YES        CE-LIC-TLM
  CE-LIC-PTP        Function       YES        CE-LIC-PTP
 N1-CE68LIC-AFRD-2  --             1          N1-CloudEngine 6800 AI Fabric RDMA Application Acceleration
Function 2
  CE-LIC-AFRD       Function       YES        CE-LIC-AFRD
 N1-CE68LIC-IAF     --             1          N1-CE6800 Intelligent Analysis Function
  CE-LIC-TLM        Function       YES        CE-LIC-TLM
```



```
N1-CE68LIC-CFFD    --          1        N1-CloudFabric Foundation SW License for CloudEngine 6800
 CE-LIC-TLM        Function    YES       CE-LIC-TLM
 CE-LIC-PTP        Function    YES       CE-LIC-PTP
 CE-LIC-BASE       Function    YES       CE-LIC-BASE
N1-CE68UPG-F-A     --          1        N1-CloudEngine 6800 Upgrade SW License:Foundation to Advanced
 CE-LIC-NSH        Function    YES       CE-LIC-NSH
N1-CE68LIC-CFMM    --          1        N1-CloudFabric Management SW License for CloudEngine 6800
 CE-LIC-BASE       Function    YES       CE-LIC-BASE
N1-CE68LIC-BS      --          1        N1-CloudEngine 6800 Basic Function
 CE-LIC-BASE       Function    YES       CE-LIC-BASE
CE68-LIC-PTP       --          1        CE6800 Precision Time Protocol Function
 CE-LIC-PTP        Function    YES       CE-LIC-PTP
CE68-LIC-PLLV      --          1        CE6800 Packet Loss and Latency Visibility Function
 CE-LIC-PLLV       Function    YES       CE-LIC-PLLV
CE68-LIC-BASE      --          1        CE6800 Basic Software Function
 CE-LIC-BASE       Function    YES       CE-LIC-BASE
N1-CE68LIC-ADA     --          1        N1-CloudEngine 6800 Advantage Function A
 CE-LIC-TLM        Function    YES       CE-LIC-TLM
```

Step 2 Enable AI-ECN and specify the lossless queues with AI-ECN enabled.

```
<CE6866-48S8CQ-P>system-view
Enter system view, return user view with return command.
Warning: The current device is single master board. Exercise caution when performing this operation.
[~CE6866-48S8CQ-P]ai-service
[*CE6866-48S8CQ-P-ai-service]ai-ecn
[*CE6866-48S8CQ-P-ai-service-ai-ecn]ai-ecn enable
[*CE6866-48S8CQ-P-ai-service-ai-ecn]assign queue 3
[*CE6866-48S8CQ-P-ai-service-ai-ecn]commit
[~CE6866-48S8CQ-P-ai-service-ai-ecn]quit
[~CE6866-48S8CQ-P-ai-service]quit
```

Step 3 Run the **display ai-ecn calculated state** command to verify that AI-ECN has been activated.

```
[~CE6866-48S8CQ-P]display ai-ecn calculated state
AI-ECN active model: AI_ECN, version 1.0.0, actived time: 2020-08-19 17:25:49
--------------------------------------------------------------------------------
Interface       Queue   Low-Threshold   High-Threshold   Probability   Mode
                        (Byte)          (Byte)          (%)
--------------------------------------------------------------------------------
25GE1/0/26      3       5120            409600          5             BBR
25GE1/0/29      3       5120            409600          5             BBR
25GE1/0/30      3       5120            409600          5             BBR
25GE1/0/31      3       5120            409600          5             BBR
25GE1/0/32      3       5120            409600          5             BBR
25GE1/0/33      3       5120            409600          5             BBR
--------------------------------------------------------------------------------
[~CE6866-48S8CQ-P]
```

----End

VLAN Configuration

Step 1 Configure global VLANs. The following example uses VLAN 55 and VLAN 66.

```
<CE6866-48S8CQ-P>system-view
Enter system view, return user view with return command.
Warning: The current device is single master board. Exercise caution when performing this operation.

[~CE6866-48S8CQ-P]vlan batch 55 66
[*CE6866-48S8CQ-P]commit
[~CE6866-48S8CQ-P]quit
<CE6866-48S8CQ-P>
```

Step 2 Configure VLANs for ports.

The following uses port 25GE1/0/26 as an example. Configure the port to work in trunk mode, add the port to VLANs 55 and 66, and set the port as an edge port.


```
<CE6866-48S8CQ-P>system-view
Enter system view, return user view with return command.
Warning: The current device is single master board. Exercise caution when performing this operation.
[~CE6866-48S8CQ-P]interface 25GE 1/0/26
[~CE6866-48S8CQ-P-25GE1/0/26]port link-type trunk
[*CE6866-48S8CQ-P-25GE1/0/26]port trunk allow-pass vlan 55 66
[*CE6866-48S8CQ-P-25GE1/0/26]stp edged-port enable
[*CE6866-48S8CQ-P-25GE1/0/26]commit
[~CE6866-48S8CQ-P]quit
<CE6866-48S8CQ-P>
```

Run the following command to verify that port 25GE1/0/26 has been added to VLANs 55 and 66:

```
[~CE6866-48S8CQ-P]display vlan

The total number of vlans is : 3
--------------------------------------------------------------------------------
U: Up;         D: Down;         TG: Tagged;         UT: Untagged;
MP: Vlan-mapping;               ST: Vlan-stacking;
#: ProtocolTransparent-vlan;    *: Management-vlan;
MAC-LRN: MAC-address learning;  STAT: Statistic;
BC: Broadcast; MC: Multicast;   UC: Unknown-unicast;
FWD: Forward;  DSD: Discard;
--------------------------------------------------------------------------------

VID         Ports
--------------------------------------------------------------------------------
  1         UT:100GE1/0/1(D)   100GE1/0/2(D)   100GE1/0/3(D)   100GE1/0/4(D)
              100GE1/0/5(D)    100GE1/0/6(D)   100GE1/0/7(D)   100GE1/0/8(D)
              25GE1/0/1(D)     25GE1/0/2(D)    25GE1/0/3(D)    25GE1/0/4(D)
              25GE1/0/5(D)     25GE1/0/6(D)    25GE1/0/7(D)    25GE1/0/8(D)
              25GE1/0/9(D)     25GE1/0/10(D)   25GE1/0/11(D)   25GE1/0/12(D)
              25GE1/0/13(D)    25GE1/0/14(D)   25GE1/0/15(D)   25GE1/0/16(D)
              25GE1/0/17(D)    25GE1/0/18(D)   25GE1/0/19(D)   25GE1/0/20(D)
              25GE1/0/21(D)    25GE1/0/22(D)   25GE1/0/23(D)   25GE1/0/24(D)
              25GE1/0/25(D)    25GE1/0/26(U)   25GE1/0/27(D)   25GE1/0/28(D)
              25GE1/0/29(U)    25GE1/0/30(U)   25GE1/0/31(U)   25GE1/0/32(U)
              25GE1/0/33(U)    25GE1/0/34(D)   25GE1/0/35(D)   25GE1/0/36(D)
              25GE1/0/37(D)    25GE1/0/38(D)   25GE1/0/39(D)   25GE1/0/40(D)
              25GE1/0/41(D)    25GE1/0/42(D)   25GE1/0/43(D)   25GE1/0/44(D)
              25GE1/0/45(D)    25GE1/0/46(D)   25GE1/0/47(D)   25GE1/0/48(D)
 55         TG:25GE1/0/26(U)   25GE1/0/29(U)   25GE1/0/30(U)   25GE1/0/31(U)
              25GE1/0/32(U)    25GE1/0/33(U)
 66         TG:25GE1/0/26(U)   25GE1/0/29(U)   25GE1/0/30(U)   25GE1/0/31(U)
              25GE1/0/32(U)    25GE1/0/33(U)
```

NOTE

Repeat this operation on all switch ports to be used, including the ports connecting to the storage systems and other switches.

----End

(Optional) iNOF Configuration (Quick Detection of Link Faults)

- For details about how to configure iNOF for CE6866 and CE8851, see **iNOF Configuration**.
- Enabling SNSD on the storage systems:
  - Method 1: Using the CLI

    Run the **change port eth_snsd_switch eth_port_id=<port_id> snsd_enable=yes** command in the developer mode. For example:

    ```
    developer:/>change port eth_snsd_switch eth_port_id=CTE.A.H0 snsd_enable=yes
    ```

  - Method 2: Using DeviceManager

i. Log in to DeviceManager.

ii. Choose **Services** > **Network** > **RoCE Network**. The **RoCE Network** page is displayed.

iii. Select the desired ports and choose **Batch Set SNSD** > **Batch Enable SNSD**.

NOTE

To set the SNSD status of a single port, click the name of the RoCE port, and change the SNSD status on the page that is displayed on the right.

Configuring the Long-Distance Mode

The following describes the long-distance mode configuration of CE6866. Unless otherwise specified, the operations must be performed on both sides of the switches.

NOTICE

- Ensure that the switch version is V300R020C10 or later.
- The operations must be performed on the ports for the long-distance mode.

Step 1 Configure plane buffer optimization of the long-distance mode for both the local and remote switches.

NOTE

You must restart the device for the configuration to take effect.

```
[~CE6866-48S8CQ-P] ai-service
[*CE6866-48S8CQ-P-ai-service] buffer optimization mode long-distance
[*CE6866-48S8CQ-P-ai-service] quit
[*CE6866-48S8CQ-P] commit
[~CE6866-48S8CQ-P] quit
<DeviceA> reboot
System will reboot! Continue? [Y/N]:Y
```

Step 2 Configure the distance-based headroom check function.

1. Set the long-distance mode of the local switch to **level-100** and enable the distance-based headroom check function.

```
<DeviceA> system-view
[DeviceA] interface 25GE1/0/26
[DeviceA-25GE1/0/26] long-distance mode level-100
[-25GE1/0/26] quit
[*DeviceA] commit
```

2. Set the long-distance mode of the remote switch to **level-100** and enable the distance-based headroom check function.

3. Because the distance-based headroom check function has not been enabled on DeviceB when it is enabled on DeviceA, the check fails. Manually send a probe packet on the local switch.

```
[DeviceA] interface 25GE1/0/26
[DeviceA-25GE1/0/26] start long-distance detect
[-25GE1/0/26] quit
[*DeviceA] commit
```

4. Verify the configuration result.

```
[~DeviceA] display buffer optimization configuration slot 1
------------------------------------------------------------------------------------------------------------------------
```



```
 Buffer unit: KB
Configure buffer optimization mode: Long-distance
Current buffer optimization mode: Long-distance
Interface that can be enabled with both PFC and long-distance
mode:                                   25GE1/0/26
-------------------------------------------------------------------------------

Pipe                  Buffer
-------------------------------------------------------------------------------

0                    20480
1                     3072
2                    20480
3                     3072
4                     3072
5                     3072
-------------------------------------------------------------------------------
Interface       Port      Chip      Pipe      PFC       Mode      DetectHdrmResult      RequiredHdrm
-------------------------------------------------------------------------------
25GE1/0/26      16        0         0         Enable    level-100       12496         12500
```

----End

9 Configuring the Quorum Network

Configure IP addresses for the quorum server, configure VLANs on the switch, and configure the quorum server software.

9.1 Configuring Quorum Site Connectivity

The quorum network devices (such as Ethernet switches) must be properly configured to connect the quorum site to both DCs.

Configure the IP addresses and VLANs for the quorum network devices by following instructions in their respective documentation.

9.2 Reference Quorum Networks

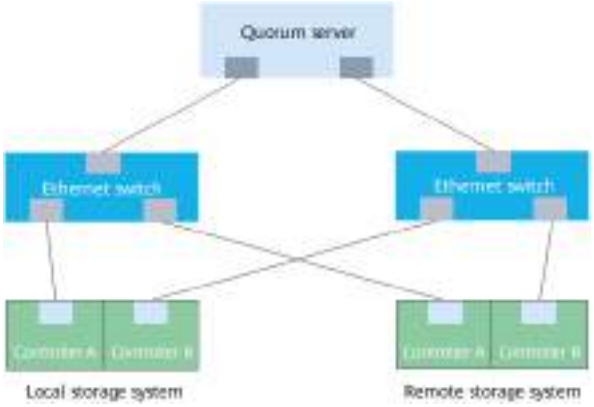
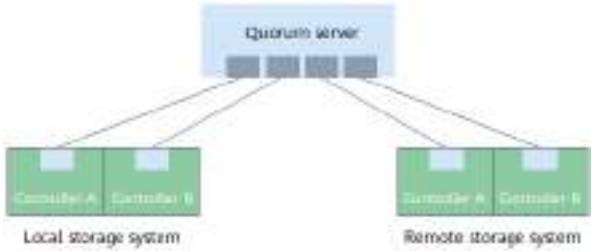
In the active-active DC solution, it is recommended that a quorum server be deployed at a third site to perform arbitration.

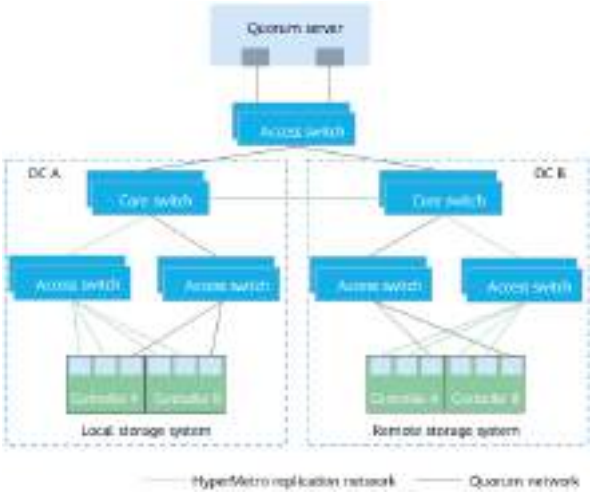
The quorum server and two DCs can be connected by a GE or 10GE network.

Using a Front-end Port as a Quorum Port

Table 9-1 lists the quorum network diagrams when a front-end port is used as the quorum port.

Table 9-1 Quorum network diagrams (using a front-end port as the quorum port)

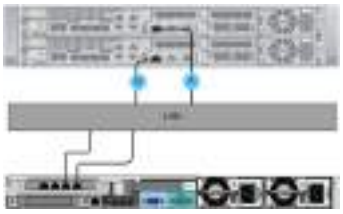
Scenario	Network Diagram	Description
Single-DC deployment		• The quorum server connects to the storage systems via two Ethernet switches. • Each controller on each storage system uses one GE/10GE port to connect to the quorum server. The quorum server uses two ports to connect to every controller on both storage systems.
		• No switch is used. The storage systems and quorum server are connected directly. • The quorum server can use a maximum of four ports (four IP addresses) to connect to the storage systems.

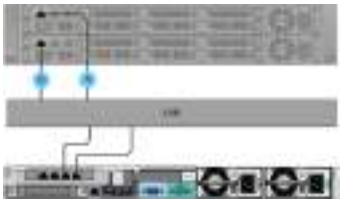
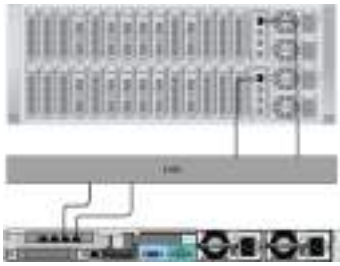
Scenario	Network Diagram	Description
Cross-DC deployment		• The quorum server is deployed at a third site. Ensure that the quorum site communicates properly with the active-active DCs. • If access switches are deployed, the quorum network and HyperMetro replication network use the access switches to connect to different NICs on the core switches for fault isolation. • If access switches are not deployed, the quorum and HyperMetro replication networks directly connect to different NICs on the core switches for fault isolation.

Using a Management Port as a Quorum Port

Table 9-2 lists the quorum network diagrams when a management port is used as the quorum port.

Table 9-2 Quorum network diagrams (using a management port as the quorum port)

Product	Network Diagram	Description
OceanStor 5310/5320		The management ports on all controllers can be used as quorum ports to connect to the quorum server.

Product	Network Diagram	Description
OceanStor 5510/5610		The management ports on all controllers can be used as quorum ports to connect to the quorum server.
OceanStor 6810/18510/18810		Only the management port 0 on each management module can be used as a quorum port to connect to the quorum server.

9.3 Installing Quorum Server Software

9.3.1 Obtaining Quorum Server Software

Table 9-3 lists the quorum server software package required for deploying HyperMetro.

Table 9-3 Software list

Software Name	Version	How to Obtain
Quorum server software **NOTE** The software package name is **OceanStor**_*Version Number*_**QuorumServer**_*Architecture Type*.**zip**.	• The quorum server software version must match the storage system version. • The quorum server software must match the architecture type of the quorum server.	Log in to **https://support.huawei.com/enterprise/** (you can register for an account if you do not have one). Click **Centralized Storage** in **Enterprise Data Center** under **PRODUCT SUPPORT**. On the page that is displayed, select your product model and click the **Software Download** tab. Specify the product version in **Select Version** and find the desired software in the **Version and Patch** area. Then download the software.

9.3.2 Installing Quorum Server Software on a Huawei Dedicated Quorum Server

This section describes how to install the quorum server software on a Huawei quorum server.

Prerequisites

- You have obtained the quorum server software package and uploaded it to the quorum server. Note that the quorum server software package cannot be uploaded by WinSCP.
- The following tools and components are ready: OpenSSL, useradd, groupadd, chown, tar, bzip2, dpkg, or rpm.
- For security purposes, the entropy must be greater than 1024. You can run the **cat /proc/sys/kernel/random/entropy_avail** command to check the entropy. If the entropy is less than 1024, you can use **haveged** to increase the entropy.
- The quorum server has been deployed and its hardware meets the requirements. For details, see **5.2 Preparing for Installation**. You are advised to install iBMA to manage the quorum server, which can be obtained from **https://support.huawei.com/enterprise/en/management-software/ibma-pid-21099187/software**.
- For versions earlier than 6.1.5, the validity period of the default arbitration certificate is 10 years. Ensure the system time of the quorum server is correct so that the default arbitration certificate is valid. 6.1.5 and later versions do not have default certificates or CA certificates.
- A Secure Shell (SSH) tool such as PuTTY has been prepared to log in to the quorum server.

NOTE

You are advised to harden the security of your operating system. For details, see the official security operation guide of the operating system.

Procedure

Step 1 Log in to the quorum server.

1. Use the **quorumAdmin** user to log in to the quorum server.

   NOTE

   - The default IP address of Huawei dedicated quorum server is 192.168.128.200.
   - For the default password of the **quorumAdmin** user, refer to the OceanStor 6.x Account List. You are advised to periodically change your password for security.
   - The IP address for accessing the iBMC management software of the quorum server is 192.168.2.100.

2. Run the **su root** command to switch to the root user.

   NOTE

   Enter the password of the root user as instructed. For the default password of the root user, refer to the OceanStor 6.x Account List. You are advised to periodically change your password for security.

Step 2 Decompress the installation package.

1. In the operating system of the quorum server, run the **unzip** command to decompress the installation package.

```
XXX@Linux:~# unzip OceanStor/QuorumServer/OceanStor_QuorumServer_VXXXRXXXCXX.zip
Archive: OceanStor_QuorumServer_VXXXRXXXCXX.zip
package/
package/quorum_server.sh
package/packages/
package/packages/QuorumServer-VXXXRXXXCXX-linux.x86_64.rpm
package/qs_version.ini
package/tools/
```

2. After decompressing the installation package, run the **cd package** command to go to its directory.

```
XXX@Linux:~# cd package
```

3. (Optional) Run the **ll** command to list files in the directory.

Step 3 Install the quorum server software.

1. Run the **./quorum_server.sh -install** command to install the quorum server software.

NOTE

The non-root user account that is used to install the quorum server software will be used to run and manage the software in follow-up operations. If a password expiration policy is configured on the quorum server, the password of this account may expire, resulting in an access failure. Change the password regularly for security purposes.

```
XXX@Linux:~# ./quorum_server.sh -install
Verify the QuorumServer existence.
The QuorumServer is not installed.
The current user is the root user. A quorum server administrator account needs to be provided. Continue to install?
<Y|N>:Y                                 #Enter "Y" to install the quorum server software.
Enter an administrator account for the quorum server:[default: quorumsvr]:      #Press "Enter". The system installs the quorum server software under the default user account quorumsvr.
Created new account: quorumsvr.
Changing password for quorumsvr.
New Password:                                   #Set the password of user quorumsvr. You are advised to periodically change your password for security.
Reenter New Password:                           #Repeat the password.
Password changed.
Installing the quorum server.
Preparing...                ########################################### [100%]
   1:QuorumServer           ########################################### [100%]
[Notice] No old configuration need to resume.
QuorumServer install success completed.
```

NOTE

quorumsvr is the default user account for the quorum server software installation. If you want to install the quorum server software under another user account, enter the user name after **Enter an administrator account for the quorum server:[default: quorumsvr]**, for example, **Enter an administrator account for the quorum server:[default: quorumsvr]:User_test**.

Non-root user permissions are restricted for security purposes. You can run the **sudo** command to obtain permissions for the following commands: **cat**, **ps**, **sh**, **useradd**, **groupadd**, **userdel**, **groupdel**, **usermod**, **passwd**, **sed**, **rm**, **rpm**, **ls**, **chmod**, **chown**, **find**, **xargs**, **killall**, **mv**, **ln**, and **unzip**. For example, run the **sudo cat** *xxx* command, where *xxx* indicates the name of a file in the system.

Step 4 (Optional) Verify that the quorum server software is installed successfully.

1. After the quorum server software is installed, it starts automatically. Enter the CLI of the quorum server, go to any directory, and run the **qsadmin** command

to open the quorum server software. If the software page is displayed, the software has restarted successfully.

```
XXX@Linux:~# qsadmin
start main!
Waiting for connecting to server...
admin:/>
```

2. Enter the CLI of the quorum server, go to any directory, and run the **ps -elf | grep quo*** command to check whether the quorum server software is installed successfully. If **/opt/quorum_server/bin/quorum_serverd** is displayed in the command output, the installation is successful.

```
XXX@Linux:~# ps -elf |grep quo*

4 S testUser  1102      1  0  80  0 -  137524 hrtime Apr29 ?     01:12:14 /opt/quorum_server/bin/
quorum_serverd
0 S testUser 21885  19967  0  80  0 -  28162 pipe_w 08:55 pts/3  00:00:00 grep --color=auto quo*
```

Step 5 (Optional) Set the cipher suite.

After the quorum server software is installed, the secure cipher suite is used by default. For compatibility with storage systems of earlier versions, the cipher suite may need to be modified.

1. Check the quorum server cipher suite on the storage device.

```
admin:/>show quorum_server general
```

The command output is as follows. Record the value of **Usable Cipher Suites**.

```
admin:/>show quorum_server general
Server ID  Server Name      Address      Port   Running Status  Usable Cipher Suites    All Cipher Suites
---------  ---------------  -----------  -----  --------------  ----------------------  --------------------------
0          QuorumServer_000  xx.xx.xx.xx  30002  Online          AES256+RSA+SHA256:AES256-GCM-SHA384:AES128-GCM-SHA256:@STRENGTH    AES256+RSA+SHA256:AES256-GCM-SHA384:AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:@STRENGTH
```

2. Check the cipher suite on the quorum server.

```
admin:/>show cipher_info
```

The command output is as follows. Record the value of **Current Cipher**.

```
admin:/>show cipher_info

Current Cipher: : ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:@STRENGTH
Default Cipher List: : AES256+RSA+SHA256:AES256+DSS+SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:@STRENGTH
Command executed successfully.
```

3. Check whether the **Usable Cipher Suites** field on the storage system and the **Current Cipher** field on the quorum server have a public cipher suite.

The link can be set up only when a public cipher suite is available. If no public cipher suite is available, run the following commands on the quorum server to change the cipher suite to at least one of the cipher suites on the storage system:

```
admin:/>change

Usage: change white_list enable_switch=?
Enable or disable the whitelist function of a quorum server.
Note:
1. By default, the whitelist function of a quorum server is enabled.
2. After the whitelist function of a quorum server is disabled, all storage arrays that have the same CA certificate as a quorum server can access the quorum server, resulting in security risks. Therefore, you are advised not to disable the function.

[Arguments List]:

<enable_switch>     status of the whitelist function of a quorum server, the value can be "yes" or "no".
```



```
Usage: change cipher list=?
Give the usable and safety cipher list for ssl.
Note:
1. By default, all default ciphers are enabled.
2. After the cipher list changed, all links between quorum_server and storage device need rebuild.
Therefore, you are advised not to disable the function.
3. Note! AES256+RSA+SHA256 with CBC mode is not recommended!

[Arguments List]:

<list>usable ciphers to be used, the value can be "0 or 0,1 or 1 etc.".
0.AES256+RSA+SHA256:
1.AES128-GCM-SHA256:
2.AES256-GCM-SHA384:
3.ECDHE-RSA-AES128-GCM-SHA256:
4.ECDHE-RSA-AES256-GCM-SHA384:

admin:/>
```

----End

Follow-up Procedure

After the installation is successful, run the **quit** command to exit the CLI of the quorum server.

9.3.3 Installing Quorum Server Software on a Third-Party Server or Other TaiShan Servers

This section describes how to install the quorum server software on a third-party quorum server.

Prerequisites

- You have obtained the quorum server software package and uploaded it to the quorum server.
- The following tools and components are ready: OpenSSL, useradd, groupadd, chown, tar, bzip2, dpkg, or rpm.
- For security purposes, the entropy must be greater than 1024. You can run the **cat /proc/sys/kernel/random/entropy_avail** command to check the entropy. If the entropy is less than 1024, you can use **haveged** to increase the entropy.
- The quorum server has been deployed and its hardware meets the requirements specified in "Preparing for Installation".
- For versions earlier than 6.1.5, the validity period of the default arbitration certificate is 10 years. Ensure the system time of the quorum server is correct so that the default arbitration certificate is valid. 6.1.5 and later versions do not have default certificates or CA certificates.
- A Secure Shell (SSH) tool such as PuTTY has been prepared to log in to the quorum server.

NOTE

You are advised to harden the security of your operating system. For details, see the official security operation guide of the operating system.

Context

If the quorum server software is installed in the Ubuntu system, you must change the Ubuntu system shell from dash (default setting) to bash because the quorum server software must be installed in bash. This operation is required for other OSs.

To disable dash, run the **sudo dpkg-reconfigure dash** command in any directory of the Ubuntu system. Press the → key, select **No**, and press **Enter** to change dash to bash.

```
The system shell is the default command interpreter for shell scripts.
xUsing dash as the system shell will improve the system's overall performance. It does not alter the shell presented to interactive users.


Use dash as the default system shell (/bin/sh)?

                <Yes>                   <No>
```

Procedure

Step 1 Log in to the quorum server as the root user.

Step 2 Decompress the installation package.

1. In the operating system of the quorum server, run the **unzip** command to decompress the installation package.

```
XXX@Linux:~# unzip OceanStor/QuorumServer/OceanStor_QuorumServer_VXXXRXXXCXX.zip
Archive: OceanStor_QuorumServer_VXXXRXXXCXX.zip
package/
package/quorum_server.sh
package/packages/
package/packages/QuorumServer-VXXXRXXXCXX-linux.x86_64.rpm
package/qs_version.ini
package/tools/
```

2. After decompressing the installation package, run the **cd package** command to go to its directory.

```
XXX@Linux:~# cd package
```

3. (Optional) Run the **ll** command to list files in the directory.

Step 3 Install the quorum server software.

1. Run the **./quorum_server.sh -install** command to install the quorum server software.

> NOTE
>
> The non-root user account that is used to install the quorum server software will be used to run and manage the software in follow-up operations. If a password expiration policy is configured on the quorum server, the password of this account may expire, resulting in an access failure. Change the password regularly for security purposes.

```
XXX@Linux:~# ./quorum_server.sh -install
Verify the QuorumServer existence.
The QuorumServer is not installed.
The current user is the root user. A quorum server administrator account needs to be provided. Continue to install?
<Y|N>:Y                                 #Enter "Y" to install the quorum server software.
Enter an administrator account for the quorum server:[default: quorumsvr]:      #Press "Enter". The system installs the quorum server software under the default user account quorumsvr.
Created new account: quorumsvr.
Changing password for quorumsvr.
New Password:                                   #Set the password of user quorumsvr. You are advised to periodically change your password for security.
```



```
Reenter New Password:                          #Repeat the password.
Password changed.
Installing the quorum server.
Preparing...                ########################################### [100%]
   1:QuorumServer           ########################################### [100%]
[Notice] No old configuration need to resume.
QuorumServer install success completed.
```

NOTE

quorumsvr is the default user account for the quorum server software installation. If you want to install the quorum server software under another user account, enter the user name after **Enter an administrator account for the quorum server:[default: quorumsvr]**, for example, **Enter an administrator account for the quorum server:[default: quorumsvr]:User_test**.

Non-root user permissions are restricted for security purposes. You can run the **sudo** command to obtain permissions for the following commands: **cat**, **ps**, **sh**, **useradd**, **groupadd**, **userdel**, **groupdel**, **usermod**, **passwd**, **sed**, **rm**, **rpm**, **ls**, **chmod**, **chown**, **find**, **xargs**, **killall**, **mv**, **ln**, and **unzip**. For example, run the **sudo cat** *xxx* command, where *xxx* indicates the name of a file in the system.

Step 4 (Optional) Verify that the quorum server software is installed successfully.

1. After the quorum server software is installed, it starts automatically. Enter the CLI of the quorum server, go to any directory, and run the **qsadmin** command to open the quorum server software. If the software page is displayed, the software has restarted successfully.

   ```
   XXX@Linux:~# qsadmin
   start main!
   Waiting for connecting to server...
   admin:/>
   ```

2. Enter the CLI of the quorum server, go to any directory, and run the **ps -elf | grep quo*** command to check whether the quorum server software is installed successfully. If **/opt/quorum_server/bin/quorum_serverd** is displayed in the command output, the installation is successful.

   ```
   XXX@Linux:~# ps -elf |grep quo*

   4 S testUser  1102      1  0  80  0 -  137524 hrtime Apr29 ?     01:12:14 /opt/quorum_server/bin/
   quorum_serverd
   0 S testUser 21885  19967  0  80  0 -  28162 pipe_w 08:55 pts/3  00:00:00 grep --color=auto quo*
   ```

Step 5 (Optional) Set the cipher suite.

After the quorum server software is installed, the secure cipher suite is used by default. For compatibility with storage systems of earlier versions, the cipher suite may need to be modified.

1. Check the quorum server cipher suite on the storage device.

   ```
   admin:/>show quorum_server general
   ```

   The command output is as follows. Record the value of **Usable Cipher Suites**.

   ```
   admin:/>show quorum_server general
   Server ID  Server Name      Address      Port   Running Status  Usable Cipher Suites    All Cipher Suites
   ---------  ---------------  -----------  -----  --------------  ----------------------  -----------------------------
   0          QuorumServer_000  xx.xx.xx.xx  30002  Online          AES256+RSA+SHA256:AES256-GCM-
   SHA384:AES128-GCM-SHA256:@STRENGTH    AES256+RSA+SHA256:AES256-GCM-SHA384:AES128-
   GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:@STRENGTH
   ```

2. Check the cipher suite on the quorum server.

   ```
   admin:/>show cipher_info
   ```

   The command output is as follows. Record the value of **Current Cipher**.

   ```
   admin:/>show cipher_info
   ```

```
Current Cipher: : ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-
SHA384:@STRENGTH
Default Cipher List: : AES256+RSA+SHA256:AES256+DSS+SHA256:AES128-GCM-SHA256:AES256-GCM-
SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:@STRENGTH
Command executed successfully.
```

3. Check whether the **Usable Cipher Suites** field on the storage system and the **Current Cipher** field on the quorum server have a public cipher suite.

   The link can be set up only when a public cipher suite is available. If no public cipher suite is available, run the following commands on the quorum server to change the cipher suite to at least one of the cipher suites on the storage system:

```
admin:/>change

Usage: change white_list enable_switch=?
Enable or disable the whitelist function of a quorum server.
Note:
1. By default, the whitelist function of a quorum server is enabled.
2. After the whitelist function of a quorum server is disabled, all storage arrays that have the same CA
certificate as a quorum server can access the quorum server, resulting in security risks. Therefore, you
are advised not to disable the function.

[Arguments List]:

<enable_switch>     status of the whitelist function of a quorum server, the value can be "yes" or
"no".

Usage: change cipher list=?
Give the usable and safety cipher list for ssl.
Note:
1. By default, all default ciphers are enabled.
2. After the cipher list changed, all links between quorum_server and storage device need rebuild.
Therefore, you are advised not to disable the function.
3. Note! AES256+RSA+SHA256 with CBC mode is not recommended!

[Arguments List]:

<list>usable ciphers to be used, the value can be "0 or 0,1 or 1 etc.".
0.AES256+RSA+SHA256:
1.AES128-GCM-SHA256:
2.AES256-GCM-SHA384:
3.ECDHE-RSA-AES128-GCM-SHA256:
4.ECDHE-RSA-AES256-GCM-SHA384:

admin:/>
```

----End

Follow-up Procedure

After the installation is successful, run the **quit** command to exit the CLI of the quorum server.

9.4 Configuring Quorum Server Software

9.4.1 Huawei Dedicated Quorum Server

This section describes how to configure the quorum server software on a Huawei quorum server.

Context

The quorum server software must be configured by the same user account used to install it.

Procedure

Step 1 Prepare for the configuration.

Before the configuration, make sure that service IP addresses and a firewall have been configured for the quorum server.

NOTE

The quorum server software needs to use port 30002, which has been enabled by default on the firewall of the quorum server.

1. Configure service IP addresses for the quorum server.

   NOTE

   If the two ports on the quorum server are not bonded, they must use IP addresses on different network segments. If they are bonded, you only need to configure a virtual IP address.

   – If the ports are not bonded, configure two IP addresses on different network segments for the ports on the quorum server. **Table 9-4** provides an example.

   Table 9-4 Service IP address configuration

Quorum Port	Service IP Address	Mask
Quorum port 1	192.168.6.31	255.255.255.0
Quorum port 2	192.168.7.31	255.255.255.0

   Run the **vi** command to open the configuration file of the network adapters used by the quorum server. The following example uses quorum ports on network adapters **eth1** and **eth2**. Modify **IPADDR** and **NETMASK** and then save the file.

   NOTICE

   - The **ONBOOT** parameter must be set to **yes**.
   - The **STARTMODE** parameter must be set to **auto**.

```
Euler:~ # vi /etc/sysconfig/network-scripts/ifcfg-eth1

BOOTPROTO="static"
```



```
DEVICE="eth1"
IPADDR="192.168.6.31"
NETMASK="255.255.255.0"
STARTMODE="auto"
ONBOOT="yes"
GATEWAY="192.168.6.1"

Euler:~ # vi /etc/sysconfig/network-scripts/ifcfg-eth2

BOOTPROTO="static"
DEVICE="eth2"
IPADDR="192.168.7.31"
NETMASK="255.255.225.0"
STARTMODE="auto"
ONBOOT="yes"
GATEWAY="192.168.7.1"
```

- If the ports are bonded, you must configure a virtual IP address. The bond1 mode is recommended.

  The port bonding method for EulerOS is the same as that for CentOS. You can refer to the documentation of CentOS for details. The following is an example of bonding ports on the 2280 quorum server:

  i. Run the **cd /etc/sysconfig/network-scripts** command to enter the path where the port configuration file is saved.

  ii. Run the **vi ifcfg-***Port name* command to edit the port configuration file. **Table 9-5** describes the content of the configuration file.

  Table 9-5 Port configuration file

File Name	Content
ifcfg-eth0	DEVICE=eth0 BOOTPROTO=none ONBOOT=yes MASTER=bond1 SLAVE=yes USERCTL=no NM_CONTROLLED=no
ifcfg-eth1	DEVICE=eth1 BOOTPROTO=none ONBOOT=yes MASTER=bond1 SLAVE=yes USERCTL=no NM_CONTROLLED=no
ifcfg-bond1	USERCTL=no TYPE=Bonding MTU=1500 BONDING_OPTS='mode=1 miimon=100' DEVICE=bond1 BOOTPROTO=static ONBOOT=yes IPADDR=*xxx.xxx.xxx.xxx* PREFIX=*xx* GATEWAY=*xxx.xxx.xxx.xxx* NM_CONTROLLED=no BONDING_SLAVE0=eth0 BONDING_SLAVE1=eth1

  iii. Press **Esc** and enter **:wq** to save and quit the configuration file.

iv. Run the **service network restart** command to restart the network service.

v. Ping the virtual IP address to verify the network connectivity.

2. Verify that the service IP addresses for the quorum server have taken effect.

   Enter the CLI of the quorum server and run the **service network restart** command in any directory for the IP address settings to take effect. Then run the **ifconfig** command to check whether the configurations for **eth1** and **eth2** have taken effect. If the IP addresses that you configured are displayed in the command output, the configurations have taken effect.

```
XXX@Linux:~#ifconfig
Euler:~ # ifconfig
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.6.31  netmask 255.255.225.0  broadcast 192.168.6.255
        inet6 fe80::3ee8:24ff:fe8d:a02e  prefixlen 64  scopeid 0x20<link>
        ether 3c:e8:24:8d:a0:2e  txqueuelen 1000  (Ethernet)
        RX packets 14234838  bytes 931264105 (888.1 MiB)
        RX errors 0  dropped 27  overruns 0  frame 0
        TX packets 6201  bytes 429317 (419.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device memory 0xc6400000-c64fffff

eth2: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 192.168.7.31  netmask 255.255.255.0  broadcast 192.168.7.255
        ether 3c:e8:24:8d:a0:31  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device memory 0xc6100000-c61fffff
```

3. Configure a gateway for the quorum port of the quorum server.

   a. Run the **vim /etc/sysconfig/network-scripts/route-ethx** command to open the configuration file.

   b. Add the following gateway information to the configuration file.

```
0.0.0.0/0 via xxx.xxx.xxx.xxx dev ethx
```

      In the preceding information, *ethx* represents the name of the quorum port and *xxx.xxx.xxx* represents the gateway address.

      For example, if the quorum port is **eth0** and gateway address is **192.168.6.1**, add the following information:

```
0.0.0.0/0 via 192.168.6.1 dev eth0
```

   c. Save and close the configuration file.

Step 2 Open the CLI of the quorum server software.

In any directory of the quorum server's operating system, run the **qsadmin** command to open the quorum server software. The quorum server software page is displayed.

```
XXX@Euler:~# qsadmin
start main!
Waiting for connecting to server...
admin:/>
```

NOTE

After you open the quorum server software, run the **help** command for information and to learn about the commands that are required during the configuration process.

Step 3 Add the service IP addresses and port ID of the quorum server to the quorum server software.

In the CLI of the quorum server software, run the **add server_ip** command to add all service IP addresses and port ID of the quorum server to the quorum server software for management.

```
admin:/>add server_ip ip=192.168.6.31 port=30002
Command executed succesfully.
admin:/>add server_ip ip=192.168.7.31 port=30002
Command executed succesfully.
```

NOTE

- The quorum server uses these service IP addresses to communicate with the storage systems. If the two ports on the quorum server are not bonded, they must use IP addresses on different network segments. If they are bonded, you only need to configure a virtual IP address.
- The monitoring port of the quorum server software must be the same as that enabled on the firewall.

After configuration is complete, run the **show server_ip** command. If the command output shows the IP addresses and port ID that you add, the configuration is successful.

```
admin:/>show server_ip
Index      Server IP       Server Port
-----      ------------    ------------------
1          192.168.6.31    30002
2          192.168.7.31    30002
Index      Local IP       Local Port      Remote IP     Remote Port    State
-----      ------------    ---------      --------     ---------      -----
```

Step 4 (Optional) Replace the original certificates of the quorum server with new ones.

NOTE

- For versions earlier than 6.1.5, the storage systems and quorum server have default security certificates and private keys. To enhance security, replace them with your own.
- 6.1.5 and later versions do not have default certificates or CA certificates.

1. Export the certificate request file of the quorum server.

   In the CLI of the quorum server software, run the **export tls_cert** command to export the device information. The **qs_certreq.csr** file is generated in the **/opt/quorum_server/export_import** directory of the quorum server.

   ```
   admin:/>export tls_cert
   Command executed succesfully.
   ```

   NOTE

   - The certificates must be replaced in user mode.
   - After installing the quorum server software, you are advised to grant the Secure File Transfer Protocol (SFTP) permission only to the **/opt/quorum_server/export_import/** directory. This allows the security certificates to be imported and exported.

2. Use the certificate request file to generate certificates.

   To generate certificates, send the **qs_certreq.csr** file to any of the following CAs:

   - A third-party CA.

- A built-in CA on the HyperMetro quorum server. See **13.12 Issuing Certificates Using the Built-in CA on the Quorum Server (Applicable to 6.1.5 and Later)**.
- A built-in CA on the storage system. See the description about the HyperMetro certificate in section "Security Certificate Management" in the *Security Configuration Guide* specific to your product model.

3. Copy the certificates to the quorum server.

   After the certificates are generated, copy the quorum server certificate (for example, **qs_cert.crt**) and CA certificate (for example, **qs_cacert.crt**) to the **/opt/quorum_server/export_import** directory.

4. Change the owning user and user group of the quorum server certificate (for example, **qs_cert.crt**) and CA certificate (for example, **qs_cacert.crt**) to the user and user group used to install the quorum server software.

   ```
   chown quorumsvr:quorumsvr qs_cacert.crt
   chown quorumsvr:quorumsvr qs_cert.crt
   ```

   NOTE

   In this example, **quorumsvr** is the default installation user of the quorum server software. Change it to the actual user and user group you use to install the quorum server software.

5. Import the certificates to the quorum server software.

   In the CLI of the quorum server software, run the **import tls_cert ca=***qs_cacert.crt* **cert=***qs_cert.crt* command to import the certificates to the quorum server software.

   ```
   admin:/>import tls_cert ca=qs_cacert.crt cert=qs_cert.crt

   Command executed succesfully.
   ```

6. After replacing the certificates on the quorum server, replace the certificates on the local and remote storage systems.

   For details, see **13.9 Replacing Certificates**.

Step 5 (Optional) Configure a whitelist.

After replacing the quorum server certificate, you must configure a whitelist.

NOTICE

The quorum server software allows a storage system to connect to the quorum server only after you have added the SN of storage system to the whitelist. When replacing the certificate again, you must configure the whitelist again.

1. In the CLI of the storage system, run the **show system general** command to query the storage system SN.

   ```
   admin:/>show system general

   System Name : XXXXXX
   Health Status : Normal
   Running Status : Normal
   Total Capacity : X.XXXTB
   SN : XXXXXXXXXXXXXXXXXXX
   Location :
   Product Model : XXXXX
   Product Version : VX00R00XC00
   High Water Level(%) : XX
   ```



```
Low Water Level(%) : XX
WWN : XXXXXXXXXXXXXXX
Time : XXXX-XX-XX/15:11:15 UTC+08:00
```

2. In the CLI of the quorum server software, run the **add white_list sn=***?* command to add the storage system SN to the quorum server software for management.

```
admin:/>add white_list sn=xxxxxxxxxxxxxxxx

Command executed succesfully.
```

3. (Optional) Run the **change white_list enable_switch=***no* command to close the whitelist if you do not need to configure it.

----End

9.4.2 Third-Party Server Running SUSE

This section describes how to configure the quorum server software on a third-party quorum server running SUSE.

Prerequisites

The quorum server software must be configured by the same user account used to install it.

Procedure

Step 1 Prepare for the configuration.

Before the configuration, make sure that service IP addresses and a firewall have been configured for the quorum server.

1. Configure service IP addresses for the quorum server.

   NOTE

   If the two ports on the quorum server are not bonded, they must use IP addresses on different network segments. If they are bonded, you only need to configure a virtual IP address.

   – If you deploy the quorum server software on a VM, you must create virtual network adapters and switches for it. The following provides an example configuration in which the ports on the quorum server are not bonded. **Table 9-6** describes the configuration requirements.

   Figure 9-1 Virtual network adapter configuration

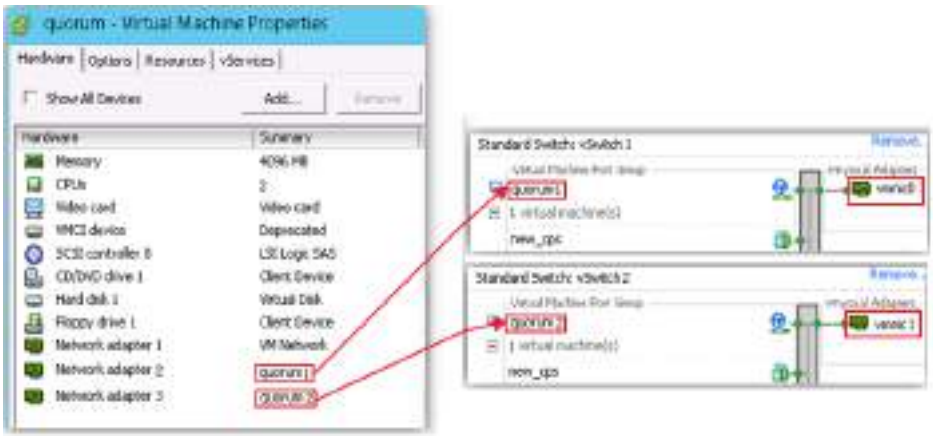


Table 9-6 Configuration requirements

Item	Configuration Requirement	Example
Network adapter 2	vmnic0 connects to controller A of the local and remote storage systems in the HyperMetro pair.	▪ Virtual switch name: vSwitch 1 ▪ Physical adapter name: vmnic0 ▪ Physical adapter IP address and mask: 192.168.6.31 and 255.255.255.0
Network adapter 3	vmnic1 connects to controller B of the local and remote storage systems in the HyperMetro pair.	▪ Virtual switch name: vSwitch 2 ▪ Physical adapter name: vmnic1 ▪ Physical adapter IP address and mask: 192.168.7.31 and 255.255.255.0

– If you deploy the quorum server software on a physical machine, it is recommended that you configure two IP addresses on different network segments for the ports on the quorum server. **Table 9-7** provides an example.

Table 9-7 Service IP address configuration

Quorum Port	Service IP Address	Mask
Quorum port 1	192.168.6.31	255.255.255.0
Quorum port 2	192.168.7.31	255.255.255.0

Run the **vi** command to open the configuration file of the network adapters used by the quorum server. The following example uses quorum ports on network adapters **eth1** and **eth2**. Modify **IPADDR** and then save the file.

NOTICE

The **STARTMODE** parameter must be set to **auto**.

```
XXX@Linux:~# vi /etc/sysconfig/network/ifcfg-eth1
BOOTPROTO='static'
BROADCAST=''
ETHTOOL_OPTIONS=''
IPADDR='192.168.6.31/24'
MTU=''
```



```
NAME='82540EM Gigabit Ethernet Controller'
NETWORK=''
REMOTE_IPADDR=''
STARTMODE='auto'
USERCONTROL='no'
XXX@Linux:~# vi /etc/sysconfig/network/ifcfg-eth2
BOOTPROTO='static'
BROADCAST=''
ETHTOOL_OPTIONS=''
IPADDR='192.168.7.31/24'
MTU=''
NAME='82540EM Gigabit Ethernet Controller'
NETWORK=''
REMOTE_IPADDR=''
STARTMODE='auto'
USERCONTROL='no'
```

- If you deploy the quorum server software on a physical machine and want to bond the ports, you must configure a virtual IP address.

  The operations for bonding ports vary with the Linux versions and host network adapters. The following is for reference only. For more details, see the documentation of your operating system.

  i. Check whether the system supports port bonding.

     Run the **#cat /boot/config-kernel-version |grep -i bonding** command.

     If **CONFIG_BONDING=m** is returned, the system supports port bonding. Otherwise, you are advised to configure an IP address for each physical port.

  ii. Create a configuration file for the bond port.

     The following provides the configuration file for **bond0** as an example.

     ```
     # vi  /etc/sysconfig/network-scripts/ifcfg-bond0
     DEVICE=bond0
     ONBOOT=yes
     BOOTPROTO=static
     IPADDR=192.168.1.202
     NETMASK=255.255.255.0
     GATEWAY=192.168.1.1
     USERCTL=no
     BONDING_OPTS="mode=0 miimon=100"
     ```

     In the configuration file, **mode** indicates the bonding mode and **miimon** indicates the interval (in milliseconds) for monitoring network links.

  iii. Modify the configuration files for the physical ports that are bonded.

     For example, to bond physical ports **eth0** and **eth1**, modify their configuration files as follows:

     ```
     #cat /etc/sysconfig/network-scripts/ifcfg-eth0
     DEVICE=eth0
     BOOTPROTO=none
     ONBOOT=yes
     USERCTL=no
     MASTER=bond0  //bond0 represents the name of the configuration file for the bond port.
     SLAVE=yes
     ```

     In the configuration file, set **MASTER** to the name of the configuration file for the bond port created in **Step 1.1.ii**.

  iv. Load the bond port.

     ```
     #vi /etc/modprobe.d/dist.conf
     alias bond0 bonding
     ```


bond0 represents the name of the configuration file for the bond port created in **Step 1.1.ii**.

v. Set the startup items.

```
#ifenslave bond0 eth0 eth1 >> /etc/rc.d/rc.local
```

vi. Restart the network service.

```
# service network restart
```

2. Verify that the service IP addresses for the quorum server have taken effect.

   Enter the CLI of the quorum server and run the **service network restart** command in any directory for the IP address settings to take effect. Then run the **ifconfig** command to check whether the configurations for **eth1** and **eth2** have taken effect. If the IP addresses that you configured are displayed in the command output, the configurations have taken effect.

```
XXX@Linux:~#ifconfig
eth1      Link encap:Ethernet  HWaddr 08:00:27:45:7A:E2
          inet addr: 192.168.6.31  Bcast:192.168.6.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe2e:fba6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:43285954 errors:0 dropped:5051127 overruns:0 frame:0
          TX packets:5819 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
           RX bytes:2916916679 (2781.7 Mb)  TX bytes:720809 (703.9 Kb)

eth2      Link encap:Ethernet  HWaddr 08:00:27:45:7A:EB
          inet addr: 192.168.7.31  Bcast:192.168.7.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe2e:fba7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:43285954 errors:0 dropped:5051127 overruns:0 frame:0
          TX packets:5819 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2916916679 (2781.7 Mb)  TX bytes:720809 (703.9 Kb)
```

3. Configure a port ID for the firewall of the quorum server.

   Enter the CLI of the quorum server and run the **vi /etc/sysconfig/SuSEfirewall2** command in any directory to open the firewall configuration file. Then, enter **FW_SERVICES_EXT_TCP="30002"** to enable port 30002.

   NOTE

   - If you want to enable other ports for the firewall, add the port IDs to the **FW_SERVICES_EXT_TCP** configuration item. For example, if you want to enable port 22, type **FW_SERVICES_EXT_TCP="30002 22"**.
   - If you deploy the quorum server software on a VM, enable the firewall port of the physical machine where the VM is deployed.

```
XXX@Linux:~# ## Type:        string
#
# 9.)
# Which TCP services _on the firewall_ should be accessible from
# untrusted networks?
#
# Format: space separated list of ports, port ranges or well known
#         service names (see /etc/services)
#
# Examples: "ssh", "123 514", "3200:3299", "ftp 22 telnet 512:514"
#
# Note: this setting has precedence over FW_SERVICES_ACCEPT_*
#
FW_SERVICES_EXT_TCP="30002"
```

4. Verify that the firewall configuration has taken effect.

   Enter the CLI of the quorum server and run the **rcSuSEfirewall2 restart** command in any directory to restart the firewall. Then run the **iptables -L**

command to check whether the firewall configuration has taken effect. If **ACCEPT tcp -- anywhere anywhere tcp dpt:pago-services2** is displayed in the command output, the firewall configuration has taken effect.

```
XXX@Linux:~# iptables -L
                    .
                    .
                    .
                    .
                    .
                    .
ACCEPT     tcp  --  anywhere     anywhere     tcp dpt:pago-services2
                    .
                    .
                    .
                    .
                    .
                    .
```

Step 2 Open the CLI of the quorum server software.

In any directory of the quorum server's operating system, run the **qsadmin** command to open the quorum server software. The quorum server software page is displayed.

```
XXX@Linux:~# qsadmin
start main!
Waiting for connecting to server...
admin:/>
```

NOTE

After you open the quorum server software, run the **help** command for information and to learn about the commands that are required during the configuration process.

Step 3 Add the service IP addresses and port ID of the quorum server to the quorum server software.

In the CLI of the quorum server software, run the **add server_ip** command to add all service IP addresses and port ID of the quorum server to the quorum server software for management.

```
admin:/>add server_ip ip=192.168.6.31 port=30002
Command executed succesfully.
admin:/>add server_ip ip=192.168.7.31 port=30002
Command executed succesfully.
```

NOTE

- The quorum server uses these service IP addresses to communicate with the storage systems.
  - If the two quorum ports on the quorum server are not bonded, the IP addresses on different network segments must be configured for the two quorum ports.
  - If the two quorum ports on the quorum server are bonded, you can only configure a virtual IP address for arbitration.
- The monitoring port of the quorum server software must be the same as that enabled on the firewall.

After configuration is complete, run the **show server_ip** command. If the command output shows the IP addresses and port ID that you add, the configuration is successful.

```
admin:/>show server_ip
Index      Server IP       Server Port
-----     ------------    ------------------
```



```
1       192.168.6.31   30002
2       192.168.7.31   30002
Index    Local IP      Local Port    Remote IP    Remote Port    State
-----    ------------  ----------    ---------    ----------     -----
```

Step 4 (Optional) Replace the original certificates of the quorum server with new ones.

NOTE

- For versions earlier than 6.1.5, the storage systems and quorum server have default security certificates and private keys. To enhance security, replace them with your own.
- 6.1.5 and later versions do not have default certificates or CA certificates.

1. Export the certificate request file of the quorum server.

   In the CLI of the quorum server software, run the **export tls_cert** command to export the device information. The **qs_certreq.csr** file is generated in the **/opt/quorum_server/export_import** directory of the quorum server.

   ```
   admin:/>export tls_cert
   Command executed succesfully.
   ```

   NOTE

   - The certificates must be replaced in user mode.
   - After installing the quorum server software, you are advised to grant the Secure File Transfer Protocol (SFTP) permission only to the **/opt/quorum_server/export_import/** directory. This allows the security certificates to be imported and exported.

2. Use the certificate request file to generate certificates.

   To generate certificates, send the **qs_certreq.csr** file to any of the following CAs:

   - A third-party CA.
   - A built-in CA on the HyperMetro quorum server. See **13.12 Issuing Certificates Using the Built-in CA on the Quorum Server (Applicable to 6.1.5 and Later)**.
   - A built-in CA on the storage system. See the description about the HyperMetro certificate in section "Security Certificate Management" in the *Security Configuration Guide* specific to your product model.

3. Copy the certificates to the quorum server.

   After the certificates are generated, copy the quorum server certificate (for example, **qs_cert.crt**) and CA certificate (for example, **qs_cacert.crt**) to the **/opt/quorum_server/export_import** directory.

4. Change the owning user and user group of the quorum server certificate (for example, **qs_cert.crt**) and CA certificate (for example, **qs_cacert.crt**) to the user and user group used to install the quorum server software.

   ```
   chown quorumsvr:quorumsvr qs_cacert.crt
   chown quorumsvr:quorumsvr qs_cert.crt
   ```

   NOTE

   In this example, **quorumsvr** is the default installation user of the quorum server software. Change it to the actual user and user group you use to install the quorum server software.

5. Import the certificates to the quorum server software.

   In the CLI of the quorum server software, run the **import tls_cert ca=***qs_cacert.crt* **cert=***qs_cert.crt* command to import the certificates to the quorum server software.


```
admin:/>import tls_cert ca=qs_cacert.crt cert=qs_cert.crt

Command executed succesfully.
```

6. After replacing the certificates on the quorum server, replace the certificates on the local and remote storage systems.

   For details, see **13.9 Replacing Certificates**.

Step 5 (Optional) Configure a whitelist.

The first time you replace the certificates, you must configure a whitelist.

NOTICE

The quorum server software allows a storage system to connect to the quorum server only after you have added the SN of storage system to the whitelist. When replacing the certificate again, you must configure the whitelist again.

1. In the CLI of the storage system, run the **show system general** command to query the storage system SN.

```
admin:/>show system general

System Name : XXXXXX
Health Status : Normal
Running Status : Normal
Total Capacity : X.XXXTB
SN : XXXXXXXXXXXXXXXXXXX
Location :
Product Model : XXXXX
Product Version : VX00R00XC00
High Water Level(%) : XX
Low Water Level(%) : XX
WWN : XXXXXXXXXXXXXXX
Time : XXXX-XX-XX/15:11:15 UTC+08:00
```

2. In the CLI of the quorum server software, run the **add white_list sn=***?* command to add the storage system SN to the quorum server software for management.

```
admin:/>add white_list sn=xxxxxxxxxxxxxx

Command executed succesfully.
```

3. (Optional) Run the **change white_list enable_switch=***no* command to close the whitelist if you do not need to configure it.

----End

9.4.3 Third-Party Server Running Ubuntu

This section describes how to configure the quorum server software on a third-party quorum server running Ubuntu.

Prerequisites

The quorum server software must be configured by the same user account used to install it.

Procedure

Step 1 Prepare for the configuration.

Before the configuration, make sure that service IP addresses and a firewall have been configured for the quorum server.

1. Configure service IP addresses for the quorum server.

   NOTE

   If the two ports on the quorum server are not bonded, they must use IP addresses on different network segments. If they are bonded, you only need to configure a virtual IP address.

   – If you deploy the quorum server software on a VM, you must create virtual network adapters and switches for it. The following provides an example configuration in which the ports on the quorum server are not bonded. **Table 9-8** describes the configuration requirements.

Figure 9-2 Virtual network adapter configuration

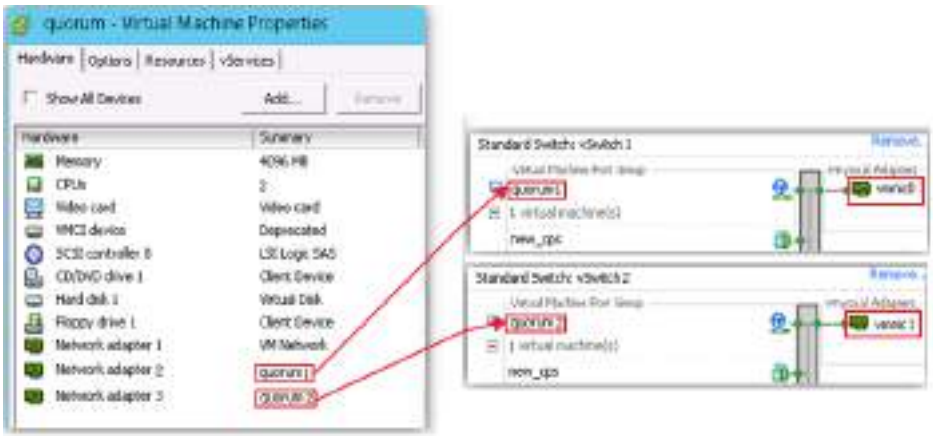


Table 9-8 Configuration requirements

Item	Configuration Requirement	Example
Network adapter 2	vmnic0 connects to controller A of the local and remote storage systems in the HyperMetro pair.	▪ Virtual switch name: vSwitch 1 ▪ Physical adapter name: vmnic0 ▪ Physical adapter IP address and mask: 192.168.6.31 and 255.255.255.0
Network adapter 3	vmnic1 connects to controller B of the local and remote storage systems in the HyperMetro pair.	▪ Virtual switch name: vSwitch 2 ▪ Physical adapter name: vmnic1 ▪ Physical adapter IP address and mask: 192.168.7.31 and 255.255.255.0

- If you deploy the quorum server software on a physical machine, it is recommended that you configure two IP addresses on different network segments for the ports on the quorum server. **Table 9-9** provides an example.

  Table 9-9 Service IP address configuration

Quorum Port	Service IP Address	Mask
Quorum port 1	192.168.6.31	255.255.255.0
Quorum port 2	192.168.7.31	255.255.255.0

  Run the **sudo vi /etc/network/interfaces** command to open the configuration file of the network adapter used by the quorum server. The following example uses quorum ports on network adapters **eth1** and **eth2**. Modify **address** and **netmask** and then save the file.

  NOTICE

  The start mode must be set to **auto**.

```
XXX@ubuntu:~$sudo vi /etc/network/interfaces
auto eth1  //The parameter must be set to auto.
iface eth1 inet static
address 192.168.6.31
gateway 192.168.6.1
netmask 255.255.255.0

auto eth2  //The parameter must be set to auto.
iface eth2 inet static
address 192.168.7.31
gateway 192.168.7.1
netmask 255.255.255.0
```

- If you deploy the quorum server software on a physical machine and want to bond the ports, you must configure a virtual IP address.

  For details about port bonding, see the documentation of your operating system.

2. Verify that the service IP addresses for the quorum server have taken effect.

   Enter the CLI of the quorum server and run **sudo ifdown eth1** and **sudo ifup eth1** in any directory to restart the network adapter. Then run the **ifconfig eth1** command to check whether the configuration has taken effect. If the IP address that you configured is displayed in the command output, the configuration has taken effect.

```
XXX@ubuntu:~$ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 08:00:27:45:7A:E2
          inet addr: 192.168.6.31  Bcast:192.168.6.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe2e:fba6/64 Scope:Link
```



```
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:43285954 errors:0 dropped:5051127 overruns:0 frame:0
        TX packets:5819 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:2916916679 (2781.7 Mb)  TX bytes:720809 (703.9 Kb)
```

Enter the CLI of the quorum server and run **sudo ifdown eth2** and **sudo ifup eth2** in any directory to restart the network adapter. Then run the **ifconfig eth2** command to check whether the configuration has taken effect. If the IP address that you configured is displayed in the command output, the configuration has taken effect.

```
XXX@ubuntu:~$ifconfig eth2
eth1      Link encap:Ethernet  HWaddr 08:00:27:45:7A:EB
          inet addr: 192.168.7.31  Bcast:192.168.7.255  Mask:255.255.0.0
          inet6 addr: fe80::a00:27ff:fe2e:fba7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:43285954 errors:0 dropped:5051127 overruns:0 frame:0
          TX packets:5819 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2916916679 (2781.7 Mb)  TX bytes:720809 (703.9 Kb)
```

3. Configure a port ID for the firewall of the quorum server.

   Enter the CLI of the quorum server and run the **sudo ufw allow 30002/tcp** command in any directory (taking **ufw** as an example) to enable port **30002**.

   NOTE

   - If you want to enable other ports for the firewall, run the **sudo ufw allow** *XXX*/*XXX* command again to add the port IDs. For example, if you want to enable port 22, run the **sudo ufw allow 22/tcp** command.
   - If you deploy the quorum server software on a VM, enable the firewall port of the physical machine where the VM is deployed.

   ```
   XXX@ubuntu:~$sudo ufw allow 30002/tcp
   Rule added
   Rule added (v6)
   ```

4. Verify that the firewall configuration has taken effect.

   Enter the CLI of the quorum server and run the **sudo ufw status** command in any directory to check whether the firewall configuration has taken effect. If **30002/tcp ALLOW Anywhere** and **30002/tcp(v6) ALLOW Anywhere (v6)** are displayed in the command output, the firewall configuration has taken effect.

   ```
   XXX@ubuntu:~$sudo ufw status
   To                         Action      From
   --                         ------      ----
                              .
                              .
                              .
                              .
   30002/tcp                  ALLOW       Anywhere
                              .
                              .
                              .
   30002/tcp (v6)             ALLOW       Anywhere (v6)
   ```

Step 2 Open the CLI of the quorum server software.

In any directory of the quorum server's operating system, run the **qsadmin** command to open the quorum server software. The quorum server software page is displayed.

```
XXX@ubuntu:~$ qsadmin
start main!
```



```
Waiting for connecting to server...
admin:/>
```

NOTE

After you open the quorum server software, run the **help** command for information and to learn about the commands that are required during the configuration process.

Step 3 Add the service IP addresses and port ID of the quorum server to the quorum server software.

In the CLI of the quorum server software, run the **add server_ip** command to add all service IP addresses and port ID of the quorum server to the quorum server software for management.

```
admin:/>add server_ip ip=192.168.6.31 port=30002
Command executed succesfully.
admin:/>add server_ip ip=192.168.7.31 port=30002
Command executed succesfully.
```

NOTE

- The quorum server uses these service IP addresses to communicate with the storage systems.
  - If the two quorum ports on the quorum server are not bonded, the IP addresses on different network segments must be configured for the two quorum ports.
  - If the two quorum ports on the quorum server are bonded, you can only configure a virtual IP address for arbitration.
- The monitoring port of the quorum server software must be the same as that enabled on the firewall.

After configuration is complete, run the **show server_ip** command. If the command output shows the IP addresses and port ID that you add, the configuration is successful.

```
admin:/>show server_ip
Index     Server IP      Server Port
1         192.168.6.31   30002
2         192.168.7.31   30002
Index     Local IP      Local Port     Remote IP     Remote Port    State
-----     ------------   ---------      --------     ---------      -----
```

Step 4 (Optional) Replace the original certificates of the quorum server with new ones.

NOTE

- For versions earlier than 6.1.5, the storage systems and quorum server have default security certificates and private keys. To enhance security, replace them with your own.
- 6.1.5 and later versions do not have default certificates or CA certificates.

1. Export the certificate request file of the quorum server.

   In the CLI of the quorum server software, run the **export tls_cert** command to export the device information. The **qs_certreq.csr** file is generated in the **/opt/quorum_server/export_import** directory of the quorum server.

   ```
   admin:/>export tls_cert

   Command executed succesfully.
   ```

NOTE

- The certificates must be replaced in user mode.
- After installing the quorum server software, you are advised to grant the Secure File Transfer Protocol (SFTP) permission only to the **/opt/quorum_server/export_import/** directory. This allows the security certificates to be imported and exported.

2. Use the certificate request file to generate certificates.

   To generate certificates, send the **qs_certreq.csr** file to any of the following CAs:

   - A third-party CA.
   - A built-in CA on the HyperMetro quorum server. See **13.12 Issuing Certificates Using the Built-in CA on the Quorum Server (Applicable to 6.1.5 and Later)**.
   - A built-in CA on the storage system. See the description about the HyperMetro certificate in section "Security Certificate Management" in the *Security Configuration Guide* specific to your product model.

3. Copy the certificates to the quorum server.

   After the certificates are generated, copy the quorum server certificate (for example, **qs_cert.crt**) and CA certificate (for example, **qs_cacert.crt**) to the **/opt/quorum_server/export_import** directory.

4. Change the owning user and user group of the quorum server certificate (for example, **qs_cert.crt**) and CA certificate (for example, **qs_cacert.crt**) to the user and user group used to install the quorum server software.

```
chown quorumsvr:quorumsvr qs_cacert.crt
chown quorumsvr:quorumsvr qs_cert.crt
```

   NOTE

   In this example, **quorumsvr** is the default installation user of the quorum server software. Change it to the actual user and user group you use to install the quorum server software.

5. Import the certificates to the quorum server software.

   In the CLI of the quorum server software, run the **import tls_cert ca=***qs_cacert.crt* **cert=***qs_cert.crt* command to import the certificates to the quorum server software.

```
admin:/>import tls_cert ca=qs_cacert.crt cert=qs_cert.crt

Command executed succesfully.
```

6. After replacing the certificates on the quorum server, replace the certificates on the local and remote storage systems.

   For details, see **13.9 Replacing Certificates**.

Step 5 (Optional) Configure a whitelist.

The first time you replace the certificates, you must configure a whitelist.

NOTICE

The quorum server software allows a storage system to connect to the quorum server only after you have added the SN of storage system to the whitelist. When replacing the certificate again, you must configure the whitelist again.

1. In the CLI of the storage system, run the **show system general** command to query the storage system SN.

```
admin:/>show system general

 System Name         : XXXXXX
 Health Status       : Normal
 Running Status      : Normal
 Total Capacity      : X.XXXTB
 SN                  : XXXXXXXXXXXXXXXXXXX
 Location            :
 Product Model       : XXXXX
 Product Version     : VX00R00XC00
 High Water Level(%) : XX
 Low Water Level(%)  : XX
 WWN                 : XXXXXXXXXXXXXXX
 Time                : XXXX-XX-XX/15:11:15 UTC+08:00
```

2. In the CLI of the quorum server software, run the **add white_list sn=***?* command to add the storage system SN to the quorum server software for management.

```
admin:/>add white_list sn=xxxxxxxxxxxxx

Command executed succesfully.
```

3. (Optional) Run the **change white_list enable_switch=***no* command to close the whitelist if you do not need to configure it.

----End

9.4.4 Huawei TaiShan or Third-Party Server Running Red Hat, Red Flag, NeoKylin, or CentOS

This section describes how to configure the quorum server software on a third-party quorum server running Red Hat, Red Flag, NeoKylin, or CentOS.

Prerequisites

The quorum server software must be configured by the same user account used to install it.

Context

Huawei TaiShan server does not support the Red Flag OS.

Procedure

Step 1 Prepare for the configuration.

Before the configuration, make sure that service IP addresses and a firewall have been configured for the quorum server.

1. Configure service IP addresses for the quorum server.

   NOTE

   If the two ports on the quorum server are not bonded, they must use IP addresses on different network segments. If they are bonded, you only need to configure a virtual IP address.

   – If you deploy the quorum server software on a VM, you must create virtual network adapters and switches for it. The following provides an

example configuration in which the ports on the quorum server are not bonded. **Table 9-10** describes the configuration requirements.

Figure 9-3 Virtual network adapter configuration

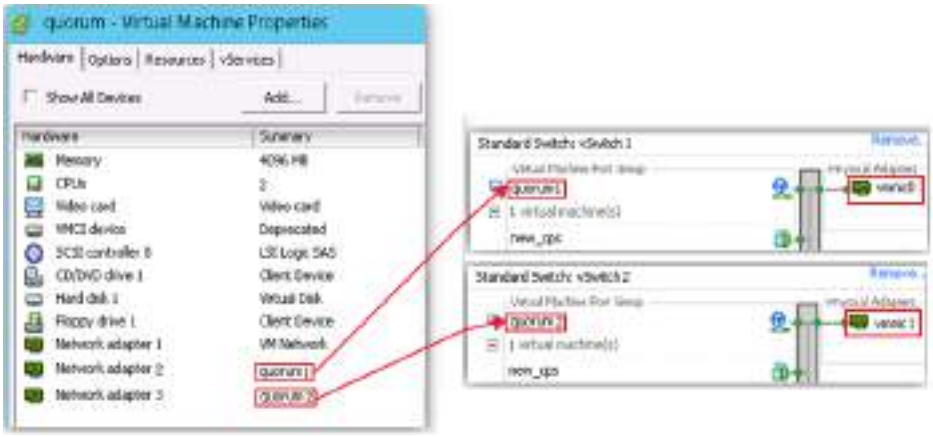


Table 9-10 Configuration requirements

Item	Configuration Requirement	Example
Network adapter 2	vmnic0 connects to controller A of the local and remote storage systems in the HyperMetro pair.	▪ Virtual switch name: vSwitch 1 ▪ Physical adapter name: vmnic0 ▪ Physical adapter IP address and mask: 192.168.6.31 and 255.255.255.0
Network adapter 3	vmnic1 connects to controller B of the local and remote storage systems in the HyperMetro pair.	▪ Virtual switch name: vSwitch 2 ▪ Physical adapter name: vmnic1 ▪ Physical adapter IP address and mask: 192.168.7.31 and 255.255.255.0

– If you deploy the quorum server software on a physical machine, it is recommended that you configure two IP addresses on different network segments for the ports on the quorum server. **Table 9-11** provides an example.

Table 9-11 Service IP address configuration

Quorum Port	Service IP Address	Mask
Quorum port 1	192.168.6.31	255.255.255.0

Quorum Port	Service IP Address	Mask
Quorum port 2	192.168.7.31	255.255.255.0

Run the **vi** command to open the configuration file of the network adapters used by the quorum server. The following example uses quorum ports on network adapters **eth1** and **eth2**. Modify **IPADDR** and **NETMASK** and then save the file.

NOTICE

The **ONBOOT** parameter must be set to **yes**.

```
XXX@Linux:~# vi /etc/sysconfig/network-scripts/ifcfg-eth1
DEVICE=eth1
HWADDR=08:00:27:45:7A:E2
TYPE=Ethernet
UUID=e9f75670-fde9-4bf0-941e-c9a251341405
ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=static
IPADDR=192.168.6.31                    #IP address of the network adapter
NETMASK=255.255.255.0                      #Subnet mask

XXX@Linux:~# vi /etc/sysconfig/network-scripts/ifcfg-eth2
DEVICE=eth2
HWADDR=08:00:27:45:7A:EB
TYPE=Ethernet
UUID=e9f75670-fde9-4bf0-941e-c9a251341406
ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=static
IPADDR=192.168.7.31                    # IP address of the network adapter
NETMASK=255.255.255.0                      #Subnet mask
```

- If you deploy the quorum server software on a physical machine and want to bond the ports, you must configure a virtual IP address.

  For details about port bonding, see the documentation of your operating system.

2. Verify that the service IP addresses for the quorum server have taken effect.

   Enter the CLI of the quorum server and run the **service network restart** command in any directory for the IP address settings to take effect. Then run the **ifconfig** command to check whether the configurations for **eth1** and **eth2** have taken effect. If the IP addresses that you configured are displayed in the command output, the configurations have taken effect.

```
XXX@Linux:~#ifconfig
eth1      Link encap:Ethernet  HWaddr 08:00:27:45:7A:E2
          inet addr: 192.168.6.31  Bcast:192.168.6.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe2e:fba6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:43285954 errors:0 dropped:5051127 overruns:0 frame:0
          TX packets:5819 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
           RX bytes:2916916679 (2781.7 Mb)  TX bytes:720809 (703.9 Kb)
```



```
eth2      Link encap:Ethernet  HWaddr 08:00:27:45:7A:EB
          inet addr: 192.168.7.31  Bcast:192.168.7.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe2e:fba7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:43285954 errors:0 dropped:5051127 overruns:0 frame:0
          TX packets:5819 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2916916679 (2781.7 Mb)  TX bytes:720809 (703.9 Kb)
```

3. Configure a port ID for the firewall of the quorum server.
   - For Red Hat/CentOS 7.X

     Write the firewall port ID to the configuration file using either of the following methods:

     - Modifying the configuration file:

     i. Enter the CLI of the quorum server and run the **vi /etc/firewalld/zones/public.xml** command in any directory to open the firewall configuration file.

     ii. Add the following item: **<port protocol="tcp" port="30002"/>**.

     ```
     XXX@Linux:~# vi /etc/firewalld/zones/public.xml
     <?xml version="1.0" encoding="utf-8"?>
     <zone>
       <short>Public</short>
       <description>For use in public areas. You do not trust the other computers on networks to not harm your computer. Only selected incoming connections are accepted.</description>
       <service name="dhcpv6-client"/>
       <service name="ssh"/>
       <port protocol="tcp" port="30002"/>
     </zone>
     ```

     - Using commands:

       Enter the CLI of the quorum server and run the **firewall-cmd --permanent --zone=public --add-port=30002/tcp** command in any directory.

       ```
       XXX@Linux:~# firewall-cmd --permanent --zone=public --add-port=30002/tcp  success
       ```

   - For OSs other than Red Hat/CentOS 7.X

     Enter the CLI of the quorum server and run the **vi /etc/sysconfig/iptables** command in any directory to open the firewall configuration file. Then add **-I INPUT -p tcp --dport=30002 -j ACCEPT** to enable port **30002**.

     ```
     XXX@Linux:~# vi /etc/sysconfig/iptables
     *filter
     :INPUT ACCEPT [0:0]
     :FORWARD ACCEPT [0:0]
     :OUTPUT ACCEPT [0:0]

     -I INPUT -p tcp --dport=30002 -j ACCEPT
     COMMIT
     ```


NOTE

- If **/etc/sysconfig/iptables** does not exist or is empty, write all of the preceding content into the configuration file.
- If **/etc/sysconfig/iptables** has content, add **-I INPUT -p tcp --dport=30002 -j ACCEPT** before **COMMIT**.
- If you want to enable other ports for the firewall, add the port IDs to the **-I INPUT -p XXX --dport=XXX -j ACCEPT** configuration item. For example, if you want to enable port **22**, enter **-I INPUT -p tcp --dport=22 -j ACCEPT**.
- If you deploy the quorum server software on a VM, enable the firewall port of the physical machine where the VM is deployed.

4. Restart the firewall for the configuration to take effect.
   - For Red Hat 6.X and CentOS 6.X:

     Run the following command in any directory on the CLI of the quorum server:

     ```
     XXX@Linux: service iptables stop
     XXX@Linux: service iptables start
     ```

   - For Red Hat 7.X, Red Flag, NeoKylin, and CentOS 7.X:

     Run the **systemctl restart firewalld** command in any directory on the CLI of the quorum server.

     ```
     XXX@Linux:~# systemctl restart firewalld
     ```

5. Verify that the firewall configuration has taken effect.

   Enter the CLI of the quorum server and run the **service iptables restart** command in any directory to restart the firewall. Then run the **iptables -L** command to check whether the firewall configuration has taken effect. If **ACCEPT tcp -- anywhere anywhere tcp dpt:pago-services2** is displayed in the command output, the firewall configuration has taken effect.

   ```
   XXX@Linux:~# iptables -L
                        .
                        .
                        .
                        .
                        .
                        .
   ACCEPT     tcp  --  anywhere     anywhere     tcp dpt:pago-services2
                        .
                        .
                        .
                        .
                        .
                        .
   ```

Step 2 Open the CLI of the quorum server software.

In any directory of the quorum server's operating system, run the **qsadmin** command to open the quorum server software. The quorum server software page is displayed.

```
XXX@Linux:~# qsadmin
start main!
Waiting for connecting to server...
admin:/>
```


NOTE

After you open the quorum server software, run the **help** command for information and to learn about the commands that are required during the configuration process.

Step 3 Add the service IP addresses and port ID of the quorum server to the quorum server software.

In the CLI of the quorum server software, run the **add server_ip** command to add all service IP addresses and port ID of the quorum server to the quorum server software for management.

```
admin:/>add server_ip ip=192.168.6.31 port=30002
Command executed succesfully.
admin:/>add server_ip ip=192.168.7.31 port=30002
Command executed succesfully.
```

NOTE

- The quorum server uses these service IP addresses to communicate with the storage systems.
  - If the two quorum ports on the quorum server are not bonded, the IP addresses on different network segments must be configured for the two quorum ports.
  - If the two quorum ports on the quorum server are bonded, you can only configure a virtual IP address for arbitration.
- The monitoring port of the quorum server software must be the same as that enabled on the firewall.

After configuration is complete, run the **show server_ip** command. If the command output shows the IP addresses and port ID that you add, the configuration is successful.

```
admin:/>show server_ip
Index      Server IP       Server Port
-----      ------------    ------------------
1          192.168.6.31    30002
2          192.168.7.31    30002
Index      Local IP        Local Port      Remote IP     Remote Port    State
-----      ------------    ---------       --------      ---------      -----
```

Step 4 (Optional) Replace the original certificates of the quorum server with new ones.

NOTE

- For versions earlier than 6.1.5, the storage systems and quorum server have default security certificates and private keys. To enhance security, replace them with your own.
- 6.1.5 and later versions do not have default certificates or CA certificates.

1. Export the certificate request file of the quorum server.

   In the CLI of the quorum server software, run the **export tls_cert** command to export the device information. The **qs_certreq.csr** file is generated in the **/opt/quorum_server/export_import** directory of the quorum server.

   ```
   admin:/>export tls_cert

   Command executed succesfully.
   ```


NOTE

- The certificates must be replaced in user mode.
- After installing the quorum server software, you are advised to grant the Secure File Transfer Protocol (SFTP) permission only to the **/opt/quorum_server/export_import/** directory. This allows the security certificates to be imported and exported.

2. Use the certificate request file to generate certificates.

   To generate certificates, send the **qs_certreq.csr** file to any of the following CAs:

   - A third-party CA.
   - A built-in CA on the HyperMetro quorum server. See **13.12 Issuing Certificates Using the Built-in CA on the Quorum Server (Applicable to 6.1.5 and Later)**.
   - A built-in CA on the storage system. See the description about the HyperMetro certificate in section "Security Certificate Management" in the *Security Configuration Guide* specific to your product model.

3. Copy the certificates to the quorum server.

   After the certificates are generated, copy the quorum server certificate (for example, **qs_cert.crt**) and CA certificate (for example, **qs_cacert.crt**) to the **/opt/quorum_server/export_import** directory.

4. Change the owning user and user group of the quorum server certificate (for example, **qs_cert.crt**) and CA certificate (for example, **qs_cacert.crt**) to the user and user group used to install the quorum server software.

```
chown quorumsvr:quorumsvr qs_cacert.crt
chown quorumsvr:quorumsvr qs_cert.crt
```

   NOTE

   In this example, **quorumsvr** is the default installation user of the quorum server software. Change it to the actual user and user group you use to install the quorum server software.

5. Import the certificates to the quorum server software.

   In the CLI of the quorum server software, run the **import tls_cert ca=***qs_cacert.crt* **cert=***qs_cert.crt* command to import the certificates to the quorum server software.

```
admin:/>import tls_cert ca=qs_cacert.crt cert=qs_cert.crt

Command executed succesfully.
```

6. After replacing the certificates on the quorum server, replace the certificates on the local and remote storage systems.

   For details, see **13.9 Replacing Certificates**.

Step 5 (Optional) Configure a whitelist.

The first time you replace the certificates, you must configure a whitelist.

NOTICE

The quorum server software allows a storage system to connect to the quorum server only after you have added the SN of storage system to the whitelist. When replacing the certificate again, you must configure the whitelist again.

1. In the CLI of the storage system, run the **show system general** command to query the storage system SN.

```
admin:/>show system general

 System Name         : XXXXXX
 Health Status       : Normal
 Running Status      : Normal
 Total Capacity      : X.XXXTB
 SN                  : XXXXXXXXXXXXXXXXXXX
 Location            :
 Product Model       : XXXXX
 Product Version     : VX00R00XC00
 High Water Level(%) : XX
 Low Water Level(%)  : XX
 WWN                 : XXXXXXXXXXXXXXX
 Time                : XXXX-XX-XX/15:11:15 UTC+08:00
```

2. In the CLI of the quorum server software, run the **add white_list sn=***?* command to add the storage system SN to the quorum server software for management.

```
admin:/>add white_list sn=xxxxxxxxxxxxx

Command executed succesfully.
```

3. (Optional) Run the **change white_list enable_switch=***no* command to close the whitelist if you do not need to configure it.

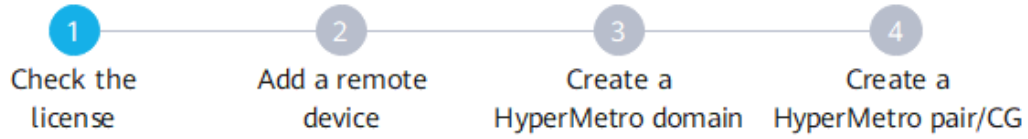
----End

10 Configuring HyperMetro (System User)

10.1 Checking the License

A license grants the permission to use HyperMetro. Ensure that the storage systems have a valid HyperMetro license.

Configuration Wizard



Prerequisites

The license file has been imported.

Context

On DeviceManager, the name of the HyperMetro license is **HyperMetro (for LUN)**.

NOTE

For OceanStor 18510 and 18810, find **HyperMetro (for LUN)** on the **License Management** page of DeviceManager and ensure that the used capacity in the **Used/Total Capacity** column does not exceed the total capacity.

Procedure

Step 1 Log in to DeviceManager of the local and remote storage systems.

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

Step 3 In the middle information pane, verify the information about the active license file.

----End

Related Operations

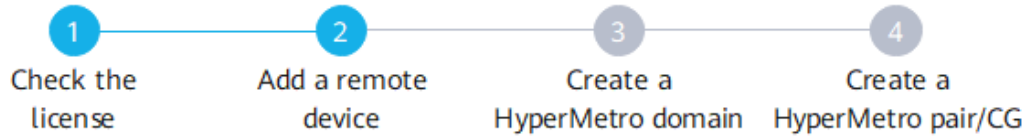
If no HyperMetro license is available, you must apply for, import, and activate the license. For details, see the initialization guide specific to your product model.

You can log in to Huawei's technical support website (**https://support.huawei.com/enterprise/**) and enter the product model + document name in the search box to search for, browse, and download the desired documents.

10.2 Adding a Remote Device

This section describes how to establish a logical connection between a local and a remote storage system for data transmission.

Configuration Wizard



Precautions

- When adding an IP or RoCE link, ensure that the maximum transmission units (MTUs) of the ports at both ends are the same.
- Before you add a remote device on a Fibre Channel network, clear the zone configurations for the ports that the switches use to connect to the storage systems. It is recommended that you allocate no more than two ports in any zone to prevent the number of remote links from exceeding the system's specifications.
- For details about the number of ports that can be used for replication on a controller, refer to the Specifications Query (**https://support-it.huawei.com/spec/#/home**).
- If a firewall is deployed, ports 12002, 12003, 12004, and 12005 must be enabled for RoCE links, and port 12001 must be enabled for IP links.

(For RoCE Replication Links) Procedure

Step 1 Add an authentication user.

1. Log in to DeviceManager of the remote device.
2. Choose **Settings** > **User and Security** > **Users and Roles** > **Users**.
3. Click **Create**.
4. Set user information.

   Set **Type** to **Local user** and configure the parameters listed in **Table 10-1**.

   Table 10-1 Local user parameters

Parameter	Description
Username	Name of the new user.
Password	Password of the new user.
Confirm Password	Confirmation of the password.
Role	Select **Remote device administrator**.
Description	Description of the new user.
Login Method	The login method for the remote device administrator is **RESTful**.

Step 2 Create VLANs.

NOTE

If **Trust Mode** of a RoCE port is **DSCP**, the VLAN created on the RoCE port cannot be used to create a logical port for the replication network. Choose **Services > Network > RoCE Network** and click the name of a RoCE port to check its trust mode.

1. Log in to DeviceManager of the local and remote storage systems.
2. Choose **Services** > **Network** > **RoCE Network** > **VLANs**.
3. Click **Create**. The **Create VLAN** dialog box is displayed.
4. In the port list, select a home port for creating a VLAN.
5. Enter an ID for the VLAN to be created and click **Add**.

   NOTE

   - The same VLAN ID must be configured for the interconnected replication ports on the local device, remote device, and switches.
   - The VLAN ID ranges from 1 to 4094. You can enter a single VLAN ID or VLAN IDs in a batch. The batch input format is "start VLAN ID-end VLAN ID".
6. Click **OK**.

Step 3 Create logical ports for the RoCE replication links.

1. Log in to DeviceManager of the local and remote storage systems.
2. Choose **Services** > **Network** > **Logical Ports**.

3. Click **Create**. The **Create Logical Port** page is displayed.
4. Set the parameters in **Table 10-2**.

Table 10-2 Logical port parameters

Parameter	Description
Name	Name of the logical port. The name must meet the following requirements: – The name must be unique. – The name can contain only letters, digits, periods (.), underscores (_), and hyphens (-). – The name contains 1 to 255 characters.
Role	Select **Replication**.
IP Address Type	IP address type of the logical port, which can be IPv4 or IPv6.
IP	IPv4 or IPv6 address of the logical port.
Subnet Mask	Subnet mask of the logical port's IPv4 address.
Prefix	Prefix length of the logical port's IPv6 address.
Gateway	IPv4 or IPv6 gateway of the logical port.
Port Type	Type of the port for which you want to create a logical port. For RoCE replication links, select **VLAN**. **NOTE** If **Port Type** is **VLAN**, the system does not display the VLANs for RoCE ports whose **Trust Mode** is **DSCP**.
Home Port	Physical port on which the logical port is created.

Step 4 (For data transmission across network segments) Configure routes.

1. Log in to DeviceManager of the local and remote storage systems.
2. Select the created logical port.
3. Click **Manage Route**. The **Manage Route** page is displayed.
4. Click **Add**.
5. In **Type**, select the type of route you want to add. **Table 10-3** lists the related parameters.

Table 10-3 Route types

Route Type	Description
Default route	A route through which data is forwarded by default if no preferred route is available. The destination address and mask (IPv4) or prefix (IPv6) of the default route are automatically set to 0. To use this option, you only need to add a gateway.
Host route	A route to a host. The subnet mask (IPv4) or prefix (IPv6) of the host route are automatically set to 255.255.255.255 or 128. To use this option, you only need to add the destination address and gateway.
Network segment route	A route to a network segment. You must add the destination address, destination mask (IPv4) or prefix (IPv6), and gateway. For example, the destination address is 172.17.0.0, subnet mask is 255.255.0.0, and gateway is 172.16.0.1.

6. Set **Destination Address**.
   - If **IP Address** is an IPv4 address, set **Destination Address** to the IPv4 address or network segment of the application server's service network port or that of the other storage system's Ethernet port.
   - If **IP Address** is an IPv6 address, set **Destination Address** to the IPv6 address or network segment of the application server's service network port or that of the other storage system's Ethernet port.
7. Set **Subnet Mask/Prefix**.
   - If **Subnet Mask** is set for an IPv4 address, this parameter specifies the subnet mask of the IPv4 address for the application server's service network port or the other storage system's Ethernet port.
   - If **Prefix** is set for an IPv6 address, this parameter specifies the prefix of the IPv6 address for the application server's service network port or the other storage system's Ethernet port.
8. In **Gateway**, enter the gateway of the local storage system's Ethernet port IP address.
9. Click  to add the route information to the route list.

Step 5 (Optional) Create an IPsec policy (applicable to 6.1.5 and later).

NOTE

- After an IPsec policy is created for the replication network logical ports on the storage devices at both ends of the replication link, data is encrypted during replication to ensure security. This operation must be performed on the storage devices at both ends of the replication link.
- Prerequisites:
  - You can create an IPsec policy only when the replication network is an IP network.
  - You can create an IPsec policy only when the replication network IP address is an IPv4 address.
  - You cannot create an IPsec policy, if the logical port of the replication network is created on a port that is bound across interface modules.
  - For details about the number of IPsec policies and IPsec link specifications, see **Specifications Query**.
  - For the interface modules that support IPsec policies, see **15.6 Which Interface Modules Support IPsec Policies?**.

1. Set the security type of the interface module to IPsec.
   a. Log in to DeviceManager.
   b. Choose **System** > **Hardware** > **Devices**.
   c. Click the controller enclosure that houses the interface module.
   d. Click  to switch to the rear view of the storage device.
   e. Click the desired interface module.
   f. On the page that is displayed, choose **Operation** > **Switch Security Type** in the upper right corner.
   g. Set **Security Type** to **IPsec**.

      When **Security Type** is **IPsec**, TOE is disabled for all ports on the interface module and cannot be enabled independently.
   h. Confirm your operation as prompted.
2. Log in to DeviceManager.
3. Choose **Services** > **Network** > **Logical Ports**.
4. Select the desired logical port and click **Manage IPsec Policy**.
5. Click **Create**.

   Table 10-8 describes the parameters.

Table 10-4 IPsec policy parameters

Parameter	Description
Name	Name of an IPsec policy.
Remote IP Address	Replication network IP address of the remote storage device in the replication link. Only IPv4 addresses are supported. **NOTE** You can add or delete IP addresses by modifying the created IPsec policy.

Parameter	Description
Pre-shared Key	User-defined pre-shared key. The pre-shared keys at both ends of a replication link must be the same. AES is used by default. [Value range] – The value contains 16 to 127 characters. – The value must contain at least two of the following types: special characters, uppercase letters, lowercase letters, and digits. Special characters include ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ ` { _ | } ~ and spaces.

6. Click **OK**.

   NOTE

   If an IPsec policy is no longer needed, delete it from both storage devices. When you delete it on one storage device, the replication service will be interrupted. After you delete it on the other storage device, the replication service will recover automatically. Therefore, you are advised to delete an IPsec policy when no replication service exists and delete it from both storage devices at a short interval.

Step 6 Add the remote device.

1. Log in to DeviceManager of the local storage system.
2. Choose **Data Protection** > **Configuration** > **Remote Devices**.
3. Click . The **Add Remote Device** page is displayed.
4. Set **Link Type** to **IP Link**.
5. Specify the **Local Port** for the IP link.
6. Specify the IP address of the logical port on the remote device.
7. Enter the user name and password of the remote device administrator created earlier.
8. Click **Connect**. After the connection is successful, click **OK**.

   NOTE

   – You can click in the upper right corner of the created remote device and choose **Add Link** to add redundant links. When adding a RoCE link, ensure that the MTUs of the ports at both ends are the same.

   – To set the data compression policy and bandwidth limit, click in the upper right corner of the created remote device and choose **Modify**.

----End

(For IP Replication Links) Procedure

Step 1 Add an authentication user.

1. Log in to DeviceManager of the remote device.
2. Choose **Settings** > **User and Security** > **Users and Roles** > **Users**.

3. Click **Create**.
4. Set user information.

   Set **Type** to **Local user** and configure the parameters listed in **Table 10-5**.

Table 10-5 Local user parameters

Parameter	Description
Username	Name of the new user.
Password	Password of the new user.
Confirm Password	Confirmation of the password.
Password Always Valid	If this function is enabled, the password is not restricted by the password validity period specified in the security policy. This function is enabled by default.
Role	Select **Remote device administrator**.
Description	Description of the new user.
Login Method	The login method for the remote device administrator is **RESTful**.

Step 2 Create logical ports for the IP replication links.

1. Log in to DeviceManager of the local and remote storage systems.
2. Choose **Services** > **Network** > **Logical Ports**.
3. Click **Create**. The **Create Logical Port** page is displayed.
4. Set the parameters in **Table 10-6**.

Table 10-6 Logical port parameters

Parameter	Description
Name	Name of the logical port. The name must meet the following requirements: – The name must be unique. – The name can contain only letters, digits, periods (.), underscores (_), and hyphens (-). – The name contains 1 to 255 characters.
Role	Select **Replication**.
IP Address Type	IP address type of the logical port, which can be IPv4 or IPv6.
IP	IPv4 or IPv6 address of the logical port.
Subnet Mask	Subnet mask of the logical port's IPv4 address.

Parameter	Description
Prefix	Prefix length of the logical port's IPv6 address.
Gateway	IPv4 or IPv6 gateway of the logical port.
Port Type	Type of the port for which you want to create a logical port. The port type can be Ethernet port, bond port, or VLAN.
Home Port	Physical port on which the logical port is created.

Step 3 (For data transmission across network segments) Configure routes.

1. Log in to DeviceManager of the local and remote storage systems.
2. Select the created logical port.
3. Click **Manage Route**. The **Manage Route** page is displayed.
4. Click **Add**.
5. In **Type**, select the type of route you want to add. **Table 10-7** lists the related parameters.

Table 10-7 Route types

Route Type	Description
Default route	A route through which data is forwarded by default if no preferred route is available. The destination address and mask (IPv4) or prefix (IPv6) of the default route are automatically set to 0. To use this option, you only need to add a gateway.
Host route	A route to a host. The subnet mask (IPv4) or prefix (IPv6) of the host route are automatically set to 255.255.255.255 or 128. To use this option, you only need to add the destination address and gateway.
Network segment route	A route to a network segment. You must add the destination address, destination mask (IPv4) or prefix (IPv6), and gateway. For example, the destination address is 172.17.0.0, subnet mask is 255.255.0.0, and gateway is 172.16.0.1.

6. Set **Destination Address**.
   - If **IP Address** is an IPv4 address, set **Destination Address** to the IPv4 address or network segment of the application server's service network port or that of the other storage system's Ethernet port.
   - If **IP Address** is an IPv6 address, set **Destination Address** to the IPv6 address or network segment of the application server's service network port or that of the other storage system's Ethernet port.
7. Set **Subnet Mask/Prefix**.

- If **Subnet Mask** is set for an IPv4 address, this parameter specifies the subnet mask of the IPv4 address for the application server's service network port or the other storage system's Ethernet port.
- If **Prefix** is set for an IPv6 address, this parameter specifies the prefix of the IPv6 address for the application server's service network port or the other storage system's Ethernet port.

8. In **Gateway**, enter the gateway of the local storage system's Ethernet port IP address.
9. Click  to add the route information to the route list.

Step 4 (Optional) Create an IPsec policy (applicable to 6.1.5 and later).

NOTE

- After an IPsec policy is created for the replication network logical ports on the storage devices at both ends of the replication link, data is encrypted during replication to ensure security. This operation must be performed on the storage devices at both ends of the replication link.
- Prerequisites:
  - You can create an IPsec policy only when the replication network is an IP network.
  - You can create an IPsec policy only when the replication network IP address is an IPv4 address.
  - You cannot create an IPsec policy, if the logical port of the replication network is created on a port that is bound across interface modules.
  - For details about the number of IPsec policies and IPsec link specifications, see **Specifications Query**.
  - For the interface modules that support IPsec policies, see **15.6 Which Interface Modules Support IPsec Policies?**.

1. Set the security type of the interface module to IPsec.
   a. Log in to DeviceManager.
   b. Choose **System** > **Hardware** > **Devices**.
   c. Click the controller enclosure that houses the interface module.
   d. Click  to switch to the rear view of the storage device.
   e. Click the desired interface module.
   f. On the page that is displayed, choose **Operation** > **Switch Security Type** in the upper right corner.
   g. Set **Security Type** to **IPsec**.

      When **Security Type** is **IPsec**, TOE is disabled for all ports on the interface module and cannot be enabled independently.
   h. Confirm your operation as prompted.
2. Log in to DeviceManager.
3. Choose **Services** > **Network** > **Logical Ports**.
4. Select the desired logical port and click **Manage IPsec Policy**.
5. Click **Create**.

   Table 10-8 describes the parameters.

Table 10-8 IPsec policy parameters

Parameter	Description
Name	Name of an IPsec policy.
Remote IP Address	Replication network IP address of the remote storage device in the replication link. Only IPv4 addresses are supported. **NOTE** You can add or delete IP addresses by modifying the created IPsec policy.
Pre-shared Key	User-defined pre-shared key. The pre-shared keys at both ends of a replication link must be the same. AES is used by default. [Value range] – The value contains 16 to 127 characters. – The value must contain at least two of the following types: special characters, uppercase letters, lowercase letters, and digits. Special characters include ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ ` { _ | } ~ and spaces.

6. Click **OK**.

   NOTE

   If an IPsec policy is no longer needed, delete it from both storage devices. When you delete it on one storage device, the replication service will be interrupted. After you delete it on the other storage device, the replication service will recover automatically. Therefore, you are advised to delete an IPsec policy when no replication service exists and delete it from both storage devices at a short interval.

Step 5 Add the remote device.

1. Log in to DeviceManager of the local storage system.
2. Choose **Data Protection** > **Configuration** > **Remote Devices**.
3. Click . The **Add Remote Device** page is displayed.
4. Set **Link Type** to **IP Link**.
5. Specify the **Local Port** for the IP link.
6. Specify the IP address of the logical port on the remote device.
7. Enter the user name and password of the remote device administrator created earlier.
8. Click **Connect**. After the connection is successful, click **OK**.

NOTE

- You can click ⋮ in the upper right corner of the created remote device and choose **Add Link** to add redundant links.
- To set the data compression policy, click ⋮ in the upper right corner of the created remote device and choose **Modify**.

----End

(For Fibre Channel Replication Links) Procedure

Step 1 Add an authentication user.

1. Log in to DeviceManager of the remote device.
2. Choose **Settings** > **User and Security** > **Users and Roles** > **Users**.
3. Click **Create**.
4. Set user information.

   Set **Type** to **Local user** and configure the parameters listed in **Table 10-9**.

   Table 10-9 Local user parameters

Parameter	Description
Username	Name of the new user.
Password	Password of the new user.
Confirm Password	Confirmation of the password.
Password Always Valid	If this function is enabled, the password is not restricted by the password validity period specified in the security policy. This function is enabled by default.
Role	Select **Remote device administrator**.
Description	Description of the new user.
Login Method	The login method for the remote device administrator is **RESTful**.

Step 2 Add the remote device.

1. Log in to DeviceManager of the local storage system.
2. Choose **Data Protection** > **Configuration** > **Remote Devices**.
3. Click +. The **Add Remote Device** page is displayed.
4. Set **Link Type** to **FC Link**.
5. Select a remote device from the **Remote Device** drop-down list.
6. Select a Fibre Channel link from the **FC Link** drop-down list.
7. Enter the user name and password of the remote device administrator created earlier.

8. Click **Connect**. After the connection is successful, click **OK**.

   NOTE

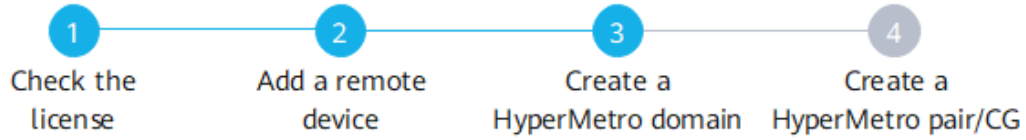
   - After the remote device is successfully connected, the storage system automatically identifies all Fibre Channel links. For reliability purposes, ensure that each controller of the storage systems at both sites has two links. If there is only one link, click ⋮ in the upper right corner of the remote device and choose **Add Link**.
   - To set the data compression policy, click ⋮ in the upper right corner of the created remote device and choose **Modify**.

----End

10.3 Creating a Block HyperMetro Domain

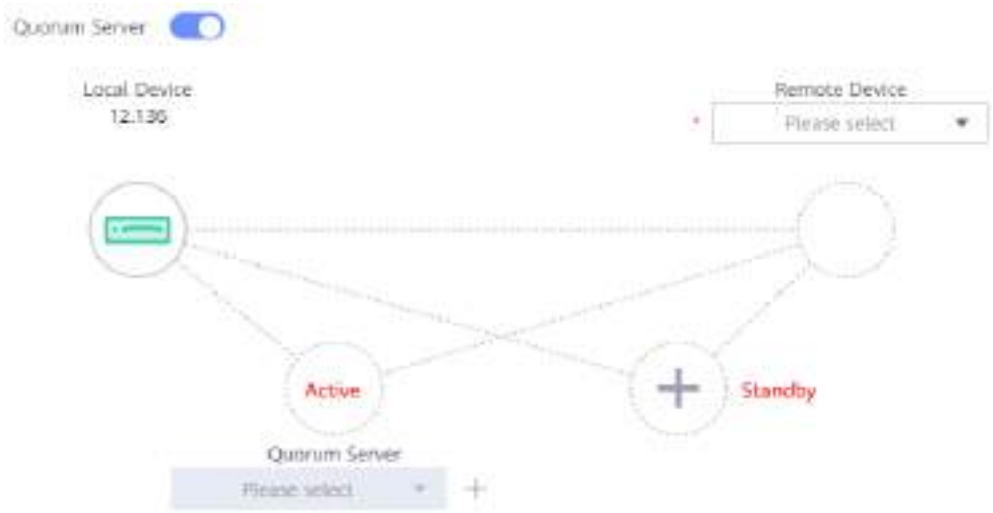
The HyperMetro domain defines the relationships among the local and remote devices as well as the quorum server.

Configuration Wizard



Context

- A HyperMetro domain is a collection of local and remote devices and a quorum server (which is optional). It defines the relationships among the local and remote devices as well as the quorum server. On DeviceManager, you can check whether the HyperMetro domain uses one or two quorum servers or no quorum server (static priority mode).
- During initial synchronization, the remote device serves as the secondary end of HyperMetro.
- If a quorum server is configured, the quorum server determines which site continues providing services in the event of a fault. If no quorum server is configured for the HyperMetro domain, the preferred site continues providing services by default in the event of a fault.
- Two quorum servers can be deployed and work in active/standby mode. On DeviceManager, the one on the left is the active quorum server by default.



Procedure

Step 1 Log in to DeviceManager of the local device.

Step 2 Choose **Data Protection** > **Configuration** > **HyperMetro Domains**.

Step 3 Click + under **HyperMetro Domains for Block**.

The **Create HyperMetro Domain** page is displayed.

Step 4 Specify the name and description for the HyperMetro domain.

NOTE

- The name must be unique.
- The name contains 1 to 31 characters.
- The name can contain only letters, digits, underscores (_), hyphens (-), and periods (.) and must start with a letter or digit.
- The description can be left blank or contain up to 127 characters.

Step 5 Determine whether to enable **Quorum Server**.

- If you enable **Quorum Server**:
  a. In the **Remote Device** area, select a remote device that you want to add to the HyperMetro domain.
  b. In the **Quorum Server** area, select a quorum server that you want to add to the HyperMetro domain.

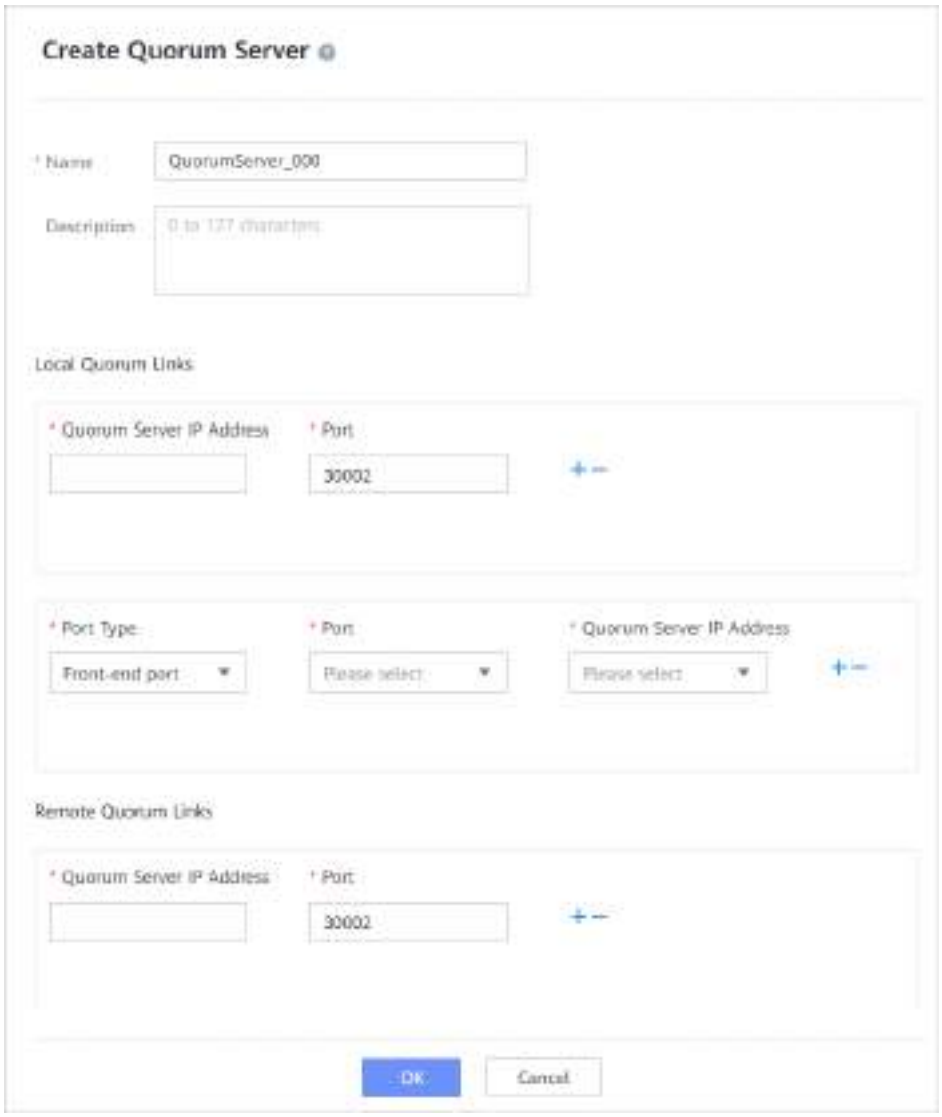
  NOTE

  You can click + in the **Quorum Server** area to add another quorum server.

  c. Click +. On the page that is displayed, create a quorum server.

NOTICE

Before adding a quorum server, ensure that the certificates used by the quorum server and HyperMetro storage systems are issued by the same CA. Otherwise, adding quorum server links fails.



i. Set **Name** and **Description** for the quorum server.

NOTE

- The name must be unique.
- The name contains 1 to 31 characters.
- The name can contain only letters, digits, underscores (_), periods (.), and hyphens (-).
- The description can be left blank or contain up to 127 characters.

ii. Set the **Local Quorum Server Links** and **Remote Quorum Server Links**.

NOTE

- You can click + or — to add or remove a link.
- Configure at least one local and one remote quorum link.
- If the port type is **Front-end port**, select a logical port whose role is **Replication** for the quorum link.
- To ensure reliability, it is recommended that you add at least one link from the quorum server to each storage controller.
- This operation will create a quorum server on both the local and remote storage systems.

iii. Click **OK**.

- If you use the static priority mode:
  a. Disable **Quorum Server**.
  b. In the **Remote Device** area, select a remote device that you want to add to the HyperMetro domain.

NOTE

- You are advised to configure quorum servers. (The current HyperMetro domain supports a maximum of two quorum servers.)
- If no quorum server is configured, when the preferred site is faulty, the non-preferred site cannot automatically take over HyperMetro services. As a result, the services stop and you need to forcibly start the non-preferred site to provide services for the host.
- You can modify the HyperMetro domain to add a quorum server in follow-up operations.

Step 6 Click **OK**.

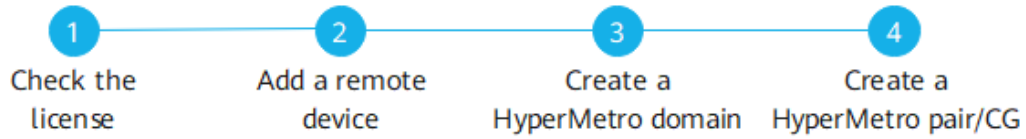
Confirm your operation as prompted.

----End

10.4 Creating a HyperMetro Pair/CG

This section describes how to set up a HyperMetro relationship between the local and remote resources.

Configuration Wizard



Context

When you create a HyperMetro CG using a LUN group, the system first creates a PG for this LUN group. If you want to create a HyperMetro CG using a PG, choose

Data Protection > **Protection Entities** > **Protection Groups** > **Protection Groups** and manually create a PG. Then create a HyperMetro CG for the PG.

Prerequisites

- A LUN has been created on the local storage system.
- A storage pool has been created on the remote storage system.
- The remote LUN (if created) has not been mapped to a host.
- You cannot create a HyperMetro pair for a LUN if a remote replication pair has been created for this LUN and the HyperMetro pair you want to create uses the same remote device as this remote replication pair.

Procedure for Creating a HyperMetro Pair for a LUN

Step 1 Create a HyperMetro pair.

1. Log in to DeviceManager of the local storage system.
2. Choose **Services** > **Block Service** > **LUN Groups** > **LUNs**.
3. Select the desired LUN, click **Protect**, and select **Create HyperMetro**. The **Create HyperMetro Pair** page is displayed.
4. Select a HyperMetro domain.
5. Set **Pair Creation** to **Automatic**.

   NOTE

   - If you set **Pair Creation** to **Automatic**, the storage system automatically creates a remote LUN in the storage pool of the remote device and creates a HyperMetro pair for the selected local and remote LUNs.
   - If you set **Pair Creation** to **Manual**, you must manually create a remote LUN and add the LUNs to the pair.
6. Select the target vStore and storage pool for creating remote resources of HyperMetro.
7. Set the remote resource name. Possible options are:
   - **Same as local**: The system uses the name of a local LUN to create a remote LUN.
   - **Custom**: Set the prefix and suffix of the remote resource names. The system then creates a remote LUN named in the format of *Prefix + Local LUN name + Suffix*.

     NOTE

     - A prefix contains 0 to 32 characters, and a suffix contains 0 to 16 characters. The prefix and suffix cannot both be left blank.
     - A prefix or suffix can contain only letters, digits, underscores (_), hyphens (-), and periods (.).
     - If a local resource name is too long, the system automatically truncates it and uses the truncated local resource name and the specified prefix and suffix to create a remote resource.
8. Set the service assurance policy of the HyperMetro pair. Possible values are:
   - **Service continuity preferred**

The system preferentially ensures service continuity. It is used when host services require low storage latency. When the average write latency difference between local and remote resources of HyperMetro pairs is greater than **Isolation Threshold**, the system automatically disconnects the HyperMetro pairs and the resources with lower write latency continues providing services. When you select **Service continuity preferred**, set **Isolation Threshold (ms)**, which ranges from 10 to 30000.

- **Data reliability preferred**

  The system ensures service data reliability preferentially. This value applies to scenarios that have high requirements for data protection. Data on local and remote resources is synchronized in real time.

9. (Optional) Select **Advanced** in the upper right corner and set the advanced parameters.

   NOTE

   By default, **Speed** is **Medium**, **Recovery Policy** is **Automatic**, and **Initial Sync** is **Automatic**.

   Table 10-10 describes the parameters.

Table 10-10 Advanced properties of a HyperMetro pair

Parameter	Description
Speed	Data synchronization speed of the HyperMetro pair. Possible values are as follows: – **Low**: 0 MB/s to 5 MB/s. At this setting, data synchronization takes a long period of time. This value is used when the service load is heavy. – **Medium**: 10 MB/s to 20 MB/s. At this setting, data synchronization takes a relatively short period of time. This value is used when the service load is relatively heavy. – **High**: 20 MB/s to 70 MB/s. At this setting, data synchronization takes a short period of time. This value is used when the service load is relatively light. – **Highest**: Above 100 MB/s. At this setting, data synchronization takes a very short period of time. This value is used when the service load is light. – **Custom**: User-defined synchronization speed. The value ranges from 1 MB/s to 1024 MB/s.
Recovery Policy	Determines how data is synchronized after a fault is rectified. – **Automatic**: The system automatically synchronizes data. – **Manual**: Data must be synchronized manually.

Parameter	Description
Initial Sync	Initial synchronization mode of local and remote resources. When **Pair Creation** is set to **Automatic**, the value can be: – **Automatic**: The system automatically synchronizes data between the local and remote resources upon pair creation. – **Manual**: Data must be manually synchronized between local and remote resources. When **Pair Creation** is set to **Manual**, the value can be: – If data is inconsistent: ▪ **Automatic**: The system automatically synchronizes data between the local and remote resources upon pair creation. ▪ **Manual**: Data must be manually synchronized between local and remote resources. – If data is consistent, synchronization is not required.

NOTE

It is recommended that you perform synchronization tests for different speeds and select a proper speed based on the test result. Choose a faster speed as long as the bandwidth is sufficient.

Step 2 Configure mappings.

1. If the local LUN has been mapped, you only need to perform the following operations on DeviceManager of the remote storage system.
2. Choose **Services** > **Block Service** > **LUN Groups** > **LUNs**.
3. Select the desired LUNs and click **Map**.
4. Set the host and port group information.
5. Select **Advanced** in the upper right corner and set advanced parameters. **Table 10-11** describes the parameters.

Table 10-11 Advanced parameters for LUN mapping

Parameter	Description
Host LUN ID	Specifies how to assign host LUN IDs. – **Automatic**: The system assigns a host LUN ID to each LUN mapped to a host. – **Start ID**: Set a start ID ranging from 0 to 4095. The system assigns a host LUN ID to each LUN mapped to a host, starting from **Start ID**. – **Specified ID**: Manually assign a host LUN ID to each LUN mapped to a host.
Same Host LUN ID	Determines whether to keep host LUN IDs consistent. If you select this option, the system forcibly ensures that the host LUN IDs of the local and remote LUNs in the HyperMetro pairs are the same in the SAN HyperMetro scenario. In scenarios involving ESX hosts, if the host LUN IDs of the local and remote LUNs in the same HyperMetro pairs are different, data may be inconsistent.

Step 3 Verify the mappings.

1. Log in to a host as user **root**.
2. Run the **hot_add** command to scan for LUNs.
3. Run the **upadmin show vlun type=all** command to query the LUNs mapped to the host.

----End

Procedure for Creating a HyperMetro CG for a LUN Group

Step 1 Create a LUN group.

1. Log in to DeviceManager of the local storage system.
2. Choose **Services** > **Block Service** > **LUN Groups**.
3. Click **Create** and follow the wizard on DeviceManager to create a LUN group.

Step 2 Create a HyperMetro CG.

1. Select the created LUN group, click **Protect**, and select **Create HyperMetro**. The **Create HyperMetro CG** page is displayed.

NOTE

When you create a HyperMetro CG using a LUN group, the system first creates a PG for this LUN group. You can change the name of the PG. If you want to create a HyperMetro CG using a PG, choose **Data Protection** > **Protection Entities** > **Protection Groups** > **Protection Groups** and manually create a PG. Then create a HyperMetro CG for the PG.

2. Select a HyperMetro domain.
3. Set **Pair Creation** to **Automatic**.

NOTE

- If **Pair Creation** is set to **Automatic**, the system automatically creates remote LUNs and a remote LUN group on the remote storage system, and adds them to HyperMetro pairs and a CG. Ensure that no HyperMetro pair has been created for the LUNs in the LUN group. If remote LUNs or HyperMetro pairs already exist, create the CG manually to prevent configuration conflicts.
- If **Pair Creation** is set to **Manual**, you must manually select a LUN group on the remote storage system, which must contain the same number and capacities of LUNs as the local LUN group, and then manually match the LUNs. Ensure that the remote LUN group and its LUNs have not been mapped. If the LUN group or any LUN has been mapped, delete the mapping first to prevent configuration conflicts.

4. Select the target vStore and storage pool for creating remote resources of HyperMetro.
5. Set the remote resource name. Possible options are:
   - **Same as local**: The system uses the name of a local LUN, local LUN group, or local PG to create a remote LUN, remote LUN group, or remote PG.
   - **Custom**: Set the prefix and suffix of the remote resource names. The system then creates a remote LUN, remote LUN group, or remote PG named in the format of *Prefix + Local LUN name/Local LUN group name/Local PG name + Suffix*.

     NOTE

     - A prefix contains 0 to 32 characters, and a suffix contains 0 to 16 characters. The prefix and suffix cannot both be left blank.
     - A prefix or suffix can contain only letters, digits, underscores (_), hyphens (-), and periods (.).
     - If a local resource name is too long, the system automatically truncates it and uses the truncated local resource name and the specified prefix and suffix to create a remote resource.

6. Set the service assurance policy of HyperMetro pairs. Possible values are:
   - **Service continuity preferred**

     The system preferentially ensures service continuity. It is used when host services require low storage latency. When the average write latency difference between local and remote resources of HyperMetro pairs is greater than **Isolation Threshold**, the system automatically disconnects the HyperMetro pairs and the resources with lower write latency continues providing services.

     When you select **Service continuity preferred**, set **Isolation Threshold (ms)**, which ranges from 10 to 30000.

- **Data reliability preferred**

  The system ensures service data reliability preferentially. This value applies to scenarios that have high requirements for data protection. Data on local and remote resources is synchronized in real time.

7. (Optional) Select **Advanced** in the upper right corner and set the advanced parameters.

   NOTE

   By default, **Speed** is **Medium**, **Recovery Policy** is **Automatic**, and **Initial Sync** is **Automatic**.

   Table 10-12 describes the parameters.

Table 10-12 HyperMetro CG advanced properties

Parameter	Description
Pair Sync Speed	Data synchronization speed of the HyperMetro CG. Possible values are as follows: – **Low**: 0 MB/s to 5 MB/s. At this setting, data synchronization takes a long period of time. This value is used when the service load is heavy. – **Medium**: 10 MB/s to 20 MB/s. At this setting, data synchronization takes a relatively short period of time. This value is used when the service load is relatively heavy. – **High**: 20 MB/s to 70 MB/s. At this setting, data synchronization takes a short period of time. This value is used when the service load is relatively light. – **Highest**: Above 100 MB/s. At this setting, data synchronization takes a very short period of time. This value is used when the service load is light. – **Custom**: User-defined synchronization speed. The value ranges from 1 MB/s to 1024 MB/s.
Recovery Policy	Determines how data is synchronized after a fault is rectified. – **Automatic**: The system automatically synchronizes data. – **Manual**: Data must be synchronized manually.

Parameter	Description
Initial Sync	Initial synchronization mode of local and remote resources. When **Pair Creation** is set to **Automatic**, the value can be: – **Automatic**: The system automatically synchronizes data between the local and remote resources upon pair creation. – **Manual**: Data must be manually synchronized between local and remote resources. When **Pair Creation** is set to **Manual**, the value can be: – If data is inconsistent: ▪ **Automatic**: The system automatically synchronizes data between the local and remote resources upon pair creation. ▪ **Manual**: Data must be manually synchronized between local and remote resources. – If data is consistent, synchronization is not required.

NOTE

It is recommended that you perform synchronization tests for different speeds and select a proper speed based on the test result. Choose a faster speed as long as the bandwidth is sufficient.

8. Click **Next**.
9. Configure the mapping.

NOTE

The LUNs at both ends of a HyperMetro pair must be mapped to the same host. You can enable **Map to Same Host or Host Group** to quickly create the mapping.

a. Enable **Map to Same Host or Host Group**.

NOTE

- When LUNs are mapped to the same host or host group, the initiator information of the hosts to which the HyperMetro LUNs are mapped must be the same on the local and remote storage systems.
- If you want to map LUNs to different hosts, disable **Map to Same Host or Host Group** and configure the mappings for the local and remote LUNs separately.

b. Select **Advanced** in the upper right corner and determine whether to select **Same Host LUN ID**. If you select this option, the system forcibly ensures that the host LUN IDs of the local and remote LUNs in the HyperMetro pairs are the same in the SAN HyperMetro scenario. In scenarios involving ESX hosts, if the host LUN IDs of the local and remote

LUNs in the same HyperMetro pairs are different, data may be inconsistent.

c. Select a host or host group to which you want to map the LUNs.

NOTE

In no host or host group is available, click **Create** to create one.

d. (Optional) Select **Local Port Group**.

NOTE

After a port group is selected, LUNs in the LUN group use the ports of the port group to communicate with hosts in the host group. If no port group is selected, available ports are randomly used.

e. Set how to assign host LUN IDs.

- **Automatic**: The system assigns a host LUN ID to each LUN mapped to a host.
- **Start ID**: Set a start ID ranging from 0 to 4095. The system assigns a host LUN ID to each LUN mapped to a host, starting from **Start ID**.
- **Specified ID**: Manually assign a host LUN ID to each LUN mapped to a host.

NOTE

- If **Map to Same Host or Host Group** and **Same Host LUN ID** are disabled, you can set the host LUN ID allocation mode of the remote LUNs to **Automatic** or **Start ID**.
- If **Map to Same Host or Host Group** is disabled but **Same Host LUN ID** is enabled, you can set the host LUN ID allocation mode of the remote LUNs only to **Automatic**.

f. Specify **Host Access Mode**. Possible values are **Load balancing** or **Asymmetric**.

NOTE

Load balancing allows the host to access both storage systems with equal priority.

Asymmetric enables the host to preferentially access a specified storage system.

10. Follow the wizard to complete later operations.

----End

10.5 Precautions for Dual-Quorum-Server Mode

This section describes the precautions for deploying two quorum servers at the quorum site.

The delivery procedure for dual-quorum-server deployment is the same as that for single-quorum-server deployment. Note the following when configuring the quorum servers:

- The quorum server software must be installed and configured on both quorum servers.

- When you create quorum servers on storage systems, the quorum server that is added first is active, and the other one is standby.
- When creating a HyperMetro domain, you must add both quorum servers to the domain.
- In dual-quorum-server mode, ensure that the HyperMetro arbitration certificates used by quorum servers and storage systems are issued by the same CA. For example, if the built-in CA on a quorum server has issued a certificate, certificates used by all connected storage systems and quorum servers must be issued by the CA on the same quorum server.

11 Configuring HyperMetro (vStore User)

The storage system allows you to configure HyperMetro in the vStore view. In the vStore view, vStore users configure protection measures for their own resources separately.

Prerequisites

- The system user has added a remote device and created a block HyperMetro domain.
- A LUN has been created on the local storage system of HyperMetro.
- A storage pool has been created on the remote storage system.
- The remote LUN (if created) has not been mapped to a host.
- You cannot create a HyperMetro pair for a LUN if a remote replication pair has been created for this LUN and the HyperMetro pair you want to create uses the same remote device as this remote replication pair.

Procedure for Creating a HyperMetro Pair for a LUN

Step 1 Create a HyperMetro pair.

1. Log in to DeviceManager of the local storage system.
2. Choose **Services** > **Block Service** > **LUN Groups** > **LUNs**.
3. Select the desired LUN, click **Protect**, and select **Create HyperMetro**. The **Create HyperMetro Pair** page is displayed.
4. Select a HyperMetro domain.
5. Set **Pair Creation** to **Automatic**.

   NOTE

   - If you set **Pair Creation** to **Automatic**, the storage system automatically creates a remote LUN in the storage pool of the remote device and creates a HyperMetro pair for the selected local and remote LUNs.
   - If you set **Pair Creation** to **Manual**, you must manually create a remote LUN and add the LUNs to the pair.
6. Select the target storage pool for creating remote resources of HyperMetro.

7. Set the service assurance policy of the HyperMetro pair. Possible options are:
   - **Service continuity preferred**

     The system preferentially ensures service continuity. It is used when host services require low storage latency. When the average write latency difference between local and remote resources of HyperMetro pairs is greater than **Isolation Threshold**, the system automatically disconnects the HyperMetro pairs and the resources with lower write latency continues providing services. When you select **Service continuity preferred**, set **Isolation Threshold (ms)**, which ranges from 10 to 30000.
   - **Data reliability preferred**

     The system ensures service data reliability preferentially. This value applies to scenarios that have high requirements for data protection. Data on local and remote resources is synchronized in real time.
8. (Optional) Select **Advanced** in the upper right corner and set the advanced parameters.

   NOTE

   By default, **Speed** is **Medium**, **Recovery Policy** is **Automatic**, and **Initial Sync** is **Automatic**.

   Table 11-1 describes the parameters.

Table 11-1 Advanced properties of a HyperMetro pair

Parameter	Description
Speed	Data synchronization speed of the HyperMetro pair. Possible values are: – **Low**: 0 MB/s to 5 MB/s. At this setting, data synchronization takes a long period of time. This value is used when the service load is heavy. – **Medium**: 10 MB/s to 20 MB/s. At this setting, data synchronization takes a relatively short period of time. This value is used when the service load is relatively heavy. – **High**: 20 MB/s to 70 MB/s. At this setting, data synchronization takes a short period of time. This value is used when the service load is relatively light. – **Highest**: Above 100 MB/s. At this setting, data synchronization takes a very short period of time. This value is used when the service load is light. – **Custom**: User-defined synchronization speed. The value ranges from 1 MB/s to 1024 MB/s.
Recovery Policy	Determines how data is synchronized after a fault is rectified. – **Automatic**: The system automatically synchronizes data. – **Manual**: Data must be synchronized manually.

Parameter	Description
Initial Sync	Initial synchronization mode of local and remote resources. When **Pair Creation** is set to **Automatic**, the value can be: – **Automatic**: The system automatically synchronizes data between the local and remote resources upon pair creation. – **Manual**: Data must be manually synchronized between local and remote resources. When **Pair Creation** is set to **Manual**, the value can be: – If data is inconsistent: ▪ **Automatic**: The system automatically synchronizes data between the local and remote resources upon pair creation. ▪ **Manual**: Data must be manually synchronized between local and remote resources. – If data is consistent, synchronization is not required.

NOTE

It is recommended that you perform synchronization tests for different speeds and select a proper speed based on the test result. Choose a faster speed as long as the bandwidth is sufficient.

Step 2 Configure mappings.

1. If the local LUN has been mapped, you only need to perform the following operations on DeviceManager of the remote storage system.
2. Choose **Services** > **Block Service** > **LUN Groups** > **LUNs**.
3. Select the desired LUNs and click **Map**.
4. Set the host and port group information.
5. Select **Advanced** in the upper right corner and set advanced parameters. **Table 11-2** describes the parameters.

Table 11-2 Advanced parameters for LUN mapping

Parameter	Description
Host LUN ID	Specifies how to assign host LUN IDs. – **Automatic**: The system assigns a host LUN ID to each LUN mapped to a host. – **Start ID**: Set a start ID ranging from 0 to 4095. The system assigns a host LUN ID to each LUN mapped to a host, starting from **Start ID**. – **Specified ID**: Manually assign a host LUN ID to each LUN mapped to a host.
Same Host LUN ID	Determines whether to keep host LUN IDs consistent. If you select this option, the system forcibly ensures that the host LUN IDs of the local and remote LUNs in the HyperMetro pairs are the same in the SAN HyperMetro scenario. In scenarios involving ESX hosts, if the host LUN IDs of the local and remote LUNs in the same HyperMetro pairs are different, data may be inconsistent.

Step 3 Verify the mappings.

1. Log in to a host as user **root**.
2. Run the **hot_add** command to scan for LUNs.
3. Run the **upadmin show vlun type=all** command to query the LUNs mapped to the host.

----End

Procedure for Creating a HyperMetro CG for a LUN Group

Step 1 Create a LUN group.

1. Log in to DeviceManager of the local storage system.
2. Choose **Services** > **Block Service** > **LUN Groups**.
3. Click **Create** and follow the wizard on DeviceManager to create a LUN group.

Step 2 Create a HyperMetro CG.

1. Select the created LUN group, click **Protect**, and select **Create HyperMetro**. The **Create HyperMetro CG** page is displayed.

NOTE

When you create a HyperMetro CG using a LUN group, the system first creates a PG for this LUN group. If you want to create a HyperMetro CG using a PG, choose **Data Protection** > **Protection Entities** > **Protection Groups** > **Protection Groups** and manually create a PG. Then create a HyperMetro CG for the PG.

2. Select a HyperMetro domain.
3. Set **Pair Creation** to **Automatic**.

NOTE

- If **Pair Creation** is set to **Automatic**, the system automatically creates remote LUNs and a remote LUN group on the remote storage system, and adds them to HyperMetro pairs and a CG. Ensure that no HyperMetro pair has been created for the LUNs in the LUN group. If remote LUNs or HyperMetro pairs already exist, create the CG manually to prevent configuration conflicts.
- If **Pair Creation** is set to **Manual**, you must manually select a LUN group on the remote storage system, which must contain the same number and capacities of LUNs as the local LUN group, and then manually match the LUNs. Ensure that the remote LUN group and its LUNs have not been mapped. If the LUN group or any LUN has been mapped, delete the mapping first to prevent configuration conflicts.

4. Select the target storage pool for creating remote resources of HyperMetro.
5. Set the service assurance policy of HyperMetro pairs. Possible options are:
   - **Service continuity preferred**

     The system preferentially ensures service continuity. It is used when host services require low storage latency. When the average write latency difference between local and remote resources of HyperMetro pairs is greater than **Isolation Threshold**, the system automatically disconnects the HyperMetro pairs and the resources with lower write latency continues providing services.

     When you select **Service continuity preferred**, set **Isolation Threshold (ms)**, which ranges from 10 to 30000.
   - **Data reliability preferred**

     The system ensures service data reliability preferentially. This value applies to scenarios that have high requirements for data protection. Data on local and remote resources is synchronized in real time.
6. (Optional) Select **Advanced** in the upper right corner and set the advanced parameters.

NOTE

By default, **Speed** is **Medium**, **Recovery Policy** is **Automatic**, and **Initial Sync** is **Automatic**.

Table 11-3 describes the parameters.

Table 11-3 HyperMetro CG advanced properties

Parameter	Description
Pair Sync Speed	Data synchronization speed of the HyperMetro CG. Possible values are: – **Low**: 0 MB/s to 5 MB/s. At this setting, data synchronization takes a long period of time. This value is used when the service load is heavy. – **Medium**: 10 MB/s to 20 MB/s. At this setting, data synchronization takes a relatively short period of time. This value is used when the service load is relatively heavy. – **High**: 20 MB/s to 70 MB/s. At this setting, data synchronization takes a short period of time. This value is used when the service load is relatively light. – **Highest**: Above 100 MB/s. At this setting, data synchronization takes a very short period of time. This value is used when the service load is light. – **Custom**: User-defined synchronization speed. The value ranges from 1 MB/s to 1024 MB/s.
Recovery Policy	Determines how data is synchronized after a fault is rectified. – **Automatic**: The system automatically synchronizes data. – **Manual**: Data must be synchronized manually.
Initial Sync	Initial synchronization mode of local and remote resources. When **Pair Creation** is set to **Automatic**, the value can be: – **Automatic**: The system automatically synchronizes data between the local and remote resources upon pair creation. – **Manual**: Data must be manually synchronized between local and remote resources. When **Pair Creation** is set to **Manual**, the value can be: – If data is inconsistent: ▪ **Automatic**: The system automatically synchronizes data between the local and remote resources upon pair creation. ▪ **Manual**: Data must be manually synchronized between local and remote resources. – If data is consistent, synchronization is not required.

NOTE

It is recommended that you perform synchronization tests for different speeds and select a proper speed based on the test result. Choose a faster speed as long as the bandwidth is sufficient.

7. Click **Next**.
8. Configure mappings.

NOTE

The LUNs at both ends of a HyperMetro pair must be mapped to the same host. You can enable **Map to Same Host or Host Group** to quickly create the mapping.

a. Enable **Map to Same Host or Host Group**.

NOTE

- If you do not enable **Map to Same Host or Host Group**, you must configure the mappings for the local and remote resources separately after configuring **Same Host LUN ID**.
- When LUNs are mapped to the same host or host group, the initiator information of the hosts to which the HyperMetro LUNs are mapped must be the same on the local and remote storage systems.
- If the local LUNs have been mapped to a host, you only need to set **Same Host LUN ID** and **Host Access Mode** after enabling **Map to Same Host or Host Group**. If you do not enable **Map to Same Host or Host Group**, you must configure the mapping for the remote resource after configuring **Same Host LUN ID**.

b. Select **Advanced** in the upper right corner and determine whether to select **Same Host LUN ID**. If you select this option, the system forcibly ensures that the host LUN IDs of the local and remote LUNs in the HyperMetro pairs are the same in the SAN HyperMetro scenario. In scenarios involving ESX hosts, if the host LUN IDs of the local and remote LUNs in the same HyperMetro pairs are different, data may be inconsistent.

c. Select a host or host group to which you want to map the LUNs.

NOTE

In no host or host group is available, click **Create** to create one.

d. (Optional) Select **Local Port Group**.

NOTE

After a port group is selected, LUNs in the LUN group use the ports of the port group to communicate with hosts in the host group. If no port group is selected, available ports are randomly used.

e. Set how to assign host LUN IDs.

- **Automatic**: The system assigns a host LUN ID to each LUN mapped to a host.
- **Start ID**: Set a start ID ranging from 0 to 4095. The system assigns a host LUN ID to each LUN mapped to a host, starting from **Start ID**.

- **Specified ID**: Manually assign a host LUN ID to each LUN mapped to a host.

NOTE

- If **Map to Same Host or Host Group** and **Same Host LUN ID** are disabled, you can set the host LUN ID allocation mode of the remote LUNs to **Automatic** or **Start ID**.
- If **Map to Same Host or Host Group** is disabled but **Same Host LUN ID** is enabled, you can set the host LUN ID allocation mode of the remote LUNs only to **Automatic**.

f. Specify **Host Access Mode**. Possible values are **Load balancing** or **Asymmetric**.

NOTE

Load balancing allows the host to access both storage systems with equal priority.

Asymmetric enables the host to preferentially access a specified storage system.

9. Follow the wizard to complete later operations.

----End

12 Check After Delivery

Check the items described in this section after HyperMetro has been configured.

Context

Table 12-1 lists the check items.

Table 12-1 Check items after delivery

Item	Criteria	Method
Both HyperMetro storage systems	Meets the requirements in **3.4 Storage Interconnection Rules**.	Use SmartKit to check the items.
Reserved space	Meets the requirements in **3.4 Storage Interconnection Rules**.	
HyperMetro replication links	Each controller has two or more replication links to the remote storage system.	
Quorum network	• The quorum network is properly connected. • The HyperMetro replication network and quorum network are on different network segments.	
HyperMetro replication ports and front-end ports connected to hosts	These ports are physically isolated.	

Item	Criteria	Method
HyperMetro LUN mapping	Both LUNs in the HyperMetro pair are mapped to the hosts in the two DCs.	
Fault domain	The active-active DCs and quorum site are in different fault domains.	Check these items manually.
Quorum server	UPS is configured for the quorum server and network devices.	

Prerequisites

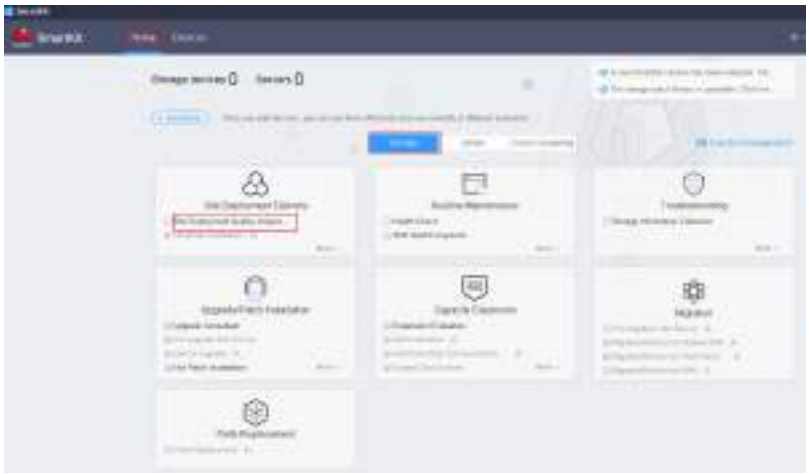
SmartKit is ready to use.

- For enterprise users, log in to **https://support.huawei.com/enterprise/** and choose **Tools** > **SmartKit**. Download and install the latest version.
- For carriers, log in to **https://support.huawei.com/carrier/**. On the home page, enter **SmartKit** in the search box and select the associated path to the SmartKit tool page. Download and install the latest version.

Procedure

Step 1 Use SmartKit to check the system. Rectify any defect according to the suggestions provided by SmartKit.

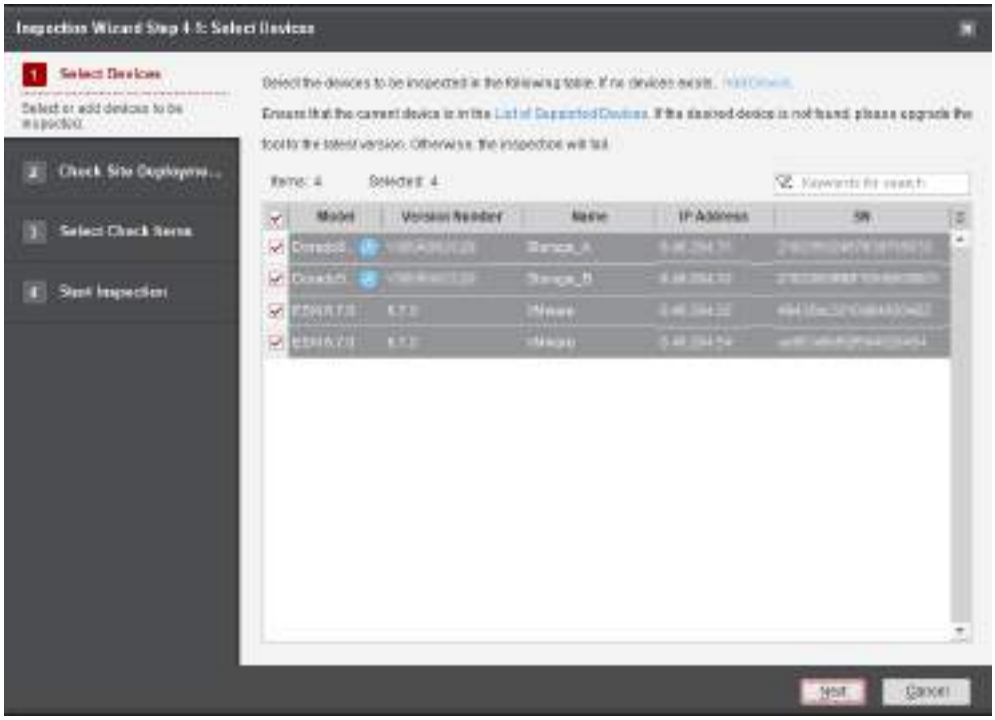
1. Log in to SmartKit.
2. Choose **Home** > **Storage** and click **Site Deployment Quality Inspection**.



3. Click **Device Selection**. On the **Select Devices** page that is displayed, click **Add Device**, add both storage systems to the device list, and click **OK**.
4. Click **Deployment Inspection**. On the **Select Devices** page that is displayed, click **Add Device** and add the hosts connected to the storage systems to the device list. Then click **Next**.

NOTE

- If HyperMetro is used on the storage systems, will be displayed on SmartKit.
- When adding devices by IP address, you can only add one device at a time. Then click **Add Device** again to add the next device.
- If not all hosts are added to SmartKit, the system asks you whether to add more hosts when you enter the **Confirm Manual Check Items** page. If you want to add more hosts, click **Previous**.



5. On the **Check Site Deployment Quality Standards** page, check the items manually according to the deployment quality criteria and import the check results. Click **Next**.
6. Set the check items for the hosts and storage systems at both DCs, and click **Next**.

   NOTE

   It is recommended that you retain the default check items.
7. Select a path for saving the inspection results and click **Next**.
8. SmartKit starts inspection.

   NOTE

   Some inspection items may take a long time.
9. After the inspection is complete, click **View the report** to view the inspection report. For the failed items, rectify the faults based on the suggestions.

Step 2 Manually check the system.

----End

13 Routine Management

This chapter describes the routine management on HyperMetro pairs, HyperMetro domains, quorum servers, and HyperMetro consistency groups (CGs).

13.1 Managing Protection Groups (System User)

This section describes how to manage protection groups (PGs)

13.1.1 Viewing PGs

This section describes how to view the information about PGs.

Context

- On the PG management page, click  to refresh the PG information.

- On the PG management page, click next to the parameter and enter the keyword to search for the desired PGs.
- On the PG management page, click and select PG information you want to view.

Procedure

Step 1 Choose **Data Protection** > **Protection Entities** > **Protection Groups** > **Protection Groups**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 In the function pane, view information about PGs. **Table 13-1** describes related parameters.

Table 13-1 PG parameters

Parameter	Description
Name	Name of the PG. **NOTE** You can click the name of a PG to view its brief information and manage its members and protection features.
ID	ID of a PG.
Owning vStore	Indicates the name of the vStore to which the protection group belongs. **NOTE** This parameter is available only when **vStore** is set to **All vStores** in **Step 2**.
vStore ID	Indicates the ID of the vStore to which the protection group belongs. **NOTE** This parameter is available only when **vStore** is set to **All vStores** in **Step 2**.
LUN Group	Name of a LUN group in a PG. **NOTE** If no LUN group exists in the PG, the LUN group is displayed as --.
LUNs	Number of LUNs in a PG. **NOTE** You can click the digit in this column to view and manage the LUNs.
Snapshot CGs	Number of snapshot CGs created for a PG. **NOTE** You can click the digit in this column to view and manage the snapshot CGs.

Parameter	Description
Clone CGs	Number of clone CGs created for a PG. **NOTE** You can click the digit in this column to view and manage the clone CGs.
HyperCDP CGs	Number of HyperCDP CGs created for a PG. **NOTE** You can click the digit in this column to view and manage the HyperCDP CGs.
Remote Replication CGs	Number of remote replication CGs created for a PG. **NOTE** You can click the digit in this column to view and manage the remote replication CGs.
HyperMetro CGs	Number of HyperMetro CGs created for a PG. **NOTE** You can click the digit in this column to view and manage the HyperMetro CGs.
DR Star Trios	Number of DR Star trios created for a PG. **NOTE** You can click the digit in this column to view and manage the DR Star trios.

Step 4 (Optional) Click the name of a PG to view its **Summary**, **Members**, and **Protection**.

----End

13.1.2 Modifying Attributes of a PG

This section describes how to modify the basic information of a PG.

Procedure

Step 1 Choose **Data Protection** > **Protection Entities** > **Protection Groups** > **Protection Groups**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Click **More** on the right of a PG and select **Modify**.

The **Modify PG** page is displayed on the right.

NOTE

You can also click the name of the desired PG. In the upper right corner of the page that is displayed, click **Operation** and then select **Modify** to modify the PG.

Step 4 Set the **Name** for the PG.

NOTE

- The name must be unique.
- The name contains letters, digits, underscores (_), periods (.), or hyphens (-).
- The name contains 1 to 255 characters.

Step 5 (Optional) Set the PG description.

NOTE

The description can be left blank or contain up to 255 characters.

Step 6 Click **OK**.

----End

13.1.3 Adding a LUN

This section describes how to add a LUN to a PG. After the operation, a HyperMetro pair is established between the new local and remote LUNs and added to the HyperMetro CG.

Prerequisites

The owning vStore of the new local LUN must be the same as that of other local LUNs in the HyperMetro CG. The owning vStore of the new remote LUN must be the same as that of other remote LUNs in the HyperMetro CG.

Procedure

Step 1 Go to the **Protection Groups** or **LUN Groups** page.

- If the members of the PG are LUN groups, choose **Services** > **Block Service** > **LUN Groups**.
- If the members of the PG are individual LUNs, choose **Data Protection** > **Protection Entities** > **Protection Groups**.

Step 2 Click **More** on the right of a PG and select **Add LUN**.

The **Add LUN** page is displayed on the right.

NOTE

Alternatively, perform any of the following operations to go to the **Add LUN** page:

- Click the name of the desired PG. In the upper right corner of the page that is displayed, select **Add LUN** from the **Operation** drop-down list.
- Click the name of the desired PG. On the page that is displayed, click the **Members** tab and then click **Add**.
- Click the value in the **LUNs** column of the desired PG if the value is not **0**. On the **Members** tab page, click **Add**.

Step 3 Add LUNs to the PG.

1. Add objects.
   a. In the **Available LUNs** area, select one or more LUNs.

b. Click **Next**.

2. Configure a HyperMetro pair.

a. In the **Pair Creation** area, set a pair creation mode.

NOTE

- If **Pair Creation** is set to **Automatic**, the system automatically creates remote LUNs on the remote storage system and adds them to a LUN group or PG, and then creates HyperMetro pairs and adds them to a CG. Ensure that no HyperMetro pair has been created for the selected LUNs. If remote LUNs or HyperMetro pairs already exist, create the CG manually to prevent configuration conflicts.
- If **Pair Creation** is set to **Manual**, you must manually select LUNs with the same capacity on the remote device. Ensure that the remote LUNs are not mapped and not added to another LUN group or PG. If a LUN has been mapped, unmap it first; if a LUN has been added to another LUN group or PG, remove it from the LUN group or PG first. Otherwise, configuration conflicts may occur.

b. If **Pair Creation** is set to **Automatic**, select a remote storage pool and select **Same as local** or **Custom** for **Remote Resource Name**. If **Pair Creation** is set to **Manual**, manually match the local and remote LUNs.

NOTE

If **Pair Creation** is set to **Automatic**, the prefix and suffix of a customized remote resource name must meet the following requirements:

- A prefix contains 0 to 32 characters, and a suffix contains 0 to 16 characters. The prefix and suffix cannot both be left blank.
- A prefix or suffix can contain only letters, digits, underscores (_), hyphens (-), and periods (.).
- If a local resource name is too long, the system automatically truncates it and uses the truncated local resource name and the specified prefix and suffix to create a remote resource.

c. Select or deselect **Run Later** as required.

NOTE

If this option is selected when you configure a HyperMetro pair, the system waits for the CG or the new pair to complete synchronization (if the CG or the new pair is synchronizing) and then add the new pair to the CG. If this option is not selected, the system suspends the CG and the new pair, adds the new pair to the CG, and then synchronizes the CG.

3. Click **Next**.

Step 4 Click **OK**.

----End

13.1.4 Removing a LUN

This section describes how to remove a LUN from a PG. After the operation, the HyperMetro pair of this LUN is removed from the HyperMetro CG.

Prerequisites

The members of the PG are LUNs.

NOTE

If the member of the PG is a LUN group, choose **Services** > **Block Service** > **LUN Groups** and remove LUNs from the LUN group. On the **Remove LUN** page, select or deselect **Remove LUN from Remote LUN Group** as required. If this option is selected, the system automatically removes the LUNs from the remote LUN group and delete the pairs. If this option is selected on neither the local nor the remote storage system, LUNs are removed from the LUN groups at both ends separately, but the HyperMetro pairs still exist in the CG. To remove the HyperMetro pairs, you must add the LUNs back and then remove the pairs.

Procedure

Step 1 Choose **Data Protection** > **Protection Entities** > **Protection Groups** > **Protection Groups**.

Step 2 Click **More** on the right of a PG and select **Remove LUN**.

The **Remove LUN** page is displayed on the right.

NOTE

Alternatively, perform any of the following operations to remove LUNs:

- Click the name of the desired PG. In the upper right corner of the page that is displayed, select **Remove LUN** from the **Operation** drop-down list.
- Click the name of the desired PG. On the page that is displayed, click the **Members** tab, select the desired LUNs, and click **Remove**.
- Click the value in the **LUNs** column of the desired PG if the value is not **0**. On the **Members** tab page, select the desired LUNs and click **Remove**.

Step 3 In the **Available LUNs** area, select one or more LUNs.

NOTE

Skip this step if you remove LUNs from the **Members** tab page.

Step 4 Select or deselect **Run Later** as required.

NOTE

Run Later is selected by default. If a CG or pair is synchronizing data, the system removes the pair from the CG after the synchronization is complete. If you deselect **Run Later** and the CG or pair is synchronizing data, the system suspends the CG or pair, removes the pair from the CG, and then synchronizes the CG.

Step 5 Click **OK**.

Confirm your operation as prompted.

----End

13.1.5 Splitting a PG

This section describes how to split a PG where HyperMetro or remote replication has been created.

Procedure

Step 1 Choose **Data Protection** > **Protection Entities** > **Protection Groups** > **Protection Groups**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Click **More** on the right of a PG and select **Split Protection**.

The **Split Protection** page is displayed on the right.

NOTE

You can also click the name of the desired PG. In the upper right corner of the page that is displayed, click **Operation** and then select **Split Protection** to split the PG.

Step 4 Set **Protection Type** of the PG.

- Remote Replication

  Set **Remote Replication CG**.
- HyperMetro

  Set **HyperMetro CG**.

Step 5 Set **New PG Name**.

Step 6 Click **OK**.

Confirm your operation as prompted.

NOTE

After the task is created successfully, the **Execution Result** page is displayed. You can view details about the current task on this page.

----End

13.1.6 Deleting a PG

This section describes how to delete unneeded PGs.

Prerequisites

- Services on a PG have been stopped and the LUN has not been configured with any value-added services.
- LUNs in a PG have been removed when the members of a PG are LUNs.

Procedure

Step 1 Choose **Data Protection** > **Protection Entities** > **Protection Groups** > **Protection Groups**.

Step 2 Select the desired vStore from the **vStore** drop-down list in the upper left corner.

Step 3 Click **More** on the right of a PG and select **Delete**.

Confirm your operation as prompted.

NOTE

You can also click the name of the desired PG. In the upper right corner of the page that is displayed, click **Operation** and then select **Delete** to delete the PG.

----End

13.2 Managing Block HyperMetro Domains (System User)

13.2.1 Modifying Attributes of a HyperMetro Domain for Block

This operation enables you to modify the configuration of a HyperMetro domain for block.

Procedure

Step 1 Choose **Data Protection** > **Configuration** > **HyperMetro Domains**.

Step 2 Click in the upper right corner of the desired HyperMetro domain for block and choose **Modify**.

The **Modify HyperMetro Domain** page is displayed on the right.

NOTE

Alternatively, click the name of the desired HyperMetro domain. In the upper right corner of the page that is displayed, select **Modify** from the **Operation** drop-down list.

Step 3 Specify the name and description for the HyperMetro domain.

NOTE

- The name must be unique.
- The name contains 1 to 31 characters.
- The name can contain only letters, digits, underscores (_), hyphens (-), and periods (.) and must start with a letter or digit.
- The description can be left blank or contain up to 127 characters.

Step 4 Determine whether to enable **Quorum Server**.

- If you enable **Quorum Server**:
  a. In the **Remote Device** area, select a remote device that you want to add to the HyperMetro domain.
  b. In the **Quorum Server** area, select a quorum server that you want to add to the HyperMetro domain.

     NOTE

     You can click + in the **Quorum Server** area to add another quorum server.

  c. You can click + to create a quorum server.

