

**OceanStor V3 Series**

**V300R006**

## **Administrator Guide**

**Issue      07**

**Date      2018-07-30**

HUAWEI TECHNOLOGIES CO., LTD.



**Copyright © Huawei Technologies Co., Ltd. 2018. All rights reserved.**

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

### **Trademarks and Permissions**



HUAWEI 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:      <http://e.huawei.com>

# About This Document

---

This document describes how to perform daily management and basic maintenance of the storage system.

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

Product Series	Product Model
OceanStor 2000 V3 series	OceanStor 2200 V3 <sup>a</sup> , 2600 V3, and 2600 V3 Video Surveillance Edition
OceanStor 5000 V3 series	OceanStor 5300 V3, 5500 V3, 5600 V3, and 5800 V3
OceanStor 6000 V3 series	OceanStor 6800 V3
OceanStor 18000 V3 series	OceanStor 18500 V3 and 18800 V3

a: OceanStor 2200 V3 (8 GB memory per controller) does not support the file system.

## 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 Conventions

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

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

## Change History

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

### Issue 07 (2018-07-30)

This issue is the seventh official release, which incorporates the following changes:

Optimized description about enabling and managing the Call Home service.

Added section **Migrating a Storage System AD Domain**.

### Issue 06 (2018-05-09)

This issue is the sixth official release, which incorporates the following changes:

Optimized description about enabling and managing the Call Home service.

Added section **Powering off a Disk Enclosure**.

### Issue 05 (2018-01-30)

This issue is the fifth official release, which incorporates the following changes:

Optimized description about enabling and managing the Call Home service.

### Issue 04 (2017-11-30)

This issue is the forth official release, which incorporates the following changes:

Added description about enabling and managing the Call Home service.

Optimized the documentation outline.

## **Issue 03 (2017-08-30)**

This issue is the third official release, which incorporates the following changes:

Optimized description about replacing DeviceManager licenses.

Optimized description about certificates and CA certificates in certificate management scenarios.

## **Issue 02 (2017-06-01)**

This issue is the second official release, which incorporates the following changes:

Added the user-defined role permission matrix.

Modified related description, and deleted content that is not applicable.

## **Issue 01 (2017-02-28)**

This issue is the first official release.

# Contents

---

<b>About This Document.....</b>	<b>ii</b>
<b>1 User Levels, Roles, and Permission.....</b>	<b>1</b>
<b>2 Common Management Software and Access Method.....</b>	<b>5</b>
2.1 Overview of Common Management Software.....	5
2.2 Logging In to the Storage System (OceanStor 2000, 5000, and 6000 Series).....	10
2.2.1 Logging In to DeviceManager (Through Web).....	10
2.2.2 Logging In to DeviceManager (Using a Tablet).....	12
2.2.3 Logging In to the CLI of the Storage System Using Username and Password.....	14
2.2.4 Logging In to the CLI of the Storage System Using a Public Key.....	21
2.3 Logging In to the Storage System (OceanStor 18000 Series).....	26
2.3.1 Logging In to DeviceManager (Through SVP).....	27
2.3.2 Logging In to DeviceManager (Through PC).....	30
2.3.3 Logging In to DeviceManager (Management Network Port).....	33
2.3.4 Logging In to DeviceManager (Using a Tablet).....	36
2.3.5 Logging In to the CLI of the Storage System (SVP's Management Network Port).....	37
2.3.6 Logging In to the CLI of the Storage System (Engine's Management Network Port).....	40
2.3.7 Logging In to the CLI of the Storage System (Public Key).....	43
2.4 Logging In to the Storage System O&M Software.....	48
2.4.1 Logging In to the eService Client.....	49
2.4.2 Logging In to the SmartKit.....	50
<b>3 Maintenance Item Overview.....</b>	<b>51</b>
<b>4 Routine Maintenance.....</b>	<b>54</b>
4.1 Inspection Using Tools.....	54
4.1.1 Inspecting a Storage Device.....	54
4.1.1.1 Inspection Using SmartKit.....	54
4.1.1.2 Inspection Using DeviceManager.....	56
4.1.2 Inspecting a Switch (OceanStor 2000, 5000, and 6000 Series) .....	57
4.2 Manual Inspection.....	60
4.2.1 Viewing and Handling Alarms.....	60
4.2.2 Checking the Operating Environment of the Storage Device.....	61
4.2.2.1 Check Method.....	61
4.2.2.2 Check Criteria.....	62

4.2.2.2.1 Temperature, Humidity, and Altitude (OceanStor 2000, 5000 and 6000 Series).....	63
4.2.2.2.2 Temperature and Humidity (OceanStor 18000 Series).....	64
4.2.2.2.3 Vibration and Shock (OceanStor 2000 Series).....	64
4.2.2.2.4 Vibration and Shock (OceanStor 5000 and 6000 Series).....	65
4.2.2.2.5 Vibration and Shock (OceanStor 18000 Series).....	65
4.2.2.2.6 Particle Contaminants.....	66
4.2.2.2.7 Corrosive Airborne Contaminants.....	67
4.2.2.2.8 Checking Racks.....	69
4.2.3 Checking Indicators.....	71
4.2.3.1 Check Method.....	71
4.2.3.2 Checking Controller Enclosure Indicators.....	71
4.2.3.2.1 Indicators on a 2 U Controller Enclosure (OceanStor 2600 V3 Video Surveillance Edition).....	71
4.2.3.2.2 Indicators on a 2 U Controller Enclosure (OceanStor 2000 Series).....	76
4.2.3.2.3 Indicators on a 2 U Controller Enclosure (OceanStor 5300 V3/5500 V3).....	82
4.2.3.2.4 Indicators on a 3 U Controller Enclosure.....	87
4.2.3.2.5 Indicators on a 6 U Controller Enclosure.....	93
4.2.3.3 Checking Disk Enclosure Indicators.....	98
4.2.3.3.1 Indicators on a 2 U Disk Enclosure.....	98
4.2.3.3.2 Indicators on a 4 U Disk Enclosure.....	101
4.2.3.3.3 Indicators on a High-Density Disk Enclosure.....	104
4.2.3.4 Checking Status of Indicators on an IP Switch.....	107
4.2.3.5 Checking Status of Indicators on a PCIe Switch.....	113
4.2.3.6 Checking the SVP Indicators (OceanStor 18000 Series).....	114
4.2.3.7 (Optional) Checking Quorum Server Indicators.....	116
4.2.4 Checking the Running Status of the Storage Device.....	121
4.2.4.1 Checking Controller Enclosures or Disk Enclosures.....	121
4.2.4.2 Checking Controllers.....	122
4.2.4.3 Checking Power Modules.....	123
4.2.4.4 Checking Controller Enclosure BBUs.....	124
4.2.4.5 Checking Fan Modules.....	125
4.2.4.6 Checking Hard Disks.....	126
4.2.4.7 Checking Host Ports.....	128
4.2.4.8 Checking Interface Modules.....	129
4.2.4.9 Checking Remote Devices.....	130
4.2.5 Checking the Running Status of Services.....	131
4.2.5.1 Checking Disk Domains.....	131
4.2.5.2 Checking Storage Pools.....	132
4.2.5.3 Checking LUNs.....	133
4.2.5.4 Checking Host Status.....	134
4.2.5.5 Viewing Mapping Status.....	135
4.2.5.6 Checking Remote Replication Tasks.....	135
4.2.5.7 Checking Consistency Groups.....	136

4.2.5.8 Checking Clone Tasks.....	138
4.2.5.9 Checking Snapshot Tasks.....	139
4.2.5.10 Checking LUN Copy Tasks.....	140
4.2.5.11 Checking HyperMirror Status.....	141
4.2.5.12 Checking File System Status.....	142
4.2.5.13 Checking Optimization Feature Status.....	143
4.3 Collecting Storage System Information.....	144
4.3.1 Types of Information to Be Collected.....	145
4.3.2 Collecting Information on DeviceManager.....	146
4.3.2.1 Exporting System Data.....	146
4.3.2.2 Exporting Alarms and Events.....	149
4.3.3 Collecting Information in the CLI.....	150
4.3.3.1 Exporting Storage System Configuration Data.....	150
4.3.3.2 Importing Storage System Configuration Data.....	152
4.3.4 Collecting Information Using SmartKit.....	153
4.3.4.1 Exporting System Data.....	153
4.3.4.2 Collecting Device Archive Information.....	154
4.3.4.3 Collecting Host Information.....	155
4.3.4.4 Analyzing Log Files Using SmartKit.....	156
4.3.5 Using a Script File to Collect Logs (OceanStor 18000 Series).....	156
4.3.5.1 Using a Script File to Collect System Logs.....	157
4.3.5.2 Using a Script File to Collect Windows System Logs.....	157
<b>5 Routine Management.....</b>	<b>159</b>
5.1 Powering on or off the Storage Device (OceanStor 2000, 5000, and 6000 Series).....	159
5.1.1 Powering on a Device.....	159
5.1.2 Powering off the Storage Device.....	161
5.1.3 Restarting the Storage Device.....	162
5.1.4 Powering off the Storage Device upon an Emergency.....	162
5.1.5 Re-Powering on the Storage Device After an Emergency Power-off.....	163
5.1.6 Powering on an Interface Module.....	163
5.1.7 Powering off an Interface Module.....	163
5.1.8 Powering off a Disk Enclosure (Applicable to V300R006C20 and later).....	164
5.2 Powering on or off the Storage Device (OceanStor 18000 Series).....	165
5.2.1 Powering on the Storage Device.....	165
5.2.2 Powering off the Storage System.....	174
5.2.3 Restarting the Storage Device.....	181
5.2.4 Restarting the SVP.....	182
5.2.5 Powering off the Storage Device upon an Emergency.....	182
5.2.6 Re-Powering on the Storage Device After an Emergency Power-off.....	183
5.2.7 Powering on an Interface Module.....	183
5.2.8 Powering off an Interface Module.....	183
5.2.9 Powering off a Disk Enclosure (Applicable to V300R006C20 and later).....	184

5.3 Managing Access Permission of a Storage System.....	185
5.3.1 Configuring a Security Policy for System User.....	185
5.3.2 Configuring Authorized IP Addresses.....	191
5.3.3 Managing Users and Their Access Permissions.....	192
5.3.3.1 Creating a Local User.....	192
5.3.3.2 Creating a Domain User.....	195
5.3.3.3 Managing User Levels.....	197
5.3.3.4 Customizing User Roles.....	199
5.3.3.5 Locking or Unlocking a User.....	201
5.3.3.6 Logging Out a User.....	202
5.3.3.7 Changing Password.....	203
5.3.3.8 Resetting the Password of an Administrator or a Read-Only User.....	204
5.3.3.9 Resetting the Password of a Super Administrator.....	206
5.3.3.10 Setting User Passwords to Never Expire.....	206
5.3.3.11 Removing a User.....	208
5.3.4 Migrating a Storage System AD Domain (Applicable to V300R006C30).....	209
5.4 Managing Alarm Notifications.....	210
5.4.1 Managing Email Notification.....	210
5.4.1.1 Adding a Backup SMTP Server.....	211
5.4.1.2 Managing Recipient Email Addresses.....	214
5.4.2 Managing SMS Notification.....	215
5.4.2.1 Managing Recipient Mobile Phone Numbers.....	215
5.4.2.2 Configuring the GSM Modem (OceanStor 2000, 5000, and 6000 Series).....	217
5.4.2.3 Configuring the GSM Modem (OceanStor 18000 Series).....	220
5.4.3 Managing Syslog Notification.....	223
5.4.3.1 Modifying the Syslog Notification Policy.....	223
5.4.3.2 Managing the Receiver Server Addresses of Syslog Notifications.....	224
5.4.4 Managing Trap Notification.....	227
5.4.4.1 Managing SNMP Community Strings.....	227
5.4.4.2 Managing USM Users.....	228
5.4.4.3 Managing Trap Server Addresses.....	232
5.4.5 Managing Alarm Dump.....	248
5.4.5.1 Configuring an FTP Server.....	248
5.4.5.2 Modifying Alarm Dump Settings.....	249
5.4.6 Configuring Alarm Masking.....	253
5.5 Enabling and Managing the Call Home Service (Applicable to V300R006C10 and later).....	255
5.5.1 About the Call Home Service.....	255
5.5.2 Configuring the Call Home Service.....	257
5.5.2.1 Configuration Process.....	257
5.5.2.2 Preparations.....	258
5.5.2.3 Obtaining Authorization from Customers.....	259
5.5.2.4 Registering with eService.....	259

5.5.2.5 Configuring the DNS Service.....	260
5.5.2.6 Enabling the Call Home Service.....	261
5.5.3 Exporting a Data Package to Be Uploaded.....	266
5.6 Monitoring Storage System Performance.....	268
5.7 Managing Basic Information About a Storage System.....	268
5.7.1 Setting the Device Time.....	268
5.7.2 Setting the Device Name and Location.....	270
5.8 Managing License Files.....	270
5.8.1 Viewing an Activated License File.....	271
5.8.2 Backing Up an Active License File.....	271
5.9 Reclaiming Space of a Storage System.....	272
5.9.1 Process for Reclaiming Space of a Storage System.....	272
5.9.2 Reclaiming Space of a Storage System (Windows).....	274
5.9.2.1 Preparing for Space Reclamation (Windows).....	274
5.9.2.2 Reclaiming Space (Windows).....	276
5.9.3 Reclaiming Space of a Storage System (Linux).....	279
5.9.3.1 Preparing for Space Reclamation (Linux).....	279
5.9.3.2 Reclaiming Space (Linux).....	280
5.9.4 Reclaiming Space of a Storage System (AIX).....	283
5.9.4.1 Preparing for Space Reclamation (AIX).....	283
5.9.4.2 Reclaiming Space (AIX).....	284
5.9.5 Reclaiming Space of a Storage System (HP-UX).....	287
5.9.5.1 Preparing for Space Reclamation (HP-UX).....	287
5.9.5.2 Reclaiming Space (HP-UX).....	288
5.9.6 Emergency Rollback of Space Reclamation.....	291
5.9.7 Disk Data Destruction.....	293
5.10 Obtaining System Version Information.....	293
5.10.1 Obtaining Current System Version Information.....	293
5.10.2 Obtaining System Historical Version Information.....	295
5.11 Interconnecting Storage Devices with a Third-Party NMS.....	295
5.12 Connection Change Between the Storage System and an Application Server.....	297
5.12.1 Configurations and Operations After an HBA Replacement (in Windows).....	298
5.12.1.1 Preparing for Configuration (in Windows).....	298
5.12.1.2 Configurations and Operations (in Windows).....	300
5.12.2 Configurations and Operations After an HBA Replacement (in Linux).....	301
5.12.2.1 Preparing for Configuration (in Linux).....	302
5.12.2.2 Configurations and Operations (in Linux).....	303
5.12.3 Configurations and Operations After an HBA Replacement (in AIX).....	304
5.12.3.1 Preparing for Configuration (in AIX).....	304
5.12.3.2 Configurations and Operations (in AIX).....	306
5.12.4 Configurations and Operations After an HBA Replacement (in HP-UX).....	307
5.12.4.1 Preparing for Configuration (in HP-UX).....	307

5.12.4.2 Configurations and Operations (in HP-UX).....	309
5.12.5 Emergency Rollback of Configurations and Operations After Replacing an HBA.....	310
5.13 Managing VMs (OceanStor 18000 Series).....	311
5.13.1 Querying VM Status.....	311
5.13.2 Restarting a VM.....	312
5.13.3 Closing a VM.....	313
5.13.4 Forcibly Closing a VM.....	314
5.13.5 Redefining a VM.....	314
5.13.6 Starting a VM.....	315
5.13.7 Logging In to the Linux VM of the SVP Using VNC.....	316
5.14 Expanding Storage Space.....	317
5.14.1 Performing the Pre-expansion Evaluation.....	317
5.14.2 Expanding LUN Capacity.....	319
5.14.2.1 Understanding the Expansion Process.....	320
5.14.2.2 Performing the Pre-expansion Check.....	321
5.14.2.3 Locating a LUN to Be Expanded.....	323
5.14.2.4 Expanding a LUN on the Storage System.....	324
5.14.2.5 Expanding Storage Space for an Application Server.....	327
5.14.2.5.1 Expanding a LUN on an Application Server in Windows.....	327
5.14.2.5.2 Expanding a LUN on an Application Server in SUSE.....	331
5.14.2.5.3 Using LVM to Expand a LUN in SUSE.....	332
5.14.2.5.4 Expanding a LUN on an Application Server in Red Hat.....	334
5.14.2.5.5 Expanding a LUN on an Application Server in Solaris.....	335
5.14.2.5.6 Expanding a LUN on an Application Server in AIX.....	338
5.14.2.5.7 Expanding a LUN on an Application Server in HP-UX.....	343
5.14.2.5.8 Expanding a LUN on an Application Server in VMware ESX.....	344
5.14.2.5.9 Expanding a LUN on an Application Server in Hyper-V.....	350
5.14.2.5.10 Expanding a LUN on an Application Server in FusionCompute.....	358
5.14.3 Adding LUNs for Storage Space Expansion.....	360
5.14.3.1 Adding LUNs at the Storage Side.....	360
5.14.3.2 Adding LUNs at the Application Server Side.....	362
5.14.3.2.1 Adding LUNs at the Application Server Side (in Windows).....	362
5.14.3.2.2 Adding LUNs at the Application Server Side (in SUSE).....	367
5.14.3.2.3 Adding LUNs at the Application Server Side (in AIX).....	369
5.14.4 Expanding a File System.....	370
5.14.5 Shrinking a File System.....	375
5.14.6 Emergency Rollback Procedure.....	379
5.14.6.1 Emergency Rollback Procedure (in Windows).....	379
5.14.6.2 Emergency Rollback Procedure (in Linux).....	381
5.14.6.3 Emergency Rollback Procedure (in AIX).....	382
5.14.6.4 Emergency Rollback Procedure (in HP-UX).....	383
<b>6 FAQ.....</b>	<b>385</b>

6.1 How Do I Query the Mapping Between Host Disks and LUNs When the UltraPath Software Is Not Installed?.....	385
6.2 How Can I Modify the Outdated Password for Default User Maintainer of the SVP's Windows VM?.....	389
6.3 How Can I Expand the Capacity of a LUN Used in the HyperMetro Feature? (Applicable to V300R006C00/C10).....	391
6.4 How Can I Expand the Capacity of a LUN Used in the HyperMetro Feature? (Applicable to V300R006C20 and Later). .....	393
6.5 How Can I Expand the Capacity of a LUN Used in a Remote Replication Pair? (Applicable to V300R006C00/C10).....	393
6.6 How Can I Expand the Capacity of a LUN Used in a Remote Replication Pair? (Applicable to V300R006C20 and Later). .....	394
6.7 How Can I Use Self-Signed Certificates to Fix the Privacy Error Displayed When I Attempt to Log In to DeviceManager?.....	395
<b>A Permission Matrix for Self-defined Roles (Applicable to V300R006C20 and Earlier Versions).....</b>	<b>400</b>
<b>B Permission Matrix for Self-defined Roles (Applicable to V300R006C30). .....</b>	<b>410</b>
<b>C How to Obtain Help.....</b>	<b>420</b>
C.1 Preparations for Contacting Huawei.....	420
C.1.1 Collecting Troubleshooting Information.....	420
C.1.2 Making Debugging Preparations.....	420
C.2 How to Use the Document.....	420
C.3 How to Obtain Help from Website.....	421
C.4 Ways to Contact Huawei.....	421
<b>D Glossary.....</b>	<b>422</b>
<b>E Acronyms and Abbreviations.....</b>	<b>423</b>

# 1 User Levels, Roles, and Permission

To prevent misoperations from compromising the storage system stability and service data security, the storage system defines user levels and roles to determine user permission and scope of permission. Before using this document, check the level and role of your account to know your permission.

## Definition of User Levels and Roles

- **Level:** determines whether a user has operation or access permission.  
The storage system defines three user levels, as described in [Table 1-1](#).

**Table 1-1** User levels

Level	Description
Super administrator	A super administrator has full administrative permissions on the storage device, and is able to create users of all levels.
Administrator	An administrator user has partial administrative permissions on the storage device but cannot manage users, upgrade the storage device, modify the system time, restart the device, or power off the device.
Read-only user	A read-only user has only the access permission on the storage device. After logging in to the storage device, read-only users can only query information about the storage device.



The storage system supports a maximum of 32 system users, among which a maximum of two super administrators can be created.

- **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. [Table 1-2](#) describes the built-in roles in detail.

- User-defined roles allow users to configure the scope of permission as required. For user-defined roles, see [A Permission Matrix for Self-defined Roles \(Applicable to V300R006C20 and Earlier Versions\)](#) and [B Permission Matrix for Self-defined Roles \(Applicable to V300R006C30\)](#).

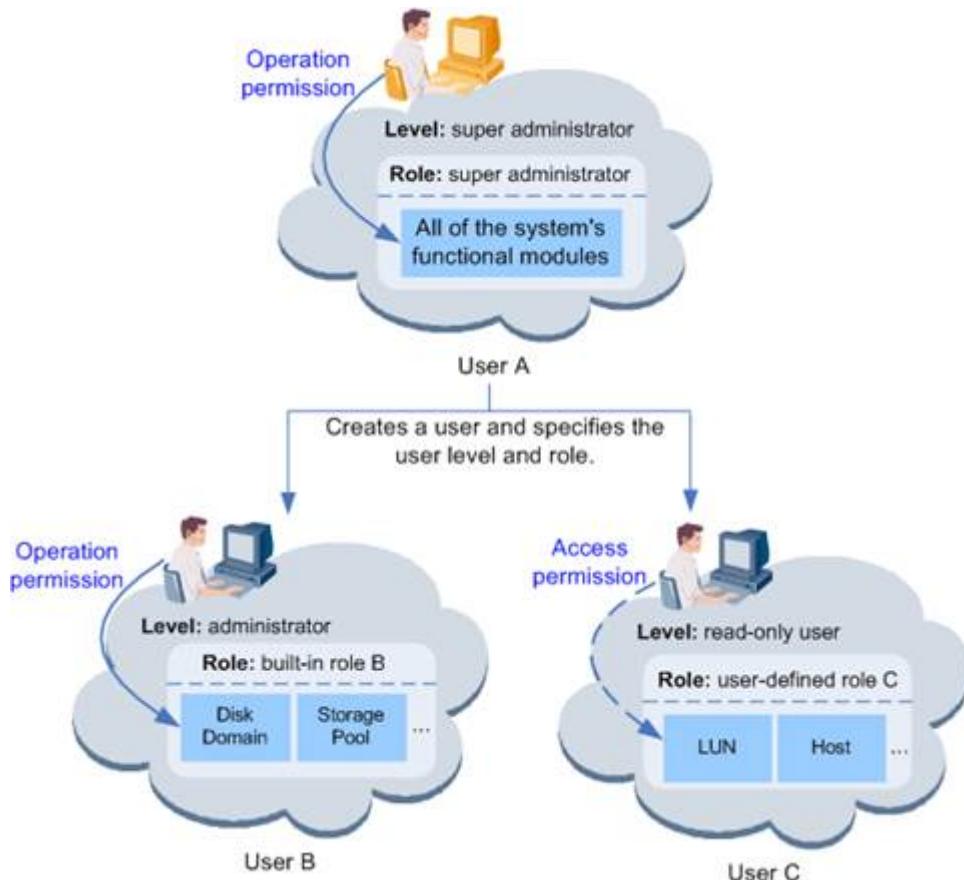
To support permission control in vStore scenarios, the storage system divides the built-in roles into the system group and vStore group.

- vStore group: The roles are used only when the user logs in to DeviceManager using a vStore account.
- System group: The roles are used only when the user logs in to DeviceManager using a system account.

**Table 1-2** Built-in roles

Built-in Role	Function Group	Scope of Permission
Super administrator	System group	All permissions over the system
Administrator	System group	All permissions except user management and security configuration
Security administrator	System group	Permission for managing system security configurations, including security rules, certificates, audit, KMC, antivirus software, data destruction, and compliance clocks
Network administrator	System group	Permission for managing system network resources, including physical ports, logical ports, VLANs, and failover groups
SAN resource administrator	System group	Permission for managing SAN resources, including storage pools, LUNs, mapping views, hosts, and ports
NAS resource administrator <sup>a</sup>	System group	Permission for managing NAS resources, including storage pools, file systems, file servers, authenticated users, networks, quota trees, and shares
Data protection administrator	System group	Permission for managing data protection, including local data protection, remote data protection, and HyperMetro data protection
Backup administrator	System group	Permission for managing data backup, including local data and mapping views
vStore administrator	vStore group	All vStore management permissions
vStore data protection administrator	vStore group	Permission for managing vStore data protection, including local data protection, remote data protection, and HyperMetro data protection for vStores

Built-in Role	Function Group	Scope of Permission
vStore protocol administrator	vStore group	Permission for managing vStore protocols, including authenticated users and shares of vStores
a: The OceanStor 2600 V3 video surveillance edition storage system does not support this role.		

**Figure 1-1** User roles and permission

## Querying the Current User's Permission

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

### Procedure

1. Log in to DeviceManager.
2. Choose **Settings > Permission Settings > User Management**.

3. Query the current user's **Level** and **Role** in the middle pane and determine the user permission and scope according to [Table 1-1, Table 1-2, A Permission Matrix for Self-defined Roles \(Applicable to V300R006C20 and Earlier Versions\)](#), and [B Permission Matrix for Self-defined Roles \(Applicable to V300R006C30\)](#).

 **NOTE**

- Super administrators can view the information about all users on the device.
- Administrators or read-only users can only view their own information.

For example, in [Figure 1-2](#), the role and level of the **safe\_admin\_reader** user are **Security administrator** and **Read-only user**, respectively. According to [Table 1-1](#) and [Table 1-2](#), the user has the permission to query the security rules, certificates, audits, KMC, antivirus function, data destruction function, and compliance clock. To modify the user level and role, see [5.3.3.3 Managing User Levels](#) and [5.3.3.4 Customizing User Roles](#).

**Figure 1-2** Information of the current user



Current user: safe_admin_reader(Read-only user)					
Username	Level	Type	Online/Offline	Password Status	Role
safe_admin_reader	Read-only user	Local user	Online	Normal	Security administrator

# 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](#)
- [2.2 Logging In to the Storage System \(OceanStor 2000, 5000, and 6000 Series\)](#)
- [2.3 Logging In to the Storage System \(OceanStor 18000 Series\)](#)
- [2.4 Logging In to the Storage System O&M Software](#)

## 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 (formerly named Toolkit, which is used as an example in this document) and eService, to improve the maintenance efficiency.

**Table 2-1** describes software commonly used to manage storage systems.

**Table 2-1** Common management software

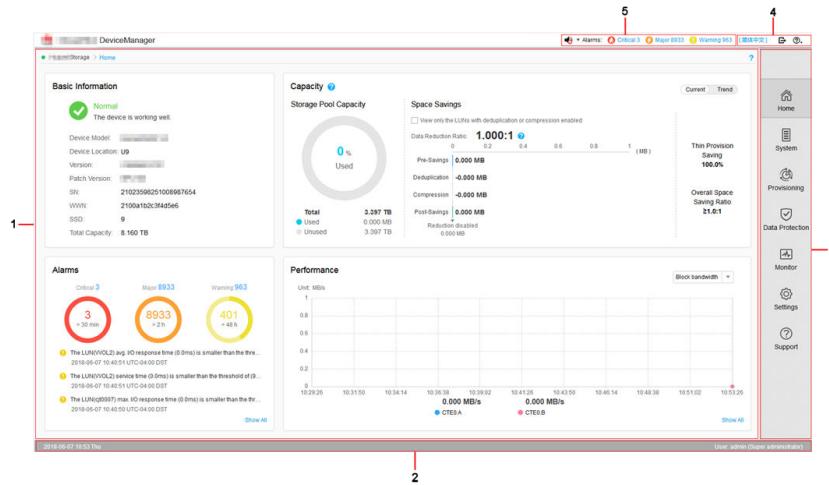
Management Software	Function
DeviceManager	Helps you to allocate storage resources, manage users, data protection features, and alarms, and monitor device performance.
CLI	Helps you to allocate storage resources, manage users, data protection features, and alarms, and monitor device performance.
SmartKit	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** shows the DeviceManager main window.

**Figure 2-1** DeviceManager main window



**Table 2-2** describes the components of the DeviceManager main window.

**Table 2-2** Components of the DeviceManager main window

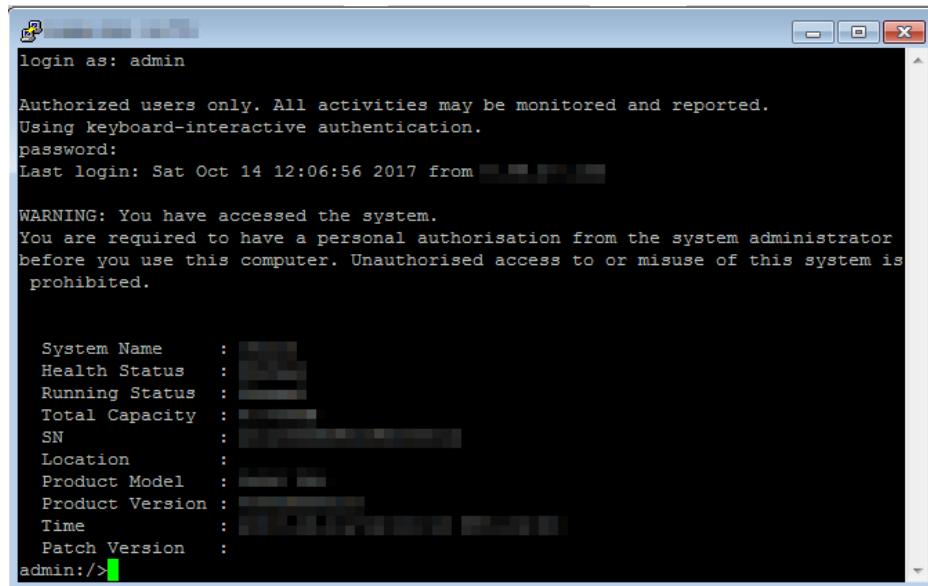
No.	Name	Description
1	Function pane	The function pane shows a page associated with the current operation.
2	Status bar	The status bar shows information such as the user name currently logged in and the login time.
3	Navigation bar	The navigation bar shows the function modules of a storage system. Users can click a function module to configure the corresponding functions.

No.	Name	Description
4	Exit, help, and language selection area	This area displays an exit button, a help button, and a language selection button. DeviceManager supports simplified Chinese and English.
5	Fault statistics area	The fault statistics area shows the number of each level of system faults, helping users understand the running status of a storage system.

## 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 2-2](#) shows the CLI main window.

[Figure 2-2](#) CLI main window

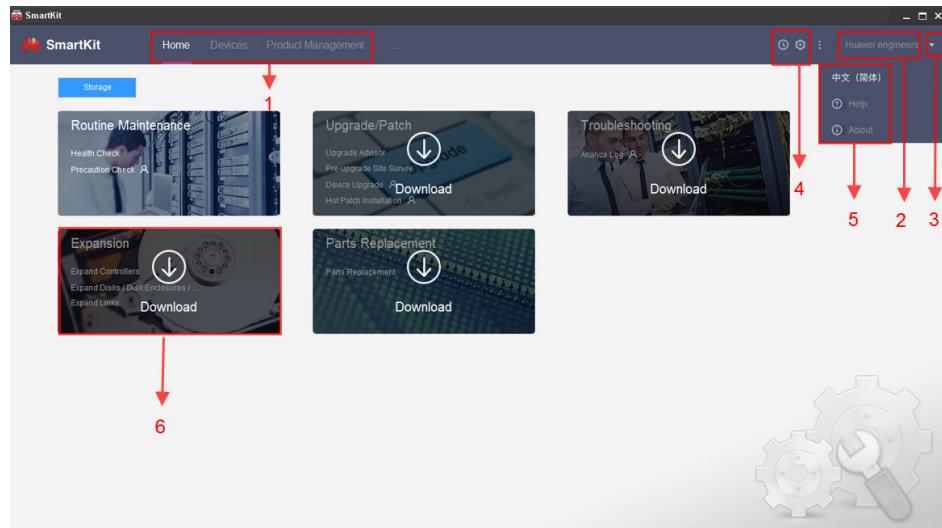


After logging in to CLI, you can view information about a storage system, including the system name, health status, running status, and total capacity.

## 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.

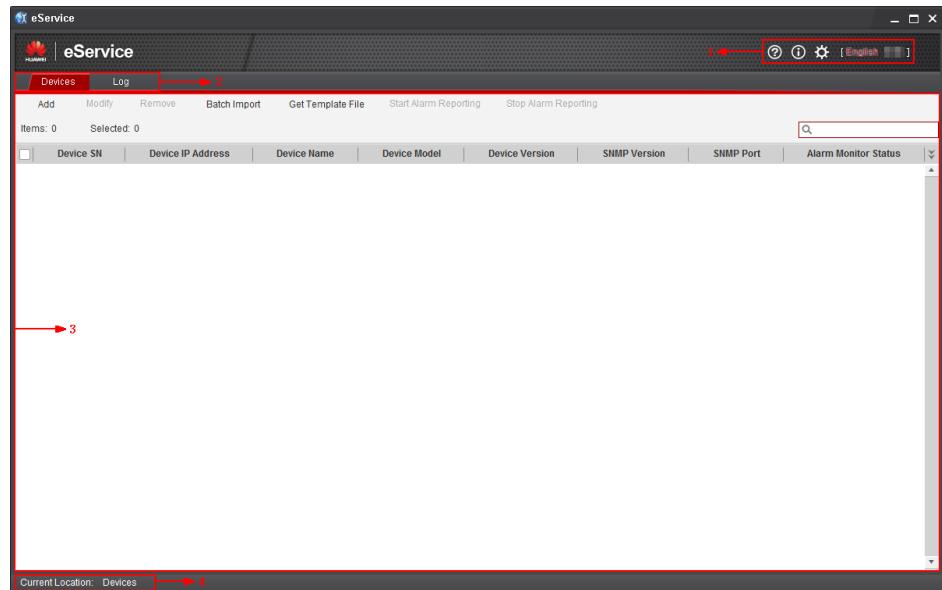
[Figure 2-3](#) shows the SmartKit main window.

**Figure 2-3** SmartKit main window**Table 2-3** describes the components of the SmartKit main window.**Table 2-3** Components of the SmartKit main window

No.	Name
1	Navigation tree: Enables you to select functions.
2	SmartKit account: Enables you to switch between accounts.
3	Exit: Enables the current user to exit when you click this button.
4	Buttons for scheduling tasks and configuring the system.
5	Buttons for obtaining online help and more information as well as selecting a language.
6	Sub-function portal: Enables you to use the corresponding tools.

## Introduction to eService

eService is a professional tool that supports alarm reporting, file uploading, and remote access. After being installed, eService can report alarms on the connected storage system to the Huawei technical support center as prescribed by the alarm policy. Then, Huawei maintenance personnel will work out troubleshooting measures based on the alarm severities and handling difficulties, improving the alarm handling efficiency and saving the customer's time and manpower. **Figure 2-4** shows the eService main window.

**Figure 2-4** eService main window

**Table 2-4** describes the components of the eService main window.

**Table 2-4** Components of the eService main window

No.	Name	Description
1	Settings and help area	<ul style="list-style-type: none"><li>This function enables you to manage device information by setting customer information, mailboxes, log dumping, and automatic eService startup. The alarm information will be sent to maintenance personnel to locate faults, facilitating real-time troubleshooting.</li><li>By clicking these buttons, you can view help documents and eService copyright and select a desired language.</li></ul>
2	Menu bar	<ul style="list-style-type: none"><li><b>Devices</b> You can add, modify, and remove devices, and manage reported alarms of existing devices. Adding devices in batches is supported.</li><li><b>Log</b> This function allows you to manage operation logs and run logs of devices to know device status in real time.</li></ul>
3	Function pane	The function pane displays all function modules of eService.
4	Status bar	The status bar shows where the current operation is located.

## 2.2 Logging In to the Storage System (OceanStor 2000, 5000, and 6000 Series)

You can log in to the storage system using either DeviceManager or CLI to configure, manage, and maintain the system.

### 2.2.1 Logging In to DeviceManager (Through Web)

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

#### Prerequisites

- Operating system and browser versions of the maintenance terminal.  
DeviceManager supports multiple operating systems and browsers. You can query the compatibility using the [OceanStor Interoperability Navigator](#).
- The maintenance terminal communicates with the storage system properly.
- The super administrator can log in to the storage system using the **Local user** authentication mode only.
- To use a Lightweight Directory Access Protocol (LDAP) domain user account to log in to DeviceManager, you must configure the LDAP server first, set the LDAP server parameters, and then create an LDAP user account on DeviceManager. [5.3.3.2 Creating a Domain User](#) details the configuration methods.
- By default, DeviceManager allows 32 users to log in concurrently.

#### Context

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

##### NOTE

The super administrator can run `change devicemanager tls min_version=?` to change the earliest version of TLS supported by DeviceManager. Then, the super administrator must run `reboot storage service service_name=devicemanager` to restart DeviceManager for the change to take effect.

- For a 2 U controller enclosure, the default IP addresses of the management network ports on controllers A and B are respectively **192.168.128.101** and **192.168.128.102**, and the default subnet mask is **255.255.0.0**. For a 3 U or 6 U controller enclosure, the default IP addresses of the management network ports on management modules 0 and 1 are respectively **192.168.128.101** and **192.168.128.102**, and the default subnet mask is **255.255.0.0**.
- The default user name and password of the super administrator are **admin** and **Admin@storage**.
- This document uses the Windows operating system as an example to explain how to log in to DeviceManager. The login operations on other operating systems need to be adjusted accordingly.
- If a user does not perform any operations after logging in to the system for a period longer than the timeout limit (the limit is 30 minutes by default and modifiable), the system logs out automatically.

- If an account is not used to log in to the system for a certain period of time (the period is 60 days by default and modifiable), it will be locked and can only be unlocked by the super administrator.

## Procedure

**Step 1** Run Internet Explorer on the maintenance terminal.

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

 **NOTE**

- **XXX.XXX.XXX.XXX** represents the management network port IP address of the storage system.
- In an environment with the firewall function, when the system externally provides web services, you need to enable port 8088.
- Your web browser may show that the website has a privacy error. If the IP address is correct, you can neglect the prompt and continue to access the storage system. If you want to fix this error, you can have the certificate request file signed by a third-party CA center or by your own CA certificates. For details about the method using your own CA certificates, see [6.7 How Can I Use Self-Signed Certificates to Fix the Privacy Error Displayed When I Attempt to Log In to DeviceManager?](#)
- If you have a usable security certificate, you are advised to use corresponding commands to import the certificate to improve system security. For details about the corresponding commands, see [Command Reference](#).

**Step 3** (Optional) Set the authentication mode and language. DeviceManager supports simplified Chinese and English.

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

 **NOTE**

- The super administrator can log in to the storage system using the **Local user** authentication mode only.
- LDAP user: You will log in to the storage system in LDAP domain authentication mode.  
You can log in to the storage system in LDAP domain authentication mode only after the LDAP server is properly configured.

3. Choose a language from the **Language** list.  
DeviceManager supports simplified Chinese and English.

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

 **NOTE**

- If you enter wrong passwords for consecutive two times, you need to enter the verification code. In **Verification Code**, enter the verification code.
- If **LDAP user** is selected, the username and password must be a domain username and password. If you want to log in as the super administrator, the default user name and password are **admin** and **Admin@storage** respectively.
- If you forget the password of an administrator or a read-only user, contact the super administrator to reset the password. If you forget the password as the super administrator (**admin** by default), contact super administrator **\_super\_admin** to log in to the CLI through a serial port and run **initpasswd** to reset the password. For details, see [5.3.3.8 Resetting the Password of an Administrator or a Read-Only User](#) and [5.3.3.9 Resetting the Password of a Super Administrator](#).
- If you enter incorrect passwords a specified number of times (equal to the value specified in **Number of Incorrect Passwords** on the **Login Policy** page), the account is automatically locked for the period of lock time (The lock period of the super administrator is 15 minutes, and the lock period of other users is 15 minutes by default).
- You must change the default login password immediately when you are logging in to the storage system for the first time and periodically change your login password in the future. This reduces the password leakage risks. For details about how to change the password, see [5.3.3.7 Changing Password](#).

**Step 5 Click Log In.**

The DeviceManager main window is displayed.

 **NOTE**

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

----End

## 2.2.2 Logging In to DeviceManager (Using a Tablet)

You can use a tablet to log in to a storage system and conduct basic maintenance operations, such as checking alarms, performance statistics, and the basic information of the storage system.

### Prerequisites

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

### Context

- DeviceManager only supports TSL protocols (including TLS 1.0, TLS 1.1, and TLS 1.2).
- Customers can use a tablet to log in to the storage system through their wireless routers. You can use iPad Air (Safari) and HUAWEI MediaPad 10 FHD (Chrome) to log in to the storage system. This section uses iPad as an example to describe how to log in to DeviceManager. The login operations on other operating systems are similar.
- For a 2 U controller enclosure, the default IP addresses of the management network ports on controllers A and B are respectively **192.168.128.101** and **192.168.128.102**, and the default subnet mask is **255.255.0.0**. For a 3 U or 6 U controller enclosure, the default IP addresses of the management network ports on management modules 0 and 1 are

respectively **192.168.128.101** and **192.168.128.102**, and the default subnet mask is **255.255.0.0**.

- The default user name and password of the super administrator are **admin** and **Admin@storage**.
- By default, DeviceManager allows 32 users to log in concurrently.
- If a user does not perform any operations after logging in to the system for a period longer than the timeout limit (the limit is 30 minutes by default and modifiable), the system logs out automatically.
- If an account is not used to log in to the system for a certain period of time (the period is 60 days by default and modifiable), it will be locked and can only be unlocked by the super administrator.

## Procedure

### Step 1 Connect the iPad to the Wi-Fi network.

1. On the iPad desktop, choose **Settings > WLAN**.  
The system goes to the **WLAN** page.
2. In the **CHOOSE A NETWORK** area, choose the Wi-Fi network.  
The **Enter Password** page is displayed.
3. In the **Password** text box, enter the password.
4. Click **Join**.  
The iPad is connected the Wi-Fi network.

### Step 2 Log in to DeviceManager.

1. On the iPad desktop, tap **Safari**.
2. Set **Address** to **https://xxx.xxx.xxx.xxx:8088/ismpad/login.html** and click **Go**.  
**xxx.xxx.xxx.xxx** is the IP address of management port on the storage system.  
The DeviceManager login page is displayed.
3. (Optional) Select a language from the **Language** check box.
4. In **User Name** and **Password**, enter the user name and password.

#### NOTE

- The default user name and password are **admin** and **Admin@storage**.
- If a verification code is required, enter the **verification code**.
- If you forget the password of an administrator or a read-only user, contact the super administrator to reset the password. If you forget the password as the super administrator (**admin** by default), contact super administrator **\_super\_admin** to log in to the CLI through a serial port and run **initpasswd** to reset the password. For details, see [5.3.3.8 Resetting the Password of an Administrator or a Read-Only User](#) and [5.3.3.9 Resetting the Password of a Super Administrator](#).
- Change the default login password immediately after you have logged in to the storage system for the first time. Periodically change your login password. For details about how to change the password, see [5.3.3.7 Changing Password](#).

5. Click **Login**.

The system enters the management page, where you can check the alarms, performance statistics, and the basic information of the storage system.

----End

## 2.2.3 Logging In to the CLI of the Storage System Using Username and Password

This document uses Windows Server 2008 as an example. For maintenance terminal running other versions of operating systems, adjust the operations based on actual conditions.

You can log in to the storage system by either of the following methods:

- Through the serial port

If you have not configured an IP address for the storage system's management network port or forget the IP address, you can connect the maintenance terminal to the serial port on the storage system's controller enclosure using a serial cable. Then you can log in to the CLI of the storage system using access software (such as PuTTY) on the maintenance terminal.

- Through the management network port

- If you have configured an IPv4 or IPv6 address for the storage system's management network port, you can log in to CLI using the IP address.
- After connecting the controller enclosure to the maintenance terminal by using a network cable, you can log in to the storage system by using any type of remote login software that supports the SSH (This document uses the PuTTY software as an example).
- For a 2 U controller enclosure, the default IP addresses of the management network ports on controllers A and B are respectively **192.168.128.101** and **192.168.128.102**, and the default subnet mask is **255.255.0.0**. For a 3 U or 6 U controller enclosure, the default IP addresses of the management network ports on management modules 0 and 1 are respectively **192.168.128.101** and **192.168.128.102**, and the default subnet mask is **255.255.0.0**.
- Make sure that the IP address of the controller enclosure's management network port is in the same network segment as that of the maintenance terminal. If they are in different network segments, you can modify the IP address of the management network port through the serial port by running the **change system management\_ip** command.

### Logging In to the CLI Using the Serial Port (Windows)

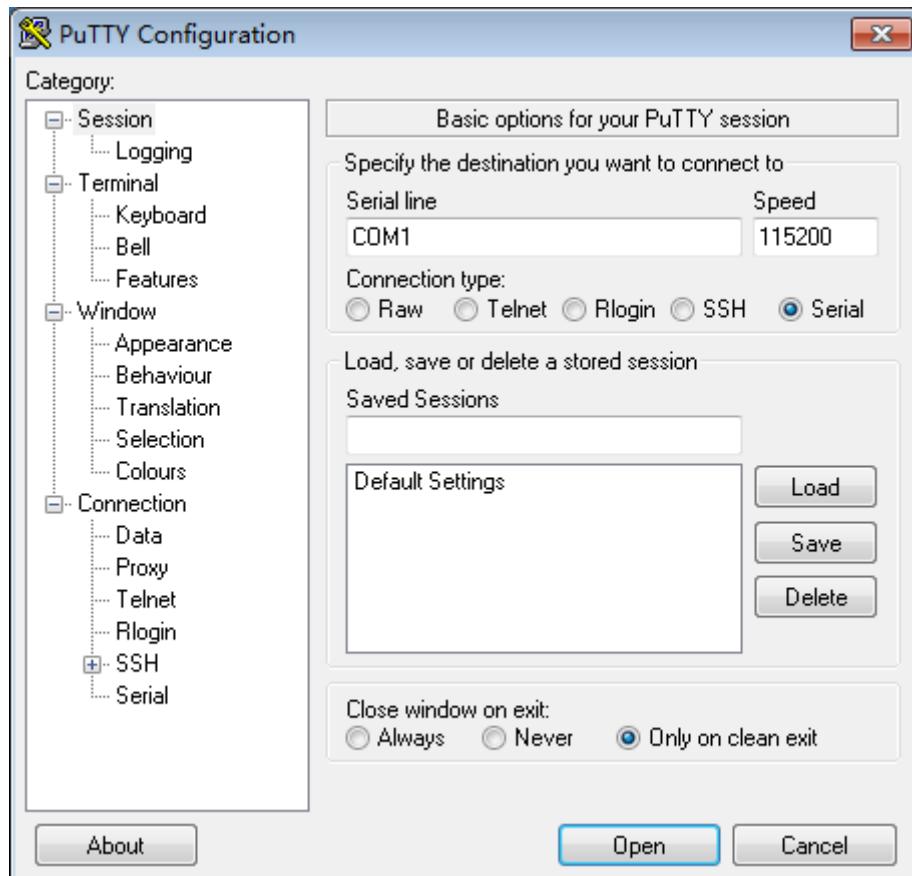
#### NOTE

- This document uses the PuTTY software as an example. You can download PuTTY from chiark website.
- You are advised to use the latest version of PuTTY, otherwise you may fail to log in to the storage system.

1. Run the PuTTY software.

The **PuTTY Configuration** dialog box is displayed, as shown in [Figure 2-5](#).

Figure 2-5 PuTTY Configuration dialog box



2. In **Connection type**, select **Serial**. In **Speed**, enter **115200**.
3. Click **Open**. When the connection succeeds, the following output is displayed.  
**storage Login:**
4. Enter the user name and password as prompted. You are required to change the password upon your initial login to ensure system security. If the login succeeds, the following information is displayed.

```
Storage login: admin

Authorized users only. All activity may be monitored and reported.
Using keyboard-interactive authentication.

password:

WARNING: You have accessed the system operated by Huawei.
You are required to have a personal authorisation from the system
administrator before you use this computer. Unauthorised access to or misuse
of this system is prohibited.

For security purposes, please change the initial password and log in to the
system using the new password.
Old password:*****
New password:*****
Reenter password:*****

System Name      : Huawei.Storage
Health Status   : Normal
Running Status  : Normal
Total Capacity  : 6.240TB
SN              : XXXXXXXXXXXXXXXXXXXXXXXXXX
```

```
Location      :  
Product Model : XXXXX  
Product Version : XXXXX  
Time          : XXXX-XX-XX/16:38:22 +08:00  
admin:/>
```

#### NOTE

- The default user name and password of the super administrator are **admin** and **Admin@storage** respectively.
- **Product Model** and **Product Version** vary with the actual device you have logged in to. The actual interface display prevails.
- You are advised to change your login password periodically in the future by executing the **change user\_password** command. This reduces the password leakage risks.
- If you forget the password of an administrator or a read-only user, contact the super administrator to run **change user** to reset the password. If you forget the password of the super administrator (**admin** by default), contact super administrator **\_super\_admin** to log in to the CLI through a serial port and run **initpasswd** to reset the password.

## Logging In to the CLI Using the Serial Port (Linux)

#### NOTE

- This document uses the Minicom software as an example. You can download Minicom from its official website.
- This document uses SSH Secure Shell Client to upload the Minicom installation package to the Linux host. You can download SSH Secure Shell Client from its official website.
- You must enable SSH on the Linux host. The default port ID is 22.

1. Check whether Minicom has been installed on the host.

Log in to the Linux client and run the **rpm -qa | grep minicom** command.

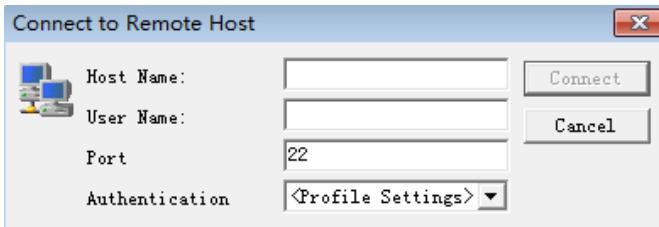
- If Minicom has been installed, its version is returned, for example:

```
[root@localhost ~]# rpm -qa |grep minicom  
[root@localhost ~]# minicom-2.3-27.24.4.1
```

Go to [5](#) to configure Minicom.

- If Minicom is not installed, no information will be returned. Go to [2](#) and [3](#) to install it.

2. Upload the Minicom and rzs2 installation package to the Linux host. This document uses SSH Secure Shell Client on a Windows host to upload the packages to the Linux host.
  - a. Install SSH Secure Shell Client on a Windows host. Double-click the **Secure File Transfer Client** shortcut to run the software.
  - b. Click **Quick Connect** on the menu bar. Input the **Host Name**, **User Name**, **Port**, and **Authentication** of the Linux host and click **connect**. Then enter the password to access the Linux host.

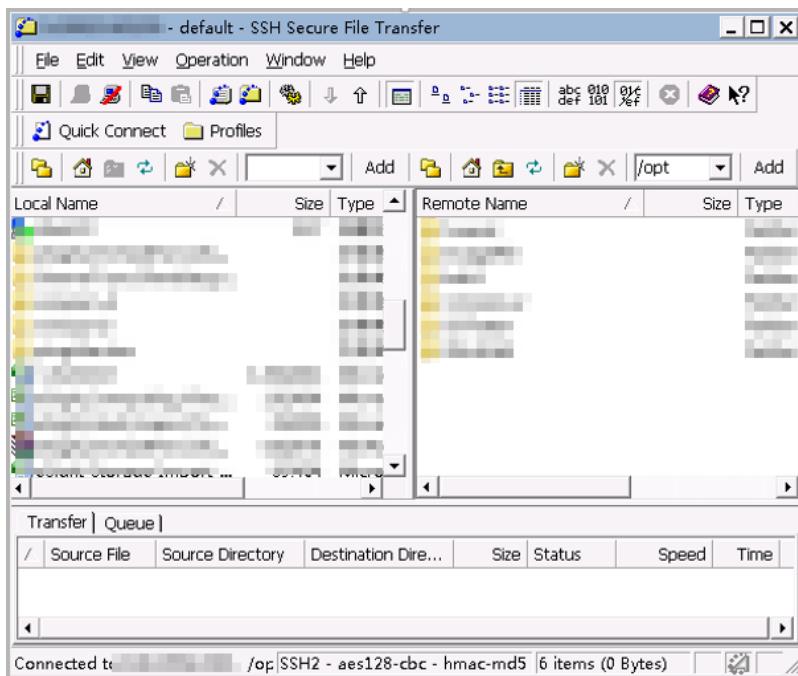


#### NOTE

The default port is 22.

- c. Click  on the menu bar. The file transfer page is displayed.

By default, **Local Name** is the file directory on the Windows host and **Remote Name** is the file directory on the Linux host.



- d. Select the Minicom installation package and rzsx installation package on the Windows host, right-click on it, and select **upload** to upload the installation packages to the Linux host.
3. Install the rzsx software.

On the Linux client, run the **rpm -ivh Installation package name** command.

```
[root@localhost minicom]# rpm -ivh rzsx-0.12.20-853.2.i586.rpm
Preparing... ##### [100%]
1:rzsx ##### [100%]
```

4. Install the Minicom software.

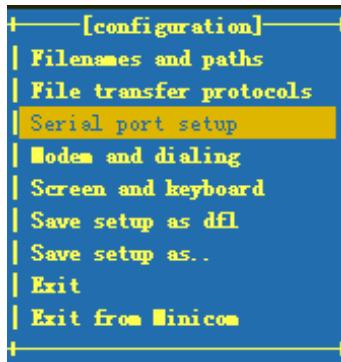
On the Linux client, run the **rpm -ivh Installation package name** command.

```
[root@localhost minicom]# rpm -ivh minicom-2.3-27.24.4.1.x86_64.rpm
Preparing... ##### [100%]
1:minicom ##### [100%]
```

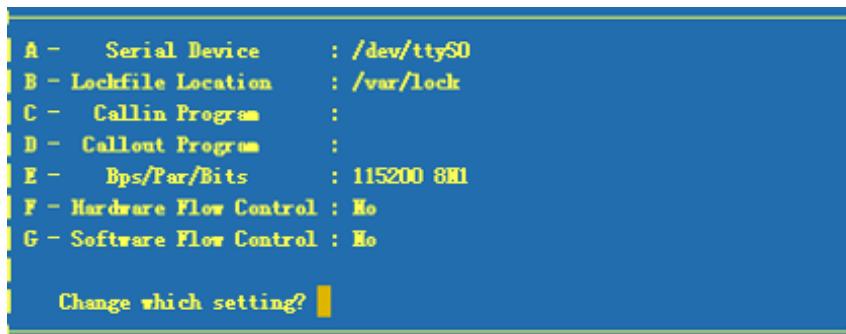
5. Configure Minicom.

After Minicom has been installed, configure Minicom to connect the Linux host to the storage system.

- a. Log in to the Linux client and run the **minicom -s** command. The **configuration** page is displayed.



- b. Select **Serial port setup** and press **Enter**.



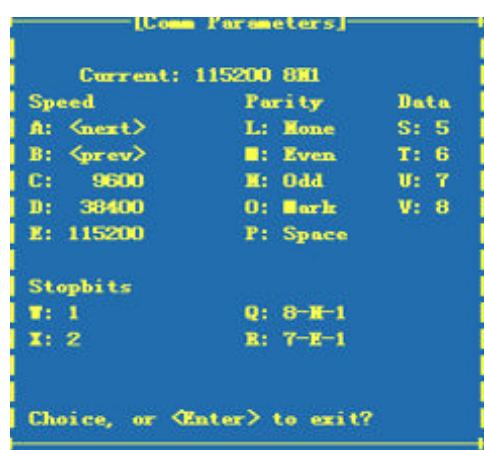
- c. Configure serial port parameters.

6. Configure the serial port device.

Press **A**. Input **/dev/ttS0** in **Serial Device** and press **Enter**.

7. Configure the Baud rate for the serial port.

Press **E**. The **Comm Parameters** page is displayed. Generally, the Baud rate of the storage system is 115200. Press **E** and select **115200**. Then press **Enter** to return to the **configuration** page.



1. On the **configuration** page, click **Save setup as dfl** to save the configurations and then click **Exit**.
2. After configuring Minicom, run the **minicom** command on the Linux client. The following message is returned:  
Storage login:

3. Enter the user name and password as prompted. The system asks you to change the password upon the first login. Change the password immediately to ensure system security. The following information is displayed if the login is successful:

```
Storage login: admin

Authorized users only. All activity may be monitored and reported.
Using keyboard-interactive authentication.
password:

WARNING: You have accessed the system operated by Huawei.
You are required to have a personal authorisation from the system
administrator before you use this computer. Unauthorised access to or misuse
of this system is prohibited.

For security purposes, please change the initial password and log in to the
system using the new password.
Old password:*****
New password:*****
Reenter password:*****

System Name      : Huawei.Storage
Health Status   : Normal
Running Status  : Normal
Total Capacity  : 6.240TB
SN              : XXXXXXXXXXXXXXXXXXXXXXXXX
Location        :
Product Model   : XXXXX
Product Version : XXXXX
Time            : XXXX-XX-XX/16:38:22 +08:00
admin:/>
```

#### NOTE

- The default super administrator name is **admin** and its password is **Admin@storage**.
- **Product Model** and **Product Version** vary with the actual device you have logged in to. The actual interface display prevails.
- You are advised to change your login password periodically in the future by executing the **change user\_password** command. This reduces the password leakage risks.
- If you forget the password of an administrator or a read-only user, contact the super administrator to run **change user** to reset the password. If the password of the super administrator **admin** is lost, another super administrator **\_super\_admin** can log in to the CLI via a serial port and run **initpasswd** to reset the password.

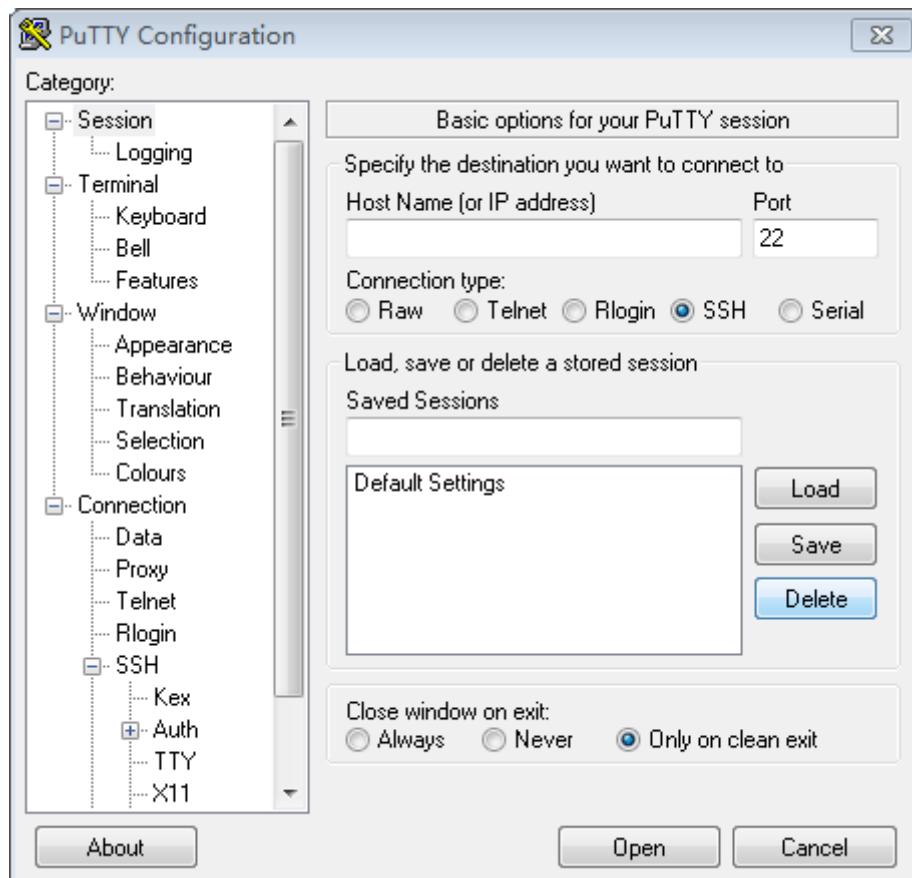
## Logging In to the CLI Through the Management Network Port (Windows)

#### NOTE

- This document uses the PuTTY software as an example. You can download PuTTY from chiark website.
- You are advised to use the latest version of PuTTY, otherwise you may fail to log in to the storage system.

1. Run the PuTTY software. The **PuTTY Configuration** dialog box is displayed, as shown in [Figure 2-6](#).

Figure 2-6 PuTTY Configuration dialog box



2. Select **Session**. Type the IP address of the management network port in the **Host Name (or IP address)** text box in the **Specify the destination you want to connect to** area. The IP address **192.168.6.96** is used as an example. Set **Connection type** to **SSH**.
3. Click **Open**, and the interface is displayed, and the following output is displayed.  
**login as:**
4. Enter the user name and password as prompted. You are required to change the password upon your initial login to ensure system security. If the login succeeds, the following information is displayed.

```
login as: admin

Authorized users only. All activity may be monitored and reported.
Using keyboard-interactive authentication.
password:

WARNING: You have accessed the system operated by Huawei.
You are required to have a personal authorisation from the system
administrator before you use this computer. Unauthorised access to or misuse
of this system is prohibited.

For security purposes, please change the initial password and log in to the
system using the new password.
Old password:*****
New password:*****
Reenter password:*****

System Name      : Huawei.Storage
Health Status   : Normal
```

```
Running Status : Normal
Total Capacity : 6.240TB
SN : XXXXXXXXXXXXXXXXXXXXXXXXX
Location :
Product Model : XXXXX
Product Version : XXXXX
Time : XXXX-XX-XX/16:38:22 +08:00
admin:/>
```

#### NOTE

- The default user name and password of the super administrator are **admin** and **Admin@storage** respectively.
- **Product Model** and **Product Version** vary with the actual device you have logged in to. The actual interface display prevails.
- You are advised to change your login password periodically in the future by executing the **change user\_password** command. This reduces the password leakage risks.
- If you forget the password of an administrator or a read-only user, contact the super administrator to run **change user** to reset the password. If you forget the password of the super administrator (**admin** by default), contact super administrator **\_super\_admin** to log in to the CLI through a serial port and run **initpasswd** to reset the password.

## 2.2.4 Logging In to the CLI of the Storage System Using a Public Key

Public key authentication uses a pair of associated public and private keys to authenticate users, instead of using usernames and passwords. This section uses PuTTY as an example to describe how to generate public and private keys as well as configure public key authentication to log in to the CLI.

### Prerequisites

- Only a super administrator has the permission to modify users' authentication mode for logging in to the CLI.
- Public key authentication for logging in to the CLI is configured for local users only, not for domain users.

### Precautions

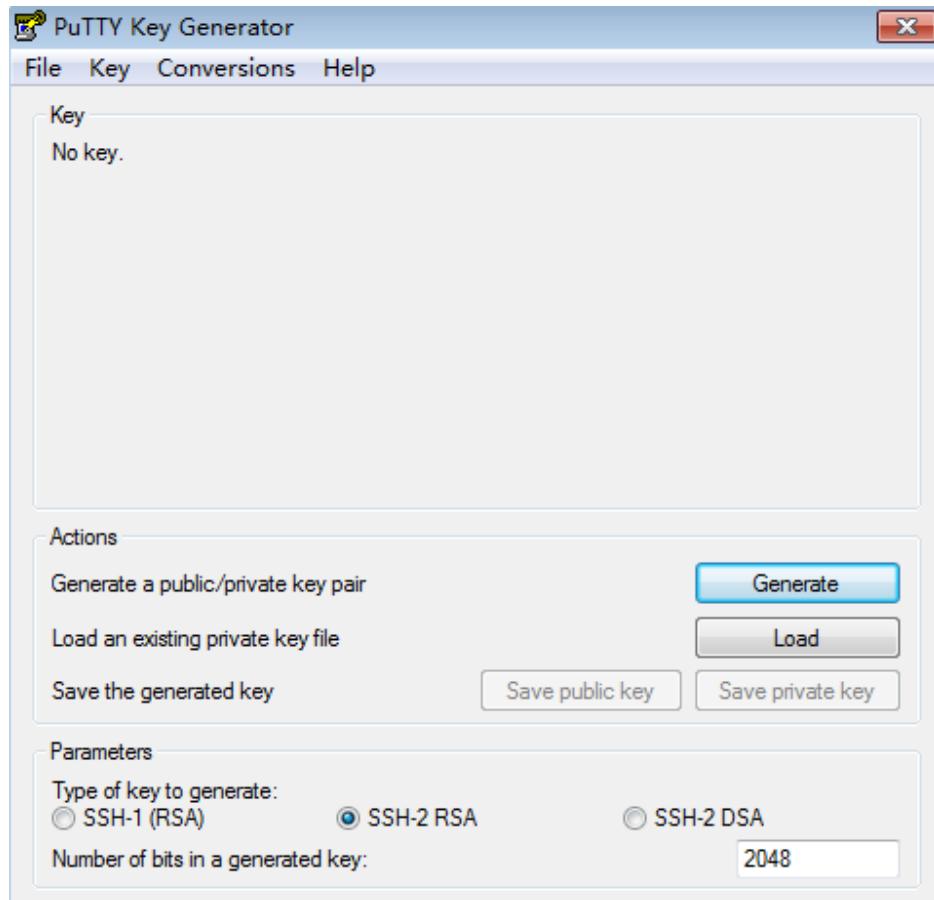
- After a private key is generated, keep it secure.
- Change the public key periodically. Use the new private-public key pair for login authentication to improve system security.

### Procedure

**Step 1** The super administrator generates a private-public key pair for a local user.

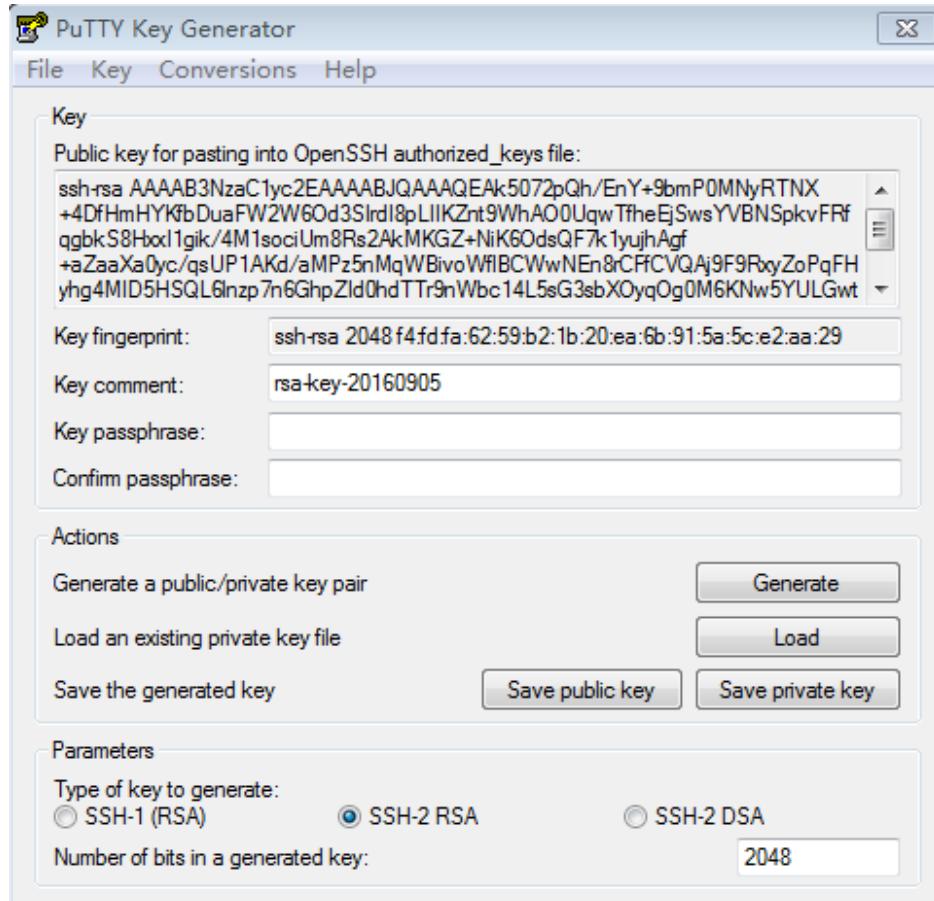
1. Run the **puttygen.exe** file.

Go to the **PuTTY Key Generator** main window, as shown in [Figure 2-7](#).

**Figure 2-7** Main window of the generator for a private-public key pair

2. In the **Parameters** area in the lower part of the page, set **Type of key to generate** to **SSH-2 RSA** or **SSH-2 DSA**, and set **Number of bits in a generated key** to an integer from 2048 to 8192.
3. Click **Generate** and move the cursor over the blank area in the lower part of the **Key** area to generate a public key.

The public key will be displayed in the area, as shown in **Figure 2-8**.

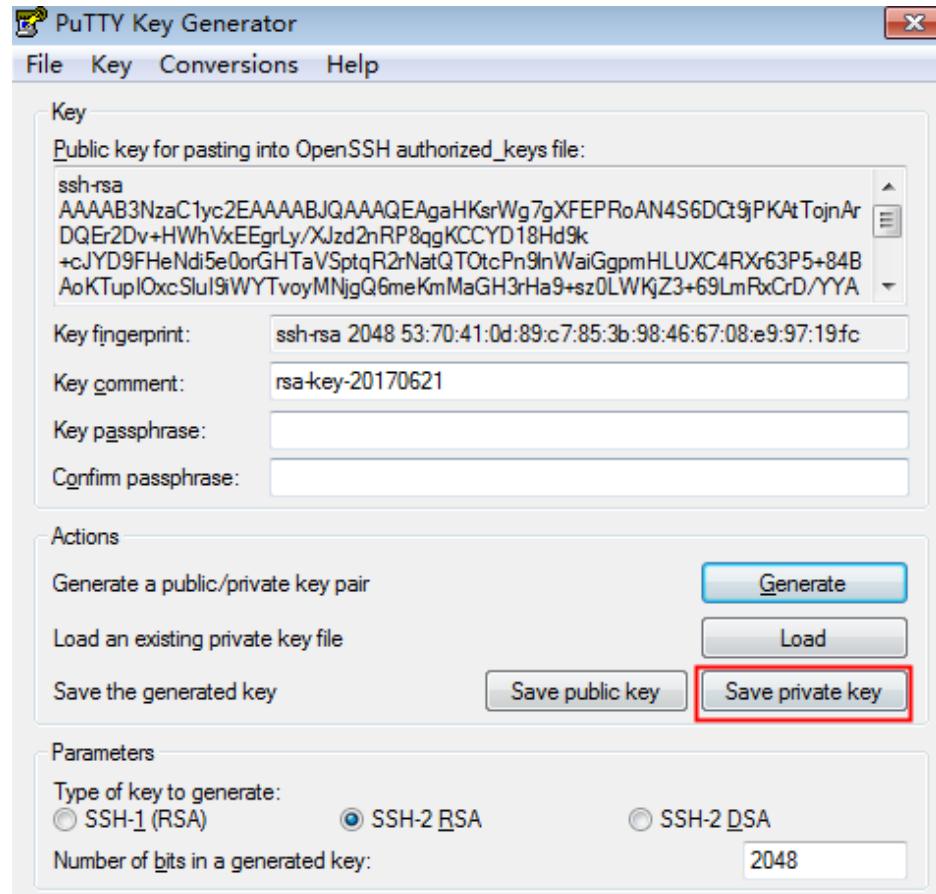
**Figure 2-8** Generating the public key

4. Copy and save the public key to the local path.
5. (Optional) In **Key passphrase**, enter a password to encrypt the private key. In **Confirm passphrase**, enter the password again.

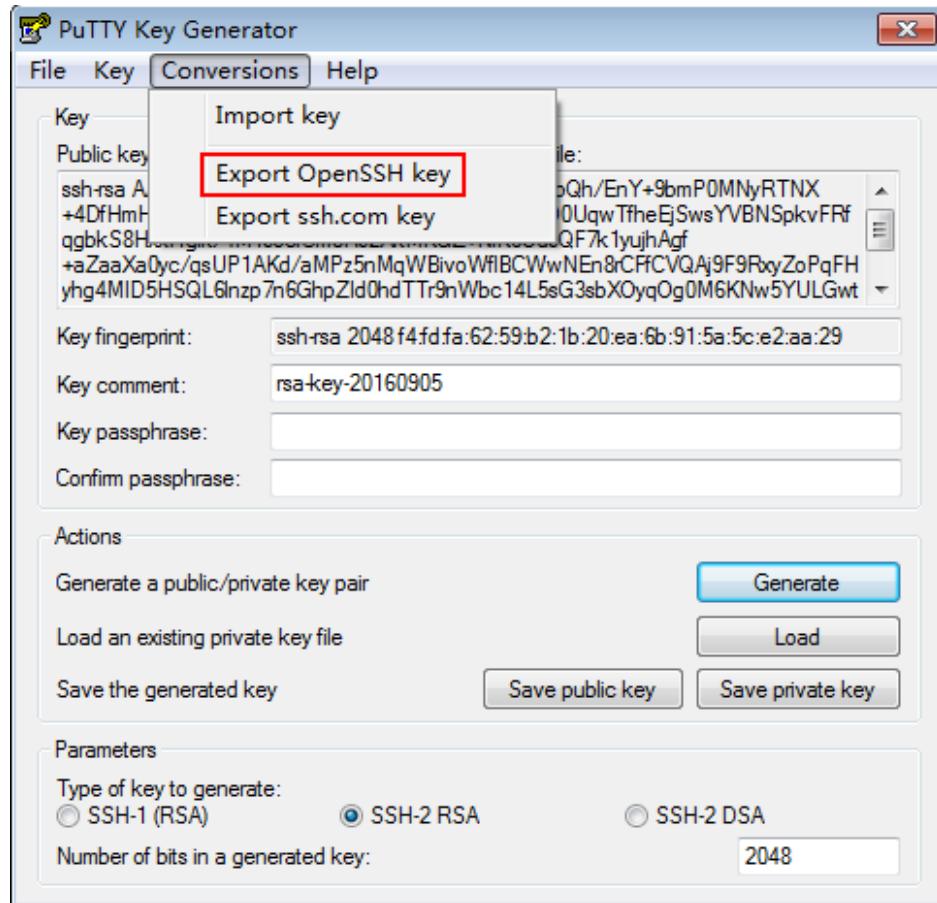
**NOTE**

For the security of the private key file, you are advised to configure a secure password to encrypt the private key file.

6. The method to generate the private key file varies with the tool used to log in to the CLI.
  - If you use PuTTY to log in to the CLI, click **Save private key** and save the private key file to the local path, as shown in **Figure 2-9**.

**Figure 2-9** Generating the private key

- If you use the other tools to log in to the CLI, choose **Conversions > Export OpenSSH key** and save the private key file to the local path, as shown in [Figure 2-10](#).

**Figure 2-10** Generating the private key

**Step 2** The super administrator modifies the login authentication mode of local users.

1. Log in to the CLI of the storage system as the super administrator.
2. Run the **change user\_ssh\_auth\_mode general user\_name=test123 auth\_mode=publickey** command to modify users' modification mode to **public key**. **user\_name** indicates the user name of the login authentication mode to be modified.
3. Copy the locally saved public key to **Public key** on the CLI as instructed, and press **Enter**.

After executing the command successfully, users map the private key to the public key to log in to the CLI.

```
admin:/>change user_ssh_auth_info general user_name=test123
auth_mode=publickey CAUTION:Only public keys generated using the SSH-2 RSA/
DSA encryption algorithm and using keys whose lengths range from 2048 to 8192
bits are supported. Public key:ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQPLuhb/
KuHbyZiln7yX6N3v5KG0JX8XdDnx0dfhN4yP7V
+WXeqRt93YGeplnsxIuvve1QCMs3jxt8uy2kDMwRY6opLRV2qh5QCk1M54owpdnjwphs1g2oKyddt5i
z7x10svZU7gfR2qP4WgGI81Ba9rA8bQ1ZWod
+tmW6OJ80Wey37FcyZwNJPNCiTWfg2ju2sQuuvmtmum8hALQu930LbRWmTTtP33IAW/
a1LMXjeEj49yhAAfL5OXVvyGMvDi3UFZJmWUZMF6eAG8joSiM50K8QuW7YUzW43t1LAXfGa7wBsp2u
6HvckMXxzyr/3tanHkclnuGZ55+Byw9mbnNn2Z root@Storage Command executed
successfully.
```

**Step 3** Local users configure PuTTY and log in to the storage system.

1. Start PuTTY.
- Go to the **PuTTY Configuration** dialog box.
2. Click **Session**. In the right pane, type the IP address of a storage system's management network port in the **Host Name (or IP address)** text box. Set **Port** and **Connection type** to **22** and **SSH** respectively.
3. Choose **Connection > Data**. In the **Login details** text box in the right pane, type the user name of the login authentication mode to be modified.
4. Choose **Connection > SSH > Auth**. In the right pane, click **Browse**. Select and open the locally saved private key file.
5. Click **Open** to log in to the CLI.

 **NOTE**

If the password of the private key is encrypted in **Step 1.5**, type the password when logging in to the CLI, and then press **Enter**.

Using username "test123".

Authorized users only. All activities may be monitored and reported.

Authenticating with public key "imported-openssh-key"

Passphrase for key "imported-openssh-key":

Last login: XX XX XX XX:XX:XX XXXX from 192.168.18.158

WARNING: You have accessed the system.

You are required to have a personal authorisation from the system administrator before you use this computer. Unauthorised access to or misuse of this system is prohibited.

System Name : Huawei.Storage

Health Status : Normal

Running Status : Normal

Total Capacity : 4.247TB

SN : XXXXXXXXXXXX

Location :

Product Model : XXXX

Product Version : XXXX

Time : XXXX-XX-XX/XX:XX:XX UTC+08:00

Patch Version :

test123:/>

----End

## Follow-up Procedure

To modify a user's login authentication mode to the **Username+Password** mode, run the **change user\_ssh\_auth\_mode general user\_name=test123 auth\_mode=password** command and use the original password to log in to the CLI of a storage system.

## 2.3 Logging In to the Storage System (OceanStor 18000 Series)

You can log in to the storage system using either DeviceManager or CLI to configure, manage, and maintain the system.

## 2.3.1 Logging In to DeviceManager (Through SVP)

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

### Prerequisites

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

### Context

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

 **NOTE**

The super administrator can run **change devicemanager tls min\_version=?** to change the earliest version of TLS supported by DeviceManager. Then, the super administrator must run **reboot storage service service\_name=devicemanager** to restart DeviceManager for the change to take effect.

### Procedure

**Step 1** Log in to the Windows operating system built in the SVP.

- If you use the KVM to operate the SVP, complete the following steps to log in to the Windows operating system built in the SVP.
  - a. Log in to the SVP host as user **svp\_user**. The default password is **Aguser@12#%**.
  - b. On the host desktop, choose **Applications > System > Terminal > Xterm**.
  - c. In the command window that is displayed, run **vncviewer -fullscreen 127.0.0.1:1**. Go to the login page of the Windows operating system built in the SVP.
  - d. Type the user name and password in the login page of the Windows operating system built in the SVP, and press **Enter**.

 **NOTE**

The initial user name and password are **maintainer** and **Maintainer@svp**, respectively.

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

 **NOTE**

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

1. Choose **Start > All Programs > Accessories > Remote Desktop Connection**. The **Remote Desktop Connection** dialog box is displayed.
2. Type the IP address of the management network port in the **Computer** text box and press **Enter**.

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

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

 **NOTE**

For storage system security, perform the following operations to modify the password of the **maintainer** account upon your first login.

1. On the SVP interface, press **Windows+R** combination keys (perform this operation in full screen mode when in a remote desktop connection), type **cmd** and press **Enter** to open the command line interface.
2. Run the command **net user maintainer password** to modify the password, where the *password* is the new password.



**Step 2** On the desktop, double-click .

 **NOTE**

- Your web browser may show that the website has a privacy error. If the IP address is correct, you can neglect the prompt and continue to access the storage system. If you want to fix this error, you can have the certificate request file signed by a third-party CA center or by your own CA certificates. For details about the method using your own CA certificates, see [6.7 How Can I Use Self-Signed Certificates to Fix the Privacy Error Displayed When I Attempt to Log In to DeviceManager?](#)
- If you have a usable security certificate, you are advised to use corresponding commands to import the certificate to improve system security. For details about the corresponding commands, see [Command Reference](#).

The DeviceManager login page is displayed.

**Step 3** (Optional) Choose an authentication mode and language.

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

 **NOTE**

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

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

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

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

**NOTE**

- If you enter wrong passwords for consecutive two times, you need to enter the verification code. In **Verification Code**, enter the verification code.
- If **LDAP user** is selected, the username and password must be a domain username and password. If you want to log in as the super administrator, the default user name and password are **admin** and **Admin@storage** respectively.
- If you forget the password of an administrator or a read-only user, contact the super administrator to reset the password. If you forget the password of the super administrator (**admin** by default), contact super administrator **\_super\_admin** to log in to the CLI through a serial port and run **initpasswd** to reset the password. For details, see [5.3.3.8 Resetting the Password of an Administrator or a Read-Only User](#) and [5.3.3.9 Resetting the Password of a Super Administrator](#).
- If you enter incorrect passwords a specified number of times (equal to the value specified in **Number of Incorrect Passwords** on the **Login Policy** page), the account is automatically locked for the period of lock time (The lock period of the super administrator is 15 minutes, and the lock period of other users is 15 minutes by default).
- You must change the default login password immediately when you are logging in to the storage system for the first time and periodically change your login password in the future. This reduces the password leakage risks. For details about how to change the password, see [5.3.3.7 Changing Password](#).

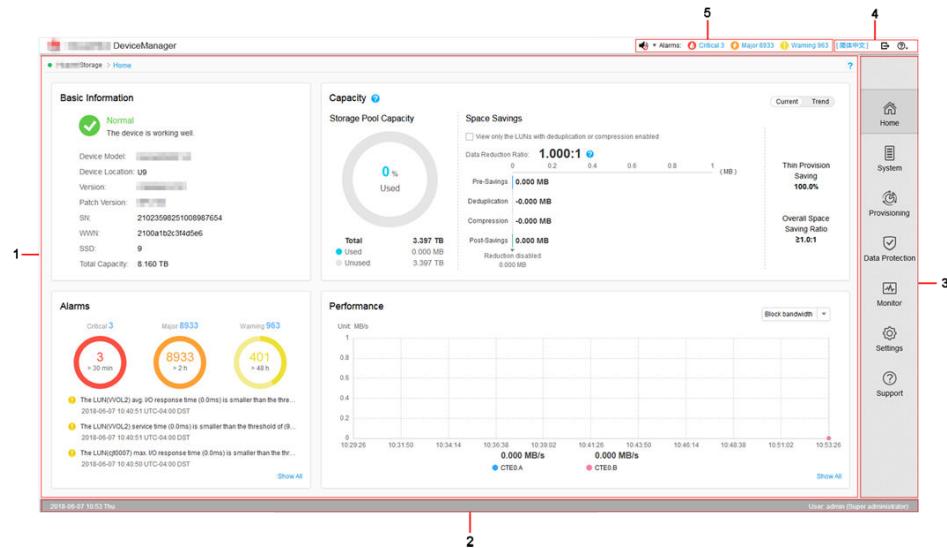
**Step 5 Click Log In.****NOTE**

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

The DeviceManager main window is displayed.

**Figure 2-11** shows the main window of DeviceManager.

**Figure 2-11** Main window of DeviceManager



**Table 2-5** describes the components of the DeviceManager main window.

**Table 2-5** Components of the DeviceManager main window

No.	Name	Function
1	Function pane	Displays the graphical user interfaces (GUIs) for completing a specific activity on DeviceManager.
2	Status bar	Shows the name and login time of the currently logged-in user.
3	Navigation bar	Lists available logical functional modules of the storage device.
4	Log out, help, and language area	The log out, help, and language area shows the log out, help, and language buttons.
5	Fault statistics pane	Displays different severities of device alarms, which can be checked by users to learn about the running status of the storage device.

----End

### 2.3.2 Logging In to DeviceManager (Through PC)

To log in to DeviceManager, open a web browser on a maintenance terminal connected to the service processor (SVP), and type the IP address of the management network port on the SVP in the address box.

#### Prerequisites

- The communication between the maintenance terminal and the SVP is normal.
- You have recorded the management IP address of the SVP.
- Before logging in to DeviceManager as a Lightweight Directory Access Protocol (LDAP) domain user, first configure the LDAP domain server, and then configure LDAP server parameters on the storage device accordingly, at last create an LDAP user.
- Operating system and browser versions of the maintenance terminal.

DeviceManager supports multiple operating systems and browsers. You can query the compatibility using the [OceanStor Interoperability Navigator](#).

#### Context

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

##### NOTE

The super administrator can run **change devicemanager tls min\_version=?** to change the earliest version of TLS supported by DeviceManager. Then, the super administrator must run **reboot storage service service\_name=devicemanager** to restart DeviceManager for the change to take effect.

- This document exemplifies how to log in to DeviceManager in Windows. For other operating systems, revise the login procedure accordingly.
- By default, DeviceManager allows 32 users to log in concurrently.

## Procedure

**Step 1** Open the web browser on the maintenance terminal.

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

The DeviceManager login page is displayed.



### NOTE

- *XXX.XXX.XXX.XXX* represents the IP address of the SVP management network port.
- Your web browser may show that the website has a privacy error. If the IP address is correct, you can neglect the prompt and continue to access the storage system. If you want to fix this error, you can have the certificate request file signed by a third-party CA center or by your own CA certificates. For details about the method using your own CA certificates, see [6.7 How Can I Use Self-Signed Certificates to Fix the Privacy Error Displayed When I Attempt to Log In to DeviceManager?](#)
- If you have a usable security certificate, you are advised to use corresponding commands to import the certificate to improve system security. For details about the corresponding commands, see [Command Reference](#).

**Step 3** (Optional) Choose an authentication mode and language.

1. Click **Advanced**.

2. Select an authentication mode from the **Authentication mode** list.

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



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

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

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

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



### NOTE

- If you enter wrong passwords for consecutive two times, you need to enter the verification code. In **Verification Code**, enter the verification code.
- If **LDAP user** is selected, the username and password must be a domain username and password. If you want to log in as the super administrator, the default user name and password are **admin** and **Admin@storage** respectively.
- If you forget the password of an administrator or a read-only user, contact the super administrator to reset the password. If you forget the password of the super administrator (**admin** by default), contact super administrator **\_super\_admin** to log in to the CLI through a serial port and run **initpasswd** to reset the password. For details, see [5.3.3.8 Resetting the Password of an Administrator or a Read-Only User](#) and [5.3.3.9 Resetting the Password of a Super Administrator](#).
- If you enter incorrect passwords a specified number of times (equal to the value specified in **Number of Incorrect Passwords** on the **Login Policy** page), the account is automatically locked for the period of lock time (The lock period of the super administrator is 15 minutes, and the lock period of other users is 15 minutes by default).
- You must change the default login password immediately when you are logging in to the storage system for the first time and periodically change your login password in the future. This reduces the password leakage risks. For details about how to change the password, see [5.3.3.7 Changing Password](#).

**Step 5** Click **Log In**.

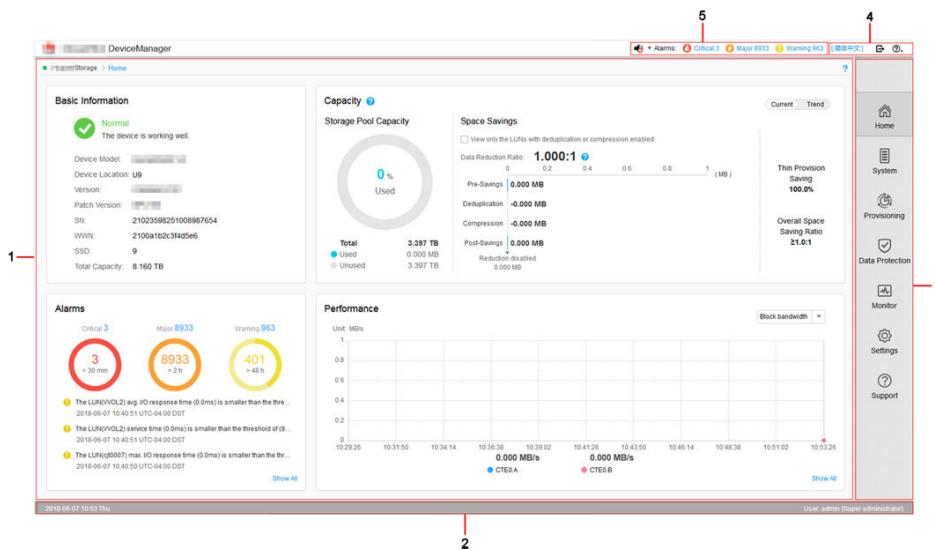
**NOTE**

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

The DeviceManager main window is displayed.

**Figure 2-12** shows the DeviceManager main window.

**Figure 2-12** DeviceManager main window



**Table 2-6** describes components of the DeviceManager main window.

**Table 2-6** Components of the DeviceManager main window

No.	Name	Function
1	Function pane	Displays the graphical user interfaces (GUIs) for completing a specific activity on DeviceManager.
2	Status bar	Shows the name and login time of the currently logged-in user.
3	Navigation bar	Lists available logical functional modules of the storage device.
4	Log out, help, and language area	The log out, help, and language buttons.

No.	Name	Function
5	Fault statistics pane	Displays different severities of device alarms, which can be checked by users to learn about the running status of the storage device.

----End

### 2.3.3 Logging In to DeviceManager (Management Network Port)

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

#### Prerequisites

- The IP address of the management port of the storage system has been configured.
- The maintenance terminal communicates with the storage system properly.
- Before logging in to DeviceManager as a Lightweight Directory Access Protocol (LDAP) domain user, first configure the LDAP domain server, and then configure LDAP server parameters on the storage device accordingly, at last create an LDAP user.
- The initial user name and password for logging in to DeviceManager are **admin** and **Admin@storage** respectively.
- Operating system and browser versions of the maintenance terminal.

DeviceManager supports multiple operating systems and browsers. You can query the compatibility using the [OceanStor Interoperability Navigator](#).

#### Context

- DeviceManager only supports TSL protocols (including TLS 1.0, TLS 1.1, and TLS 1.2).
- The default IP addresses of the management network ports on management modules 0 and 1 are respectively **192.168.128.101** and **192.168.128.102**, and the default subnet mask is **255.255.0.0**.
- This document exemplifies how to log in to DeviceManager in Windows using Mozilla Firefox. For other operating systems, revise the login procedure accordingly.
- By default, DeviceManager allows 32 users to log in concurrently.

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

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

## Procedure

**Step 1** Open Mozilla Firefox on the maintenance terminal.

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

The DeviceManager login page is displayed.

 **NOTE**

- *XXX.XXX.XXX.XXX* represents the IP address of the storage system management network port.
- Your web browser may show that the website has a privacy error. If the IP address is correct, you can neglect the prompt and continue to access the storage system. If you want to fix this error, you can have the certificate request file signed by a third-party CA center or by your own CA certificates. For details about the method using your own CA certificates, see [6.7 How Can I Use Self-Signed Certificates to Fix the Privacy Error Displayed When I Attempt to Log In to DeviceManager?](#)
- If you have a usable security certificate, you are advised to use corresponding commands to import the certificate to improve system security. For details about the corresponding commands, see [Command Reference](#).

**Step 3** (Optional) Choose an authentication mode and language.

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

 **NOTE**

- The **admin** user can log in to the storage system only in **Local user** authentication mode.
- **LDAP user**: Logs in to the storage system using LDAP domain authentication.

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

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

 **NOTE**

- If you enter wrong passwords for consecutive two times, you need to enter the verification code. In **Verification Code**, enter the verification code.
- If **LDAP user** is selected, the username and password must be a domain username and password. If you want to log in as the super administrator, the default user name and password are **admin** and **Admin@storage** respectively.
- If you forget the password of an administrator or a read-only user, contact the super administrator to reset the password. If you forget the password as the super administrator (**admin** by default), contact super administrator **\_super\_admin** to log in to the CLI through a serial port and run **initpasswd** to reset the password. For details, see [5.3.3.8 Resetting the Password of an Administrator or a Read-Only User](#) and [5.3.3.9 Resetting the Password of a Super Administrator](#).
- If you enter incorrect passwords a specified number of times (equal to the value specified in **Number of Incorrect Passwords** on the **Login Policy** page), the account is automatically locked for the period of lock time (The lock period of the super administrator is 15 minutes, and the lock period of other users is 15 minutes by default).
- You must change the default login password immediately when you are logging in to the storage system for the first time and periodically change your login password in the future. This reduces the password leakage risks. For details about how to change the password, see [5.3.3.7 Changing Password](#).

**Step 5** Click **Log In**.

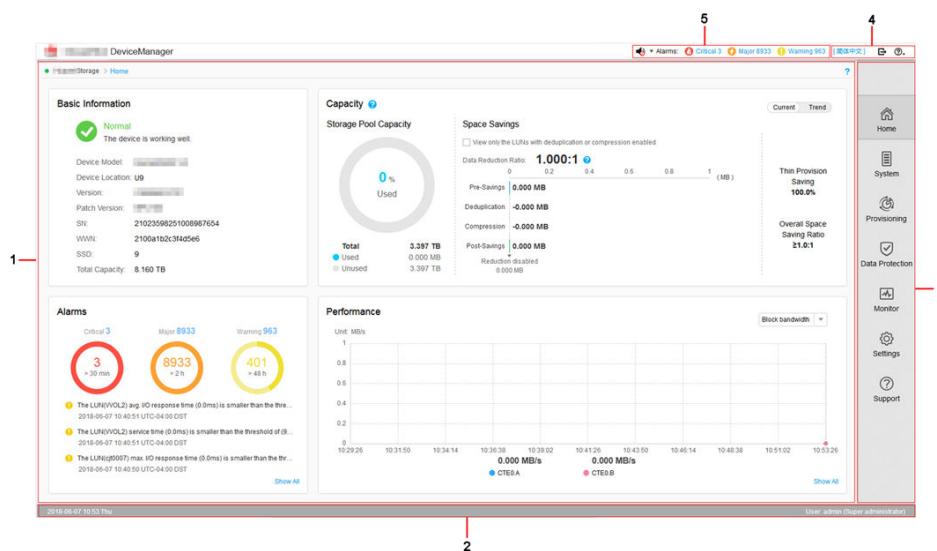
**NOTE**

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

The DeviceManager main window is displayed.

**Figure 2-13** shows the DeviceManager main window.

**Figure 2-13** DeviceManager main window



**Table 2-7** describes components of the DeviceManager main window.

**Table 2-7** Components of the DeviceManager main window

No.	Name	Function
1	Function pane	Displays the graphical user interfaces (GUIs) for completing a specific activity on DeviceManager.
2	Status bar	Shows the name and login time of the currently logged-in user.
3	Navigation bar	Lists available logical functional modules of the storage device.
4	Log out, help, and language area	The log out, help, and language buttons.

No.	Name	Function
5	Fault statistics pane	Displays different levels of device alarms, which can be checked by users to better understand the running status of the storage device.

----End

### 2.3.4 Logging In to DeviceManager (Using a Tablet)

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

#### Context

- The default user name and password of the super administrator are **admin** and **Admin@storage** respectively.
- In terms of tablet-based login, you can only use iPad Air (Safari) and HUAWEI MediaPad 10 FHD (Chrome of the latest version). This section uses iPad as an example to describe how to log in to the management software. The login operations on other mobile devices are similar.
- By default, DeviceManager allows 32 users to log in concurrently.
- If a user does not perform any operations after logging in to the system for a period longer than the timeout limit (the limit is 30 minutes by default and modifiable), the system logs out automatically.
- If an account is not used to log in to the system for a certain period of time (the period is 60 days by default and modifiable), it will be locked and can only be unlocked by the super administrator.

#### Procedure

##### Step 1 Access a Wi-Fi network.

1. On the desktop of iPad, choose **Settings > WLAN**.  
The **WLAN** page is displayed.
2. In the **CHOOSE A NETWORK** area, select the desired Wi-Fi network.  
The **Enter Password** page is displayed.
3. Set **Password** to the password of the Wi-Fi network.
4. Click **Join**.  
The iPad is connected to the Wi-Fi network.

##### Step 2 Log in to the management software.

1. On the desktop of iPad, click **Safari**.
2. Set **Address** to **https://xxx.xxx.xxx.xxx:8088/ismpad/login.html** and click **Go**.  
xxx.xxx.xxx.xxx indicates the IP address of the management network port on the SVP.  
The login page of the management software is displayed.
3. (Optional) In **Language**, select a language.
4. Set **Username** and **Password** to the user name and password for logging in to the management software.

 **NOTE**

- The default user name and password are **admin** and **Admin@storage** respectively.
- If a verification code is required, enter the correct verification code.
- You must change the default login password immediately when you are logging in to the storage system for the first time and periodically change your login password in the future. This reduces the password leakage risks. For details about how to change the password, see [5.3.3.7 Changing Password](#).
- If you forget the password of an administrator or a read-only user, contact the super administrator to reset the password. If you forget the password as the super administrator (**admin** by default), contact super administrator **\_super\_admin** to log in to the CLI through a serial port and run **initpasswd** to reset the password. For details, see [5.3.3.8 Resetting the Password of an Administrator or a Read-Only User](#) and [5.3.3.9 Resetting the Password of a Super Administrator](#).

5. Click **Log In**.

The home page of the management software is displayed.

---End

## 2.3.5 Logging In to the CLI of the Storage System (SVP's Management Network Port)

After logging in to the storage system through the command line interface (CLI), you can query, set, manage, and maintain the storage system.

You can log in to the storage system by either of the following methods:

- Through the remote login software
  - You can log in to the CLI by using the IPv4 address or IPv6 address.
  - After the maintenance terminal can correctly communicate with the SVP, you can log in to the storage system by using the remote login software (for example, PuTTY) that supports the SSH protocol.
- Through the service processor (SVP)
  - From a local computer
  - From a remote desktop

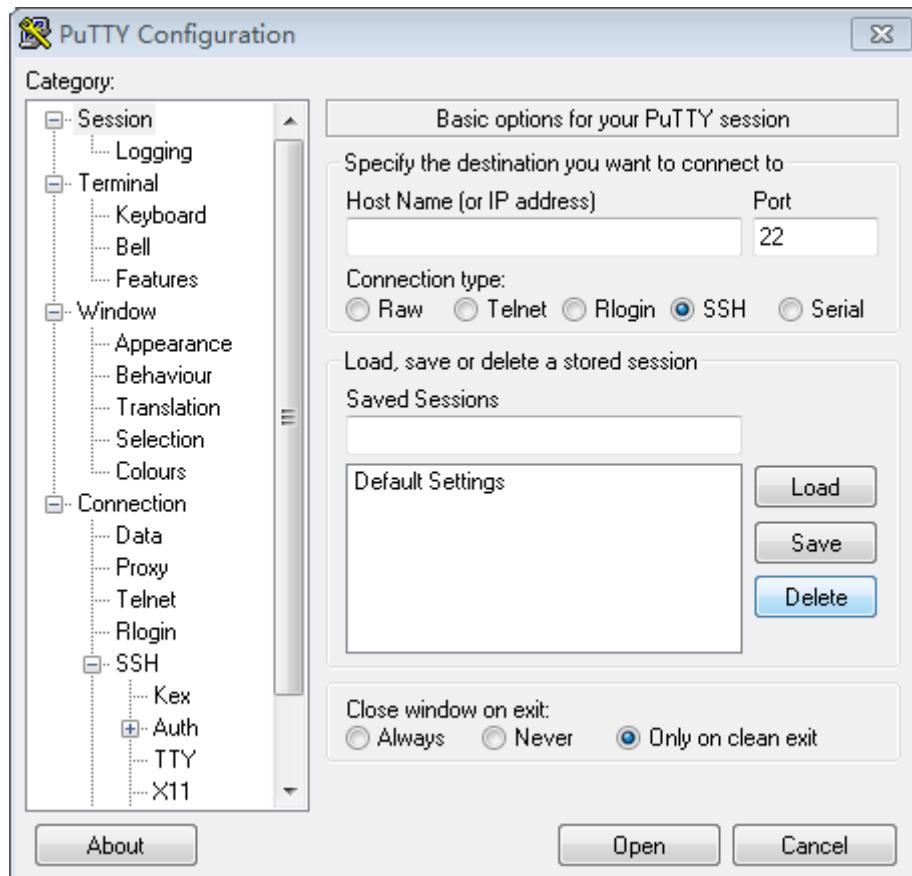
## Logging In to the Storage System Through the Remote Login Software

 **NOTE**

- This document uses the PuTTY software as an example. You can download PuTTY from chiark website.
- You are advised to use the latest version of PuTTY, otherwise you may fail to log in to the storage system.

1. Run the PuTTY software. The **PuTTY Configuration** dialog box is displayed, as shown in [Figure 2-14](#).

Figure 2-14 PuTTY Configuration dialog box



2. Select **Session**. Type the IP address of the SVP management network port in the **Host Name (or IP address)** text box in the **Specify your connection by host name or IP address** area. The IP address **192.168.6.96** is used as an example. Set **Connection type** to **SSH**.
3. Click **Open**, and the interface is displayed, and the following output is displayed.  
**login as:**
4. Enter the user name and password as prompted. You are required to change the password upon your initial login to ensure system security. If the login succeeds, the following information is displayed.

```
login as: admin

Authorized users only. All activity may be monitored and reported.
Using keyboard-interactive authentication.

password:

WARNING: You have accessed the system operated by Huawei.
You are required to have a personal authorisation from the system
administrator before you use this computer. Unauthorised access to or misuse
of this system is prohibited.

For security purposes, please change the initial password and log in to the
system using the new password.
Old password:*****
New password:*****
Reenter password:*****


System Name      : Huawei.Storage
```

```
Health Status : Normal
Running Status : Normal
Total Capacity : 6.240TB
SN : 210235G6TFZ0C7000045
Location :
Product Model : XXXXX
Product Version : VXXXRXXXCXX
Time : XXXX-XX-XX/16:38:22 +08:00
admin:/>
```

 **NOTE**

- The default user name and password of the super administrator are **admin** and **Admin@storage** respectively.
- **Product Model** and **Product Version** vary with the actual device you have logged in to. The actual interface display prevails.
- You are advised to change your login password periodically in the future by executing the `change user_password` command. This reduces the password leakage risks.
- If you forget the password of an administrator or a read-only user, contact the super administrator to run **change user** to reset the password. If you forget the password as the super administrator (**admin** by default), contact super administrator **\_super\_admin** to log in to the CLI through a serial port and run **initpasswd** to reset the password.

## Logging In to the Storage System Through the SVP

1. Log in to the SVP.
  - When logging in to the SVP from a local computer, log in to the Windows operating system built in the SVP by using the keyboard, video, and mouse (KVM) of system bay 0.
2. Log in to the SVP host as user **svp\_user**. The default password is **Aguser@12#\$**.
3. On the host desktop, choose **Applications > System > Terminal > Xterm**.
4. In the command window that is displayed, run **vncviewer -fullscreen 127.0.0.1:1**.  
Go to the login page of the Windows operating system built in the SVP.
5. Type the user name and password in the login page of the Windows operating system built in the SVP, and press **Enter**.

 **NOTE**

The initial user name and password are **maintainer** and **Maintainer@svp**, respectively.

- When logging in to the Windows operating system built in the SVP from a remote desktop, perform the following operations:
  1. On a maintenance terminal, choose **Start > All Programs > Attachment > Remote Desktop Connection**.  
The **Remote Desktop Connection** dialog box is displayed.
  2. In the **Computer** text box, type the IP address of the SVP management network port that is connected to the maintenance terminal. Press **Enter**.
  3. Type the user name and password to log in to the Windows operating system built in the SVP.

 **NOTE**

The initial user name and password are **maintainer** and **Maintainer@svp**.

1. On the desktop of the Windows operating system built in the SVP, start PuTTY and click **Session**. In the **Host Name (or IP Address)** text box of the **Specify your connection by host name or IP address** area, enter **172.17.126.11** (to log in to the CLI of the SVP) or

**172.16.192.200 or 172.16.193.200** (to log in to the CLI of the disk array). Then set **Connection type to SSH**.

2. Click **Open**, and the interface is displayed, and the following output is displayed.  
`login as:`
3. Enter the user name and password as prompted. You are required to change the password upon your initial login to ensure system security. If the login succeeds, the following information is displayed.

```
login as: admin

Authorized users only. All activity may be monitored and reported.
Using keyboard-interactive authentication.

password:

WARNING: You have accessed the system operated by Huawei.
You are required to have a personal authorisation from the system
administrator before you use this computer. Unauthorised access to or misuse
of this system is prohibited.

For security purposes, please change the initial password and log in to the
system using the new password.
Old password:*****
New password:*****
Reenter password:*****

System Name      : Huawei.Storage
Health Status   : Normal
Running Status  : Normal
Total Capacity  : 6.240TB
SN              : XXXXXX
Location        :
Product Model   : XXXXX
Product Version : VXXXRXXXCXX
Time            : 2015-04-09/16:38:22 +08:00
admin:/>
```

#### NOTE

- The default user name and password of the super administrator are **admin** and **Admin@storage** respectively.
- **Product Model** and **Product Version** vary with the actual device you have logged in to. The actual interface display prevails.
- You are advised to change your login password periodically in the future by executing the **change user\_password** command. This reduces the password leakage risks.
- If you forget the password of an administrator or a read-only user, contact the super administrator to run **change user** to reset the password. If you forget the password as the super administrator (**admin** by default), contact super administrator **\_super\_admin** to log in to the CLI through a serial port and run **initpasswd** to reset the password.

## 2.3.6 Logging In to the CLI of the Storage System (Engine's Management Network Port)

The storage system allows the maintenance terminal to log in to the CLI of the storage system through the controller's management network port, to configure, manage, maintain, and query on the storage system. This document uses Windows Server 2008 as an example. Adjust the operations if you use other operating systems.

### Context

- You can log in to the CLI by using the IPv4 address or IPv6 address.

- After connecting the maintenance terminal to the controller with cables, you can use remote login software that supports the SSH protocol (such as PuTTY) to log in to the CLI of the storage system on the maintenance terminal.
- Default IPv4 address of the management network port: **192.168.128.101** for management module 0, **192.168.128.102** for management module 1, and **255.255.0.0** for the subnet mask.

## Precautions

You must ensure that the IP addresses of the maintenance terminal and the management network port of the target controller fall in to the same network segment. This section explains how to change the management network port IP address through a serial port when the management network port IP address of the controller is not on the same network segment as that of the maintenance terminal. For details, see the **change system management\_ip** command.

### NOTE

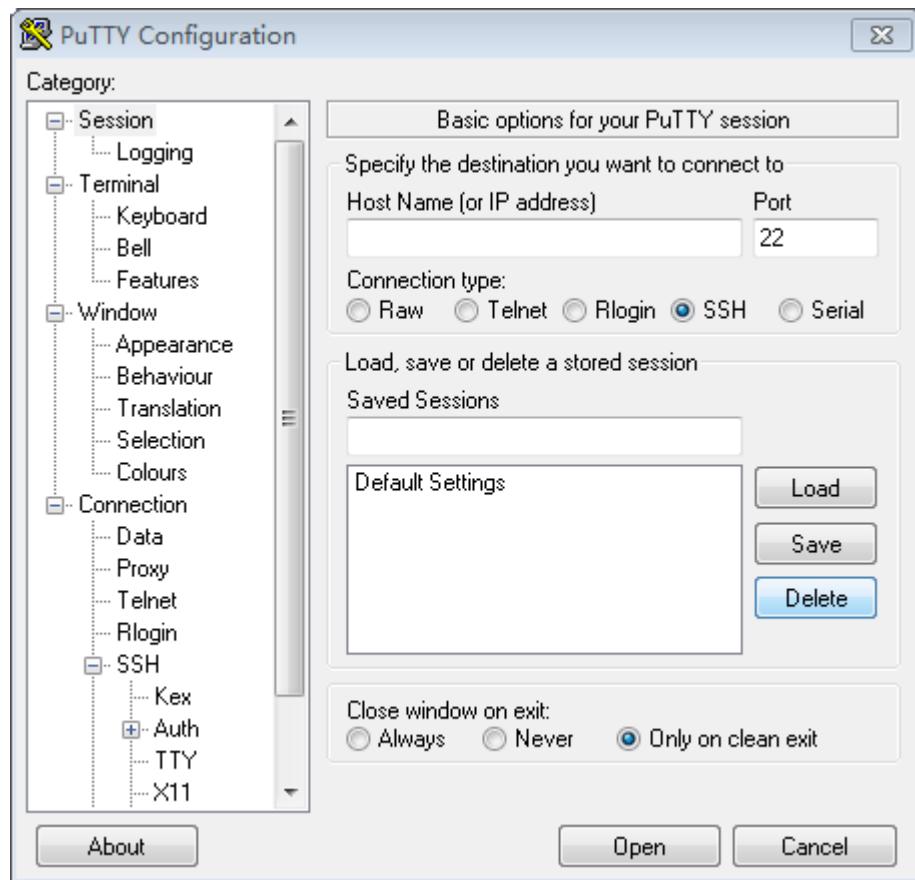
- This document uses the PuTTY software as an example. You can download PuTTY from chiark website.
- You are advised to use the latest version of PuTTY, otherwise you may fail to log in to the storage system.

## Procedure

**Step 1** Run the PuTTY software.

The **PuTTY Configuration** dialog box is displayed, as shown in [Figure 2-15](#).

Figure 2-15 PuTTY Configuration dialog box



**Step 2** Select **Session**. In the **Specify the destination you want to connect to** area, enter the IP address of the management network port that connects to the maintenance terminal in **Host Name (or IP address)** and set **Connection type** to **SSH**. Assume the IP address is **192.168.6.96** in this example.

**Step 3** Click **Open**. The CLI login page is displayed, as shown in the following:

```
login as: admin

Authorized users only. All activity may be monitored and reported.
Using keyboard-interactive authentication.

password:

WARNING: You have accessed the system operated by Huawei.
You are required to have a personal authorisation from the system administrator
before you use this computer. Unauthorised access to or misuse of this system is
prohibited.

For security purposes, please change the initial password and log in to the
system using the new password.
Old password:*****
New password:*****
Reenter password:*****

System Name      : Huawei.Storage
Health Status   : Normal
Running Status  : Normal
Total Capacity  : 6.240TB
SN              : XXXXX
Location        :
```

```
Product Model : XXXXX
Product Version : XXXRXXXCXX
Time           : XXXX-XX-XX/16:38:22 +08:00
admin:/>
```

 **NOTE**

- The default user name and password of the super administrator are **admin** and **Admin@storage** respectively.
- **Product Model** and **Product Version** vary with the actual device you have logged in to. The actual interface display prevails.
- You are advised to change your login password periodically in the future by executing the **change user\_password** command. This reduces the password leakage risks.
- If you forget the password of an administrator or a read-only user, contact the super administrator to run **change user** to reset the password. If you forget the password as the super administrator (**admin** by default), contact super administrator **\_super\_admin** to log in to the CLI through a serial port and run **initpasswd** to reset the password.

----End

### 2.3.7 Logging In to the CLI of the Storage System (Public Key)

When a maintenance terminal manages the storage system through the engine's management network port, you can log in to the CLI of the storage system in public key authentication mode to improve system security. This section uses PuTTY as an example to illustrate how to generate a public and private key pair and how to authenticate the public key for logging in to the CLI.

#### Prerequisites

- Only a super administrator has the permission to modify users' authentication mode for logging in to the CLI.
- Public key authentication for logging in to the CLI is configured for local users only, not for domain users.

#### Precautions

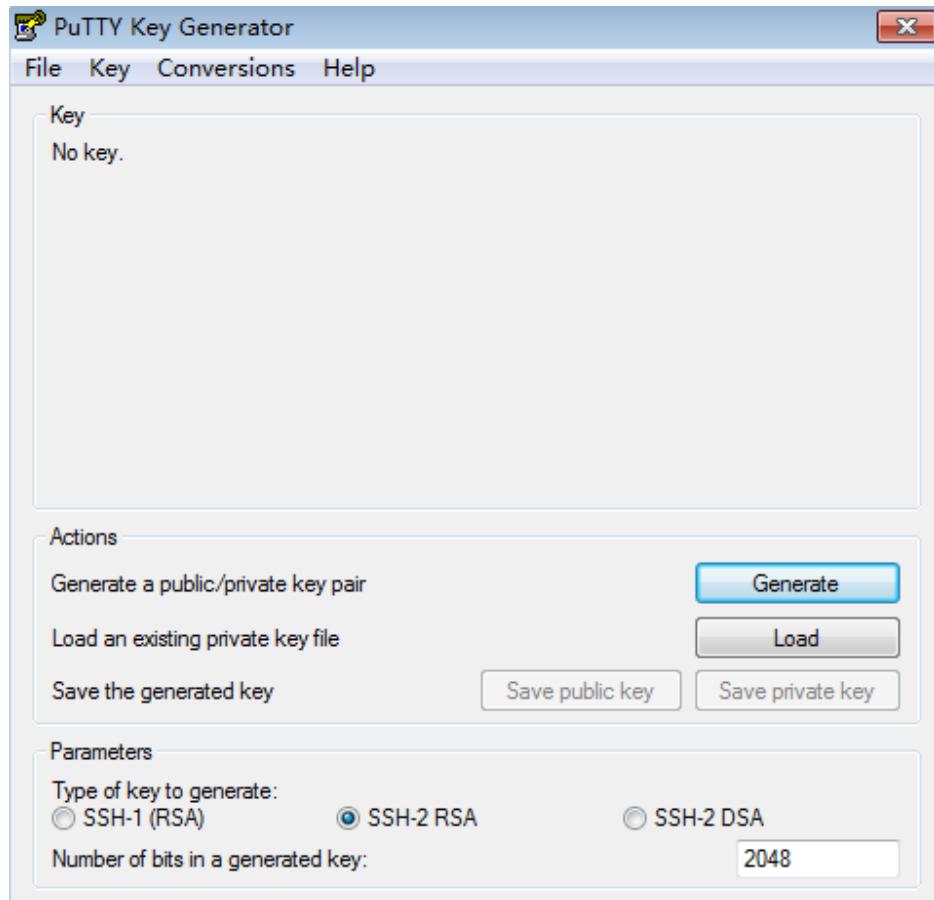
- Configure the management IP address on management network port 0 of the controller's management module for public key authentication.
- After a private key is generated, keep it secure.
- Change the public key periodically. Use the new private-public key pair for login authentication to improve system security.

#### Procedure

**Step 1** The super administrator generates a private-public key pair for a local user.

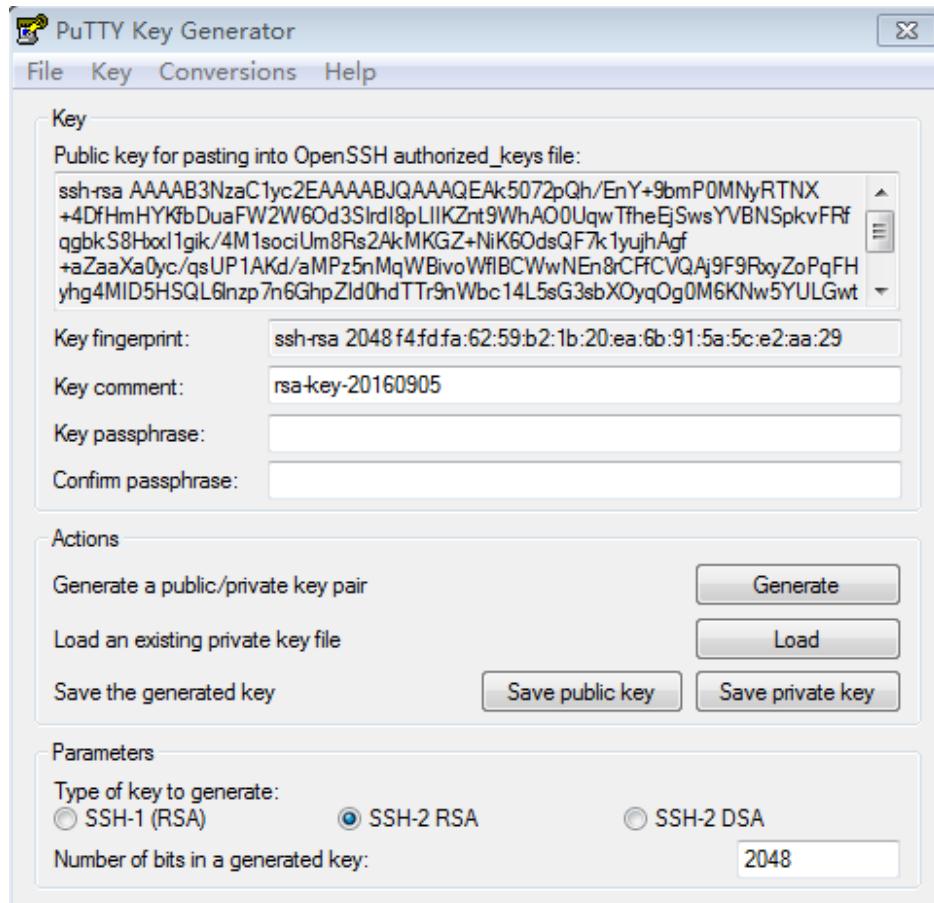
1. Run the **puttygen.exe** file.

Go to the **PuTTY Key Generator** main window, as shown in [Figure 2-16](#).

**Figure 2-16** Main window of the generator for a private-public key pair

2. In the **Parameters** area in the lower part of the page, set **Type of key to generate** to **SSH-2 RSA** or **SSH-2 DSA**, and set **Number of bits in a generated key** to an integer from 2048 to 8192.
3. Click **Generate** and move the cursor over the blank area in the lower part of the **Key** area to generate a public key.

The public key will be displayed in the area, as shown in **Figure 2-17**.

**Figure 2-17** Generating the public key

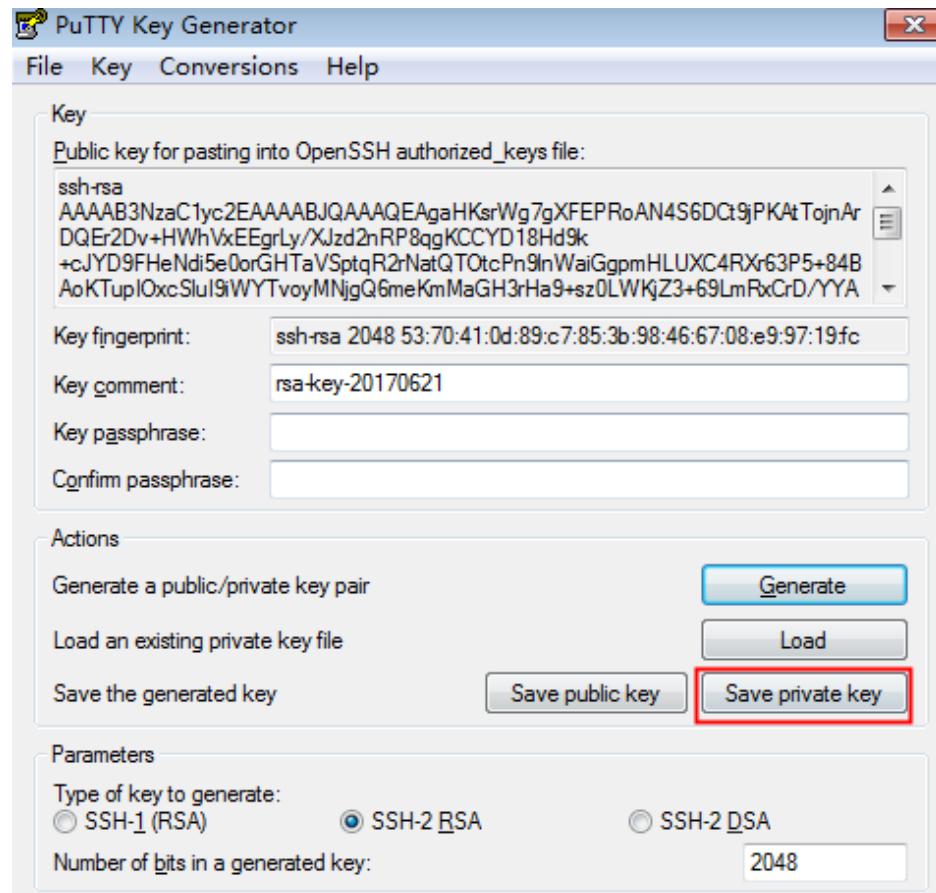
4. Copy and save the public key to the local path.
5. (Optional) In **Key passphrase**, enter a password to encrypt the private key. In **Confirm passphrase**, enter the password again.

**NOTE**

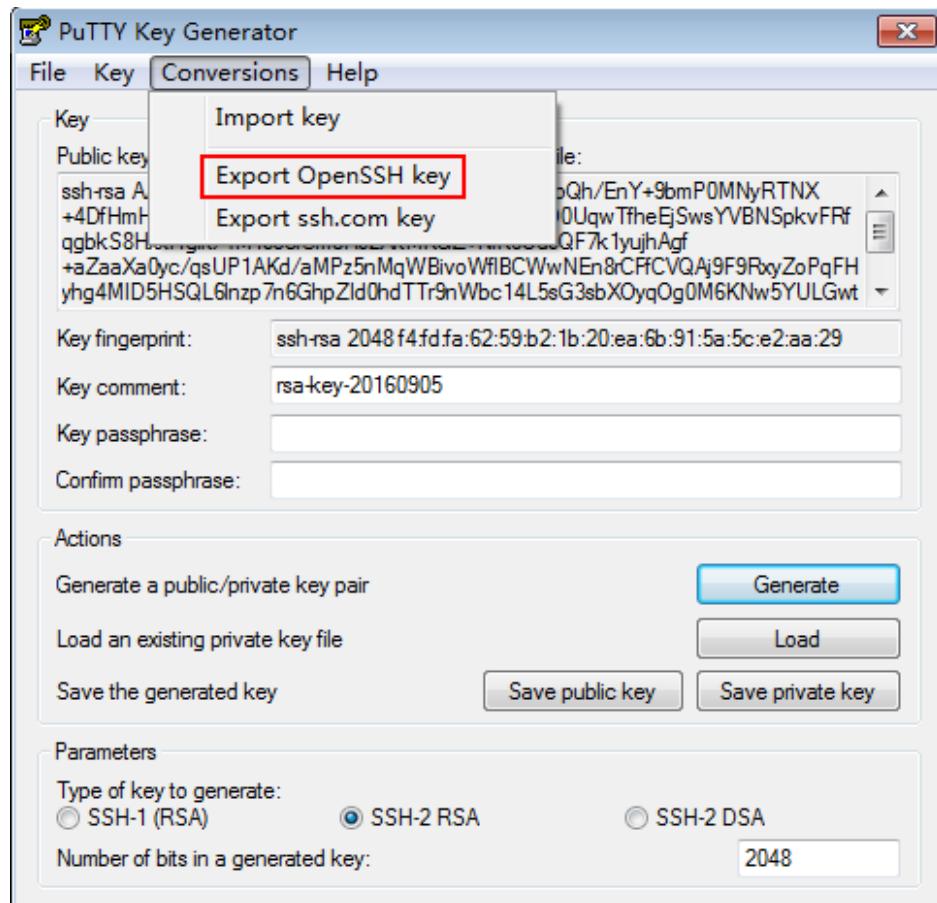
For the security of the private key file, you are advised to configure a secure password to encrypt the private key file.

6. The method to generate the private key file varies with the tool used to log in to the CLI.
  - If you use PuTTY to log in to the CLI, click **Save private key** and save the private key file to the local path, as shown in [Figure 2-18](#).

**Figure 2-18** Generating the private key



- If you use the other tools to log in to the CLI, choose **Conversions > Export OpenSSH key** and save the private key file to the local path, as shown in [Figure 2-19](#).

**Figure 2-19** Generating the private key

**Step 2** The super administrator modifies the login authentication mode of local users.

1. Log in to the CLI of the storage system as the super administrator.
2. Run the **change user\_ssh\_auth\_mode general user\_name=test123 auth\_mode=publickey** command to modify users' modification mode to **public key**. **user\_name** indicates the user name of the login authentication mode to be modified.
3. Copy the locally saved public key to **Public key** on the CLI as instructed, and press **Enter**.

After executing the command successfully, users map the private key to the public key to log in to the CLI.

```
admin:/>change user_ssh_auth_info general user_name=test123
auth_mode=publickey
CAUTION:Only public keys generated using the SSH-2 RSA/DSA encryption
algorithm and using keys whose lengths range from 2048 to 8192 bits are
supported.
Public key:ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQPLuhb/
KuHbyZi1n7yX6N3v5KG0JX8XdDnX0dfhN4yP7V
+WXeqRt93YGepnsxIuvve1QCms3jxt8uy2kDMwRY6opLRV2qh5QCk1M54owpdnjwphs1g2oKyddt5i
Z7x10svZU7gfR2qP4WgGI81Ba9rA8bQ1ZWOd
+mw6OJ80Wey37FcYzwnJpRNciTWfg2ju2sQuuvmtmum8hALQu930LbRWmTTtP33IAW/
a1LMXjeEj49yhAAfL50XVvyGMvDi3UFZJmWUZMF6eAG8joSiM50K8QuW7YUzW43t1LAXfGa7wBsp2u
6HvckMXxzyr/3tanHkc1nuGZ55+Byw9mbnNn2Z root@Storage
Command executed successfully.
```

**Step 3** Local users configure PuTTY and log in to the storage system.

1. Start PuTTY.
2. Go to the **PuTTY Configuration** dialog box.
3. Click **Session**. In the right pane, type the IP address of a storage system's management network port in the **Host Name (or IP address)** text box. Set **Port** and **Connection type** to **22** and **SSH** respectively.
4. Choose **Connection > Data**. In the **Login details** text box in the right pane, type the user name of the login authentication mode to be modified.
5. Choose **Connection > SSH > Auth**. In the right pane, click **Browse**. Select and open the locally saved private key file.
6. Click **Open** to log in to the CLI.

 **NOTE**

If the password of the private key is encrypted in **Step 1.5**, type the password when logging in to the CLI, and then press **Enter**.

Using username "test123".

Authorized users only. All activities may be monitored and reported.

Authenticating with public key "imported-openssh-key"

Passphrase for key "imported-openssh-key":

Last login: XX XX XX XX:XX:XX XXXX from 192.168.18.158

WARNING: You have accessed the system.

You are required to have a personal authorisation from the system administrator before you use this computer. Unauthorised access to or misuse of this system is prohibited.

System Name : Huawei.Storage

Health Status : Normal

Running Status : Normal

Total Capacity : 4.247TB

SN : XXXXXXXXXXXX

Location :

Product Model : XXXX

Product Version : VX00R00XC00

Time : XXXX-XX-XX/XX:XX:XX UTC+08:00

Patch Version :

test123:/>

----End

## Follow-up Procedure

To modify a user's login authentication mode to the **Username+Password** mode, run the **change user\_ssh\_auth\_mode general user\_name=test123 auth\_mode=password** command and use the original password to log in to the CLI of a storage system.

## 2.4 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 to report the alarm notification and configuration data of storage systems.

## 2.4.1 Logging In to the eService Client

This section explains how to log in to eService Client.

### Prerequisites

eService 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**.

**NOTE**

Use the default password to log in to eService. The default administrator password is **Admin@123**.

#### Step 3 (Optional) Change the login password.

1. Click **OK** in the dialog box that is displayed upon the first login indicating **Please change the default password upon the first login**.  
**Change Password** is displayed.
2. Enter the old password in **Old Password** and the new password in **New Password** and click **OK**.  
**Successfully changed the password** is displayed.

**NOTE**

- The password must contain 8 to 32 characters including case-sensitive letters and special characters. The new password must be different from the default password.
- The password validity period is six months. Please change the password within the specified period.

3. After the password is changed, the login dialog box is displayed again. In the dialog box that is displayed, select **Language**, enter the password in **Administrator Password**, and click **Log In**.

**NOTE**

The account is locked after incorrect passwords are entered for five consecutive times. It will be unlocked 5 minutes later.

----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.

## 2.4.2 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 the SmartKit.

### Context

- After the SmartKit is installed, the background programs in ToolStore keep running and access the technical support website, obtaining upgrading information about the 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 the SmartKit as an operating system administrator.

### Procedure

**Step 1** Run SmartKit on the maintenance terminal.



**Step 2** and **Step 3** are dedicated to SmartKit running on mid-range and entry-level storage devices. In scenarios where SmartKit is running on SVP environments of high-end storage devices, a message will be displayed prompting you to enter the account and log in.

**Step 2** (Optional) If you use SmartKit for the first time, a usage guide page is displayed introducing major functions of SmartKit.

1. Click **Check the tool operation guide**, a page is displayed in your browser listing the corresponding documents related to SmartKit. You can select a document to view.
2. Click **Next**, major functions of **ToolStore** are displayed on the usage guide page.
3. Click **Next**, major functions of **Scenario-based Task** are displayed on the usage guide page.
4. Click **Close**. The **Activating** page is displayed.

**Step 3** Activate SmartKit.

1. In the **Please select a location** drop-down list, select your location.
2. Select your identity.
3. Select whether to activate ToolStore.
  - Select **Activating** and enter the account and password for logging in to Huawei support website, and then click **Activating Store**.
  - Select **Not activate**. If you want to use ToolStore, activate it on the ToolStore page.



If you select **Not activate**, you will log in to SmartKit as a visitor and cannot use ToolStore.

4. Click **OK**. The **Operation Safety Precautions** page is displayed.
5. Select your location. You can click **Download** to download the *Authorization for Accessing the Customer's Network for Operation and Processing Data*.
6. Read the safety precautions carefully and click **Close**.

----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	<p>On the maintenance terminal, check whether SmartKit tools have been installed.</p> <ul style="list-style-type: none"><li>● Collect Device Archives</li><li>● Information Collection</li><li>● Disk Health Analysis</li><li>● Inspection</li><li>● Patch Tool</li></ul> <p><b>NOTE</b></p> <p>If SmartKit has not been installed, log in to <a href="http://enterprise.huawei.com">http://enterprise.huawei.com</a>, search <b>SmartKit</b>, and download the installation package and operation guide of the corresponding version. Follow instructions in the operation guide to install tools.</p>
Checking the installation and configuration of eService	<p>On the maintenance terminal, check whether eService has been installed and an appropriate alarm policy has been configured.</p> <p><b>NOTE</b></p> <p>If eService has not been installed, log in to <a href="http://enterprise.huawei.com">http://enterprise.huawei.com</a>, search <b>eService</b>, and download the installation package and operation guide of the corresponding version. Follow instructions in the operation guide to install tools.</p>

Maintenance Item	Operation
Checking the alarm policy configuration	<p>On DeviceManager, check whether the alarm policy has been configured.</p> <ul style="list-style-type: none"><li>● Email notification</li><li>● SM notification</li><li>● System notification</li><li>● Alarm dump</li><li>● Trap IP address management</li><li>● USM user management</li><li>● Alarm masking</li><li>● Syslog notification</li></ul> <p><b>NOTE</b></p> <p>If it has not been configured, see section <b>Configuring Alarm Handling Policies</b> of the <i>Installation Guide</i> of the corresponding product model.</p>

**Table 3-2** Daily maintenance items

Maintenance Item	Operation
Checking and handling alarms	<p>Log in to DeviceManager or use the alarm reporting mode that has been configured to view alarms and handle the alarms in a timely manner based on the suggestions.</p> <p><b>NOTE</b></p> <p>If an alarm still exists, use SmartKit tools to collect relevant information and contact Huawei technical support.</p>

**Table 3-3** Weekly maintenance items

Maintenance Item	Operation
Checking storage devices	<p>On a maintenance terminal, use the tool <b>Inspection</b> of SmartKit to perform checks.</p> <ul style="list-style-type: none"><li>● Hardware status</li><li>● Software status</li><li>● Value-added services</li><li>● Alarm check</li></ul> <p><b>NOTE</b></p> <p>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.</p>

Maintenance Item	Operation
Checking the equipment room environment	<p>Check the equipment room environment according to <a href="#"><b>4.2.2.1 Check Method</b></a>.</p> <p><b>NOTE</b></p> <p>If the equipment room environment cannot meet the requirements, adjust the environment in a timely manner based on the related specifications.</p>
Checking the rack environment	<p>Check whether the rack environment meets requirements in section <a href="#"><b>4.2.2.8 Checking Racks</b></a>.</p> <p><b>NOTE</b></p> <p>If the rack environment cannot meet the requirements, adjust the environment accordingly in a timely manner.</p>

# 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 Tools](#)
- [4.2 Manual Inspection](#)
- [4.3 Collecting Storage System Information](#)

## 4.1 Inspection Using Tools

This section describes the inspection items that are conducted by tools. The inspection results help maintenance engineers understand the health status and potential risks of the devices and networks, and improve the emergency processing efficiency.

### 4.1.1 Inspecting a Storage Device

You can use the SmartKit or DeviceManager to inspect a storage device.

#### 4.1.1.1 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

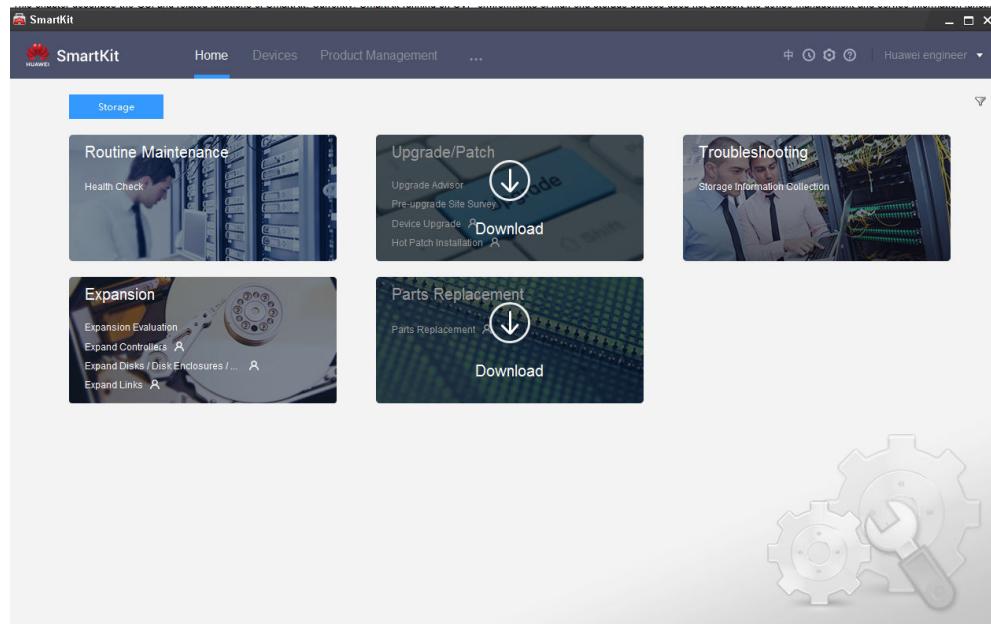
After starting **SmartKit**, you can obtain tool use instructions by clicking  in the upper right corner of the interface.

#### 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.

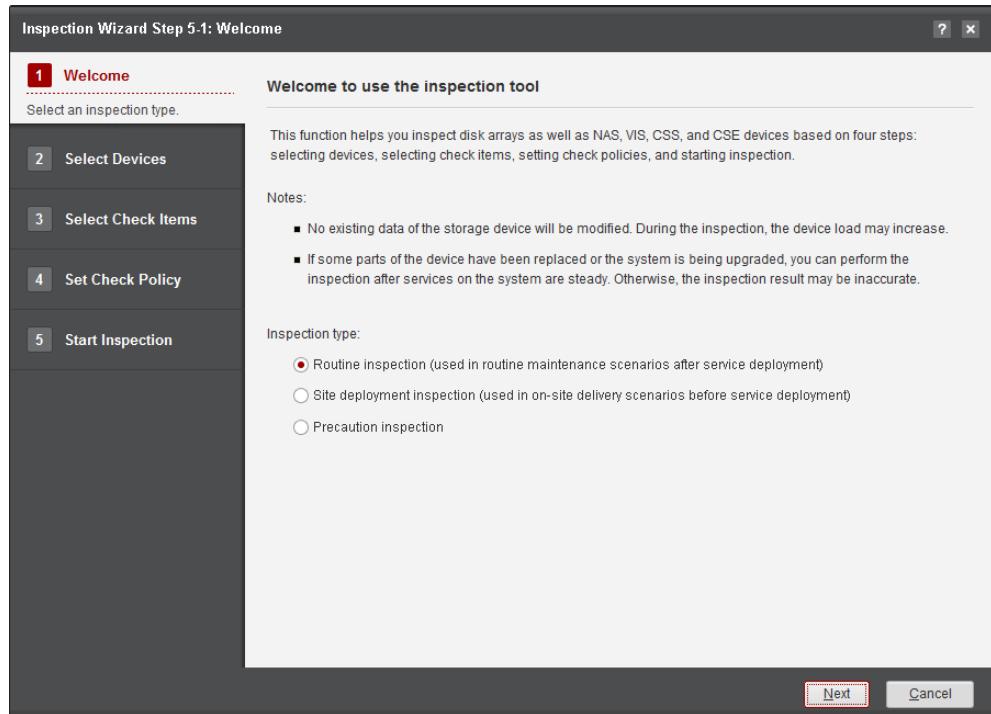
2. Enter basic information, including the IP address and proxy. In the **Add Policy** and **Select Proxy** areas, select **Specify IP Address (add a device by the IP address)** and **No Proxy**, respectively.
3. Enter configurations, including the user name, password, and port of the device. Click **Next**. In the **Login Information** area, enter the **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 ... > **MyTools** > **Storage** > **Routine Maintenance** > **Inspection**.

The **Inspection Wizard step 5-1: Welcome** dialog box is displayed.

**Figure 4-2** Page of Inspection Wizard

2. Follow the inspection wizard to set the inspection type, device to be inspected, check items, and inspection policy. After completing the settings, start the inspection.

**NOTE**

- You can set **Inspection type** to **Routine inspection**, **Site deployment inspection** or **Precaution inspection**. Select the inspection type based on your requirement.
- The storage system can check the hardware status, software status, value-added services, and alarms.

3. In the **Inspection Wizard step 5-5: Start Inspection** dialog box, click **Finish**.

**Step 4** Check the inspection results.

- If the value of **Check result** is **Passed**, you have completed the inspection.
- If the value of **Check result** is **Not passed**, the **Information** dialog box is displayed.
  - a. Read the information in the **Information** dialog box and click **OK**.  
The **Information Collection** dialog box is displayed.
  - b. Click **Collect** to start collecting device information.
  - c. Save the collected log information and inspection result and contact Huawei technical engineers.

----End

#### 4.1.1.2 Inspection Using DeviceManager

The detailed descriptions and troubleshooting suggestions of each alarm help you identify and rectify the fault quickly.

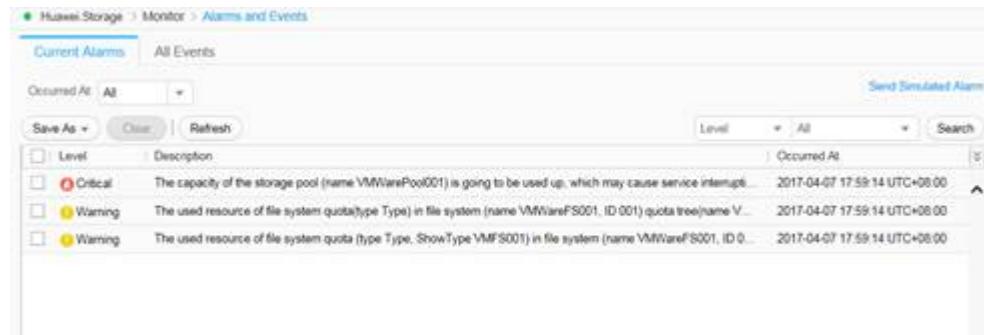
## Precautions

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  Monitor >  Alarms and Events > Current Alarms.



**Step 3** (Optional) Set **Occurred At** to **All** or **Custom** based on site requirements.

**Step 4** (Optional) Set search criteria and click **Search** to search for desired alarms.

**Step 5** Select an alarm and handle it by taking actions described in **Suggestion**.

**Step 6** (Optional) Clear alarms.

1. In the alarm list, select the alarms that you want to clear and click **Clear**.
2. In the security alert dialog box that is displayed, click **OK**.
3. In the **Execution Result** dialog box that is displayed, click **Close**.

**Step 7** (Optional) Export alarms.

Click **Save As** > **Save All** or select the alarms that you want to export and click **Save As** > **Save Selected**. In the dialog box that is displayed, perform operations as prompted.

**Step 8** (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

### 4.1.2 Inspecting a Switch (OceanStor 2000, 5000, and 6000 Series)

If SmartKit is not installed, you can use the command-line interface (CLI) to check the health and operating status of a switch.

## Context

To query switch information, you must use the serial port to log in to the CLI and run required commands. You can use a terminal program (such as PuTTY) to log in to the CLI of the switch.

### NOTE

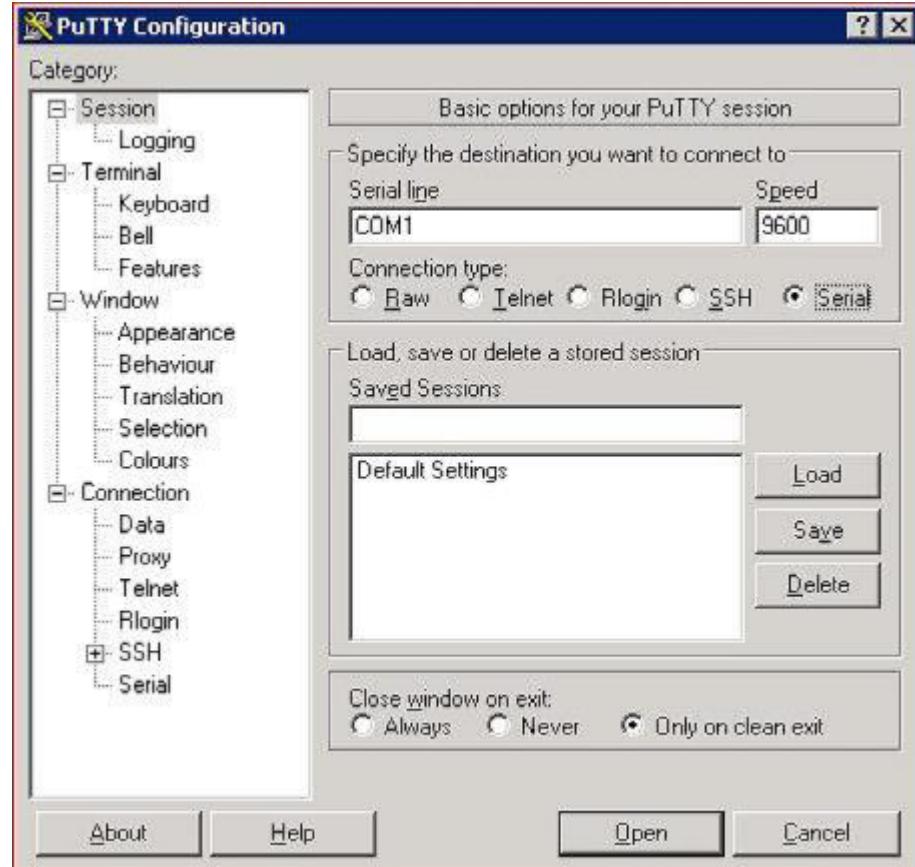
- This section uses PuTTY as an example. You can download PuTTY from chiark website.
- An earlier version of PuTTY may cause a login failure. Therefore, you are advised to use PuTTY of the latest version.

## Procedure

### Step 1 Run PuTTY.

The **PuTTY Configuration** dialog box is displayed, as shown in [Figure 4-3](#).

**Figure 4-3** PuTTY Configuration dialog box



### Step 2 Set Connection type to Serial and Speed to 9600.

### Step 3 Click Open, and log in to the serial port.

### NOTE

You can set a login password at your first login and use the password for following logins.

**Step 4** Run the **display health** command to check switch health status. You can use this command to check device health status, including information about the device temperature, power supply, fan, CPU and memory usage, and storage media usage.

```
<HUAWEI>display health
Power:
-----
Slot PowerNo Present Mode State      Current Voltage ActualPower RatedPower
                           (Ampere)   (Volt)    (Watts)     (Watts)
-----
1     PWR1      YES     AC NotSupply 0.0        0.0       0       350
      PWR2      YES     AC Supply   8.0        12.1      97       350
-----

Fan:
-----
Slot FanID     FanNum   Status      Speed      Mode     Airflow Direction
-----
1     FAN1      [1-2]    Normal     50%(8750)   Auto    Back-to-Front
      1          8800
      2          8700
      FAN2      [1-2]    Normal     50%(8800)   Auto    Back-to-Front
      1          8800
      2          8800
-----
N/A:Fan not available

Temperature:
-----
Slot   Card   SensorName   Status      Major   Current
                           (Celsius) (Celsius)
-----
1     -       Outlet-1    NORMAL     61       42
      -       Intake-1   NORMAL     72       51
      -       CPU        NORMAL     95       55
-----

System Memory Usage Information:
System Memory Usage at 2015-03-31 14:57:08
-----
Slot Total Memory(MB) Used Memory(MB) Used Percentage Upper Limit
-----
1     1837           740            40%          95%
-----

System CPU Usage Information:
System CPU Usage at 2015-03-31 14:57:08
-----
Slot CPU Usage      Upper Limit
-----
1     23%            95%
-----

System Disk Usage Information:
System Disk Usage at 2015-03-31 14:57:08
-----
Slot Device   Total Memory(MB) Used Memory(MB) Used Percentage
-----
1     flash:     1024           458            44%
-----
```

**Step 5** Run required commands to check the operating status of the switch, as shown in [Table 4-1](#).

**Table 4-1** Commands for checking operating status of a switch

Check Item	Command	Description
Fan status	display device fan	If <b>Status</b> is <b>Normal</b> , the fan is normal.
Power supply status	display device power	If <b>Status</b> is <b>Supply</b> , the power supply is normal.
Device temperature	display device temperature	If <b>Status</b> is <b>Normal</b> , the device temperature is normal.
CPU status	display cpu	If <b>Status</b> is <b>Non-overload</b> , the CPU is normal.
Memory usage	display memory	If <b>Status</b> is <b>Non-overload</b> , the memory usage is normal.
Data center bridging (DCB) configuration and protocol status	display dcb	If <b>PFC Status</b> and <b>ETS Status</b> is <b>SUCCEED</b> , the negotiation is successful.

----End

## Follow-up Procedure

If the health status or operating status of the switch is abnormal, contact technical support engineers.

For details about commands used for checking switch status, see the *CloudEngine 7800&6800&5800 Product Documentation*.

## 4.2 Manual Inspection

This section describes the manual inspection items, including routine inspections on the environment 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.

### Precaution

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  Monitor >  Alarms and Events > Current Alarms.

**Step 3** (Optional) Set Occurred At to All or Custom based on site requirements.

**Step 4** (Optional) Set search criteria and click Search to search for desired alarms.

**Step 5** Select an alarm and handle it by taking actions described in Suggestion.

**Step 6** (Optional) Clear alarms.

1. In the alarm list, select the alarms that you want to clear and click Clear.
2. In the security alert dialog box that is displayed, click OK.
3. In the Execution Result dialog box that is displayed, click Close.

**Step 7** (Optional) Export alarms.

Click Save As > Save All or select the alarms that you want to export and click Save As > Save Selected. In the dialog box that is displayed, perform operations as prompted.

**Step 8** (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 under 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 4-2](#) lists the environment check items. For the check criteria, see [4.2.2.2 Check Criteria](#).

**Table 4-2** Environment check items

Item	Check Method
Temperature, humidity, and altitude	Read the thermometer, and hygrometer, and barometer in the equipment room.

Item	Check Method
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.
Internal rack environment	<ul style="list-style-type: none"><li>● 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.</li><li>● Verify that labels are clearly marked and securely attached.</li><li>● Verify that vacant slots are covered with filler panels.</li><li>● 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.</li><li>● Verify that signal cables are fully plugged into appropriate device ports.</li><li>● 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.</li><li>● Verify that two groups of power cables are available for redundancy.</li><li>● Verify that one end of each network cable or optical fiber is fully plugged into a storage device host port and the other end into an application server port or a switch port.</li><li>● Verify that one end of each management network cable is fully plugged into a storage device management network port and the other end is connected to the network where the maintenance terminal resides.</li></ul>

## 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 Temperature, Humidity, and Altitude (OceanStor 2000, 5000 and 6000 Series)

Temperature, humidity, and altitude requirements must be met so that storage systems can correctly work or be properly preserved.

**Table 4-3** lists the temperature, humidity, and altitude requirements of the storage systems.

**Table 4-3** Temperature, humidity, and altitude requirements of storage systems

Parameter	Condition	Requirement
Temperature	Operating temperature	<ul style="list-style-type: none"><li>● 5°C to 40°C (41°F to 104°F) when the altitude is between -60 m and +1800 m (-196.85 ft. and +5905.51 ft.)</li><li>● At altitudes between 1800 m and 3000 m (5905.51 ft. and 9842.52 ft.), the temperature drops by 1°C (1.8°F) for 220 m (721.78 ft.) of altitude increase.</li></ul>
	Temperature variation in the operating environment	1°C (1.8°F)/min
	Non-operating ambient temperature	-40°C to +70°C (-40°F to +158°F)
	Storage temperature (during transportation and storage with packages)	-40°C to +70°C (-40°F to +158°F)
Humidity	Operating humidity	10% RH <sup>a</sup> to 90% RH
	Non-operating ambient humidity	5% RH to 95% RH
	Maximum humidity variation	10%/h
	Storage humidity (during transportation and storage with packages)	5% RH to 95% RH
Altitude	Operating altitude of disks	<ul style="list-style-type: none"><li>● HDDs: -304.8 m to +3048 m (-1000 ft. to +10000 ft.)</li><li>● SSDs: -305 m to +3048 m (-1000.66 ft. to +10000 ft.)</li></ul>
	Non-operating altitude of disks	<ul style="list-style-type: none"><li>● HDDs: -305 m to +12192 m (-1000.66 ft. to +40000 ft.)</li><li>● SSDs: -305 m to +12192 m (-1000.66 ft. to +40000 ft.)</li></ul>
a: relative humidity (RH)		

#### 4.2.2.2.2 Temperature and Humidity (OceanStor 18000 Series)

The requirements of the storage system on temperature and humidity vary depending on the altitude at which the storage systems reside.

**Table 4-4** lists the requirements of the storage system on temperature and humidity.

**Table 4-4** Requirements on ambient temperature and humidity

Parameter	Condition	Requirement
Temperature	Operating temperature	<ul style="list-style-type: none"><li>● 5°C to 35°C (41°F to 95°F) when the altitude is below 1800 m (5905.51 ft)</li><li>● 5°C to 30°C (41°F to 86°F) when the altitude ranges from 1800 m to 3000 m (5905.51 ft to 9842.52 ft)</li></ul>
	Temperature variation in the operating environment	10°C/h (18°F /h)
	Non-operating temperature	-40°C to 60°C (-40°F to 140°F)
	Temperature variation in the non-operating environment	10°C/h (18°F /h)
	Storage temperature (during transportation and storage with packages)	-40°C to 60°C (-40°F to 140°F)
Humidity	Humidity	10% RH <sup>a</sup> to 90% RH
	Storage humidity	5% RH to 95% RH
	Non-operating humidity	5% RH to 95% RH
	Maximum humidity variation	25%/h

a: relative humidity (RH)

#### 4.2.2.2.3 Vibration and Shock (OceanStor 2000 Series)

Vibration and shock requirements must be met so that storage systems can work correctly or be properly preserved.

**Table 4-5** shows the vibration and shock requirements of storage systems.

**Table 4-5** Vibration and shock requirements of storage systems

Parameter	Requirement
Operating vibration	5 to 350 Hz, PSD: 0.0002 g <sup>2</sup> /Hz, 350 to 500 Hz, -3 dB, 0.3 Grms, axial direction: 3 axes

Parameter	Requirement
Non-operating vibration	10 to 500 Hz, 1.49 Grms, 3 axes, 15 min/axis PSD: <ul style="list-style-type: none"><li>● 10 HZ@0.1g<sup>2</sup>/HZ</li><li>● 20 HZ@0.1g<sup>2</sup>/HZ</li><li>● 50 HZ@0.004g<sup>2</sup>/HZ</li><li>● 100 HZ@0.001g<sup>2</sup>/HZ</li><li>● 500 HZ@0.001g<sup>2</sup>/HZ</li></ul>
Non-operating shock	Half sine, 70 Gs/2 ms, 1 shock/face, total 6 faces

#### 4.2.2.2.4 Vibration and Shock (OceanStor 5000 and 6000 Series)

Vibration and shock requirements must be met so that storage systems can correctly work or be properly preserved.

**Table 4-6** shows the vibration and shock requirements of storage systems.

**Table 4-6** Vibration and shock requirements of storage systems

Parameter	Requirement
Operating vibration	5 to 350 Hz, PSD: 0.0002 g <sup>2</sup> /Hz, 350 to 500 Hz, -3 dB, 0.3 Grms, 3 axes, 15min/axis
Non-operating vibration	10 to 500 Hz, 1.49 Grms, 3 axes, 15 min/axis PSD: <ul style="list-style-type: none"><li>● 10 HZ@0.1g<sup>2</sup>/HZ</li><li>● 20 HZ@0.1g<sup>2</sup>/HZ</li><li>● 50 HZ@0.004g<sup>2</sup>/HZ</li><li>● 100 HZ@0.001g<sup>2</sup>/HZ</li><li>● 500 HZ@0.001g<sup>2</sup>/HZ</li></ul>
Non-operating shock	Half sine, 70 Gs/2 ms, 1 shock/face, total 6 faces

#### 4.2.2.2.5 Vibration and Shock (OceanStor 18000 Series)

Vibration and shock requirements must be met so that storage systems can correctly work or be properly preserved.

**Table 4-7** shows the vibration and shock requirements of storage systems.

**Table 4-7** Vibration and shock requirements of storage systems

Parameter	Requirement
Operating variation (random vibration)	5 Hz to 10 Hz: +12 dB/Oct; 10 Hz to 50 Hz: 0.04 m <sup>2</sup> /s <sup>3</sup> ; 50 Hz to 100 Hz: -12 dB/Oct
Operating variation (sinusoidal vibration)	5 Hz to 9 Hz: 1.2 mm; 9 Hz to 200 Hz: 4 m/s <sup>2</sup>
Operating shock	Peak acceleration: 30 m/s <sup>2</sup> ; pulse duration: 11 ms
Non-operating vibration	Power spectrum density: 5 Hz to 30 Hz, 0.00052 g <sup>2</sup> /Hz; 100 Hz to 500 Hz, 0.0001 g <sup>2</sup> /Hz
Non-operating shock	8 g/15 ms (peak acceleration/pulse width)

#### 4.2.2.2.6 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 *Gaseous and Particulate Contamination Guidelines for Data Centers published in 2011* 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 *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 14664-1 Class 8:

- Each cubic meter contains not more than 3,520,000 particles that are greater than or equal to 0.5  $\mu\text{m}$ .
- Each cubic meter contains not more than 832,000 particles that are greater than or equal to 1  $\mu\text{m}$ .
- Each cubic meter contains not more than 29,300 particles that are greater than or equal to 5  $\mu\text{m}$ .

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 4-8** gives the air cleanliness classification by particle concentration.

**Table 4-8** Air cleanliness classification by particle concentration of ISO 14664-1

<b>ISO Class</b>	<b>Maximum allowable concentrations (particles/m<sup>3</sup>) for particles equal to and greater than the considered sizes shown below</b>					
-	≥ 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	2370	1020	352	83	-
Class 5	100,000	23,700	10,200	3520	832	29
Class 6	1,000,000	237,000	102,000	35,200	8320	293
Class 7	-	-	-	352,000	83,200	2930
Class 8	-	-	-	3,520,000	832,000	29,300
Class 9	-	-	-	-	8,320,000	293,000

#### 4.2.2.2.7 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 article specifies the limitation on corrosive airborne contaminants with an aim at avoiding such risks.

**Table 4-9** lists common corrosive airborne contaminants and their sources.

**Table 4-9** Common corrosive airborne contaminants and their sources

<b>Symbol</b>	<b>Sources</b>
H <sub>2</sub> S	Geothermal emissions, microbiological activities, fossil fuel processing, wood rot, sewage treatment
SO <sub>2</sub> , SO <sub>3</sub>	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 <sub>x</sub>	Automobile emissions, fossil fuel combustion, chemical industry
NH <sub>3</sub>	Microbiological activities, sewage, fertilizer manufacture, geothermal emissions, refrigeration equipment

Symbol	Sources
C	Incomplete combustion (aerosol constituent), foundry
CO	Combustion, automobile emissions, microbiological activities, tree rot
Cl <sub>2</sub> , ClO <sub>2</sub>	Chlorine manufacture, aluminum manufacture, zinc manufacture, refuse decomposition
HCl	Automobile emissions, combustion, forest fire, oceanic processes, polymer combustion
HBr, HI	Automobile emissions
O <sub>3</sub>	Atmospheric photochemical processes mainly involving nitrogen oxides and oxygenated hydrocarbons
C <sub>N</sub> H <sub>N</sub>	Automobile emissions, animal waste, sewage, tree rot

The concentration level of corrosive airborne contaminants in a data center should meet the requirements listed in the white paper entitled *Gaseous and Particulate Contamination Guidelines for Data Centers published in 2011* 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, severity level G1 per ANSI/ISA-71.04-1985
- 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 4-10**.

**Table 4-10** Gaseous corrosivity levels 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.

Severity Level	Copper Reactivity Level	Description
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 4-11](#) for the copper and silver corrosion rate requirements.

**Table 4-11** Concentration limitation of corrosive airborne contaminants in a data center

Group	Gas	Unit	Concentration
Group A	H <sub>2</sub> S	ppb <sup>a</sup>	< 3
	SO <sub>2</sub>	ppb	< 10
	Cl <sub>2</sub>	ppb	< 1
	NO <sub>2</sub>	ppb	< 50
Group B	HF	ppb	< 1
	NH <sub>3</sub>	ppb	< 500
	O <sub>3</sub>	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% of 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.

#### 4.2.2.2.8 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 4-12** lists the items and standards for checking rack conditions.

**Table 4-12** Rack condition check items and standards

Check Item	Standard
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.
Host port connection	<ul style="list-style-type: none"><li>● For <b>Ethernet</b> host ports, one end of each network cable is fully plugged into a storage device host port and the other end into an application server port or a switch port.</li><li>● For <b>Fibre Channel</b> or <b>FCoE</b> host ports, one end of each optical fiber is fully plugged into a storage device host port and the other end into an application server port or a switch port.</li></ul>
Management network port connection	One end of each management network cable is fully plugged into a storage device management network port and the other end is connected to the network where the maintenance terminal resides.

## 4.2.3 Checking Indicators

Indicators reflect the hardware working status 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 in 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 Checking Controller Enclosure Indicators

Controller enclosure indicators show the running status of the controller enclosure. By checking these indicators, you can quickly learn about the status of each component module.

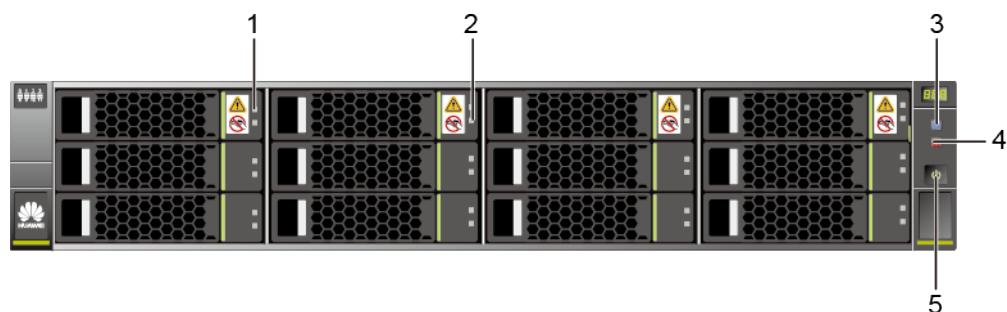
#### 4.2.3.2.1 Indicators on a 2 U Controller Enclosure (OceanStor 2600 V3 Video Surveillance Edition)

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

##### Indicators on the Front Panel

[Figure 4-4](#) shows the indicators on the front panel of a 2 U 12-disk controller enclosure.

**Figure 4-4** Indicators on the front panel of a 2 U 12-disk controller enclosure



1	Running indicator of the disk module	2	Location/Alarm indicator of the disk module
3	Location indicator of the controller enclosure	4	Alarm indicator of the controller enclosure

5	Power indicator/ Power button of the controller enclosure		
---	---	--	--

**Table 4-13** describes the indicators on the front panel of a controller enclosure.

**Table 4-13** Description of the indicators on the front panel of a controller enclosure

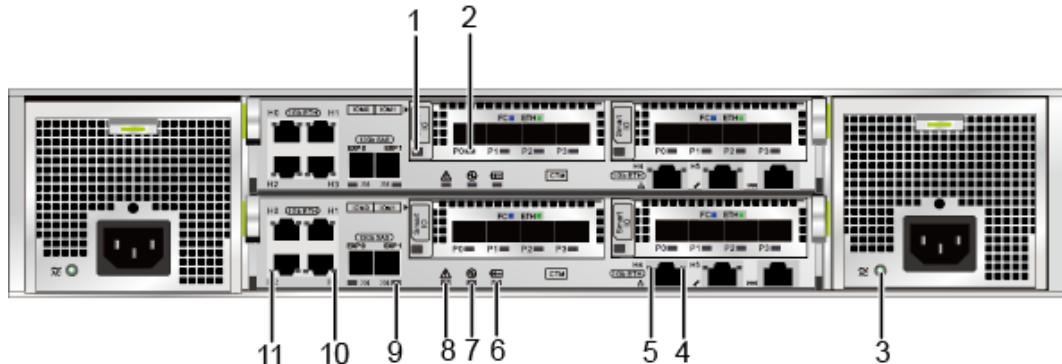
Module	No.	Indicator	Status and Description
Disk module	1	Running indicator of the disk module	<ul style="list-style-type: none"><li>● Steady green: The disk module is working correctly.</li><li>● Blinking green: Data is being read and written on the disk module.</li><li>● Off: The disk module is powered off or powered on incorrectly.</li></ul>
	2	Location/Alarm indicator of the disk module	<ul style="list-style-type: none"><li>● Steady red: The disk module is faulty.</li><li>● Blinking red: The disk module is being located.</li><li>● Off: The disk module is working correctly or hot swappable.</li></ul>
System enclosure	3	Location indicator of the controller enclosure	<ul style="list-style-type: none"><li>● Blinking blue: The controller enclosure is being located.</li><li>● Off: The controller enclosure is not located.</li></ul>
	4	Alarm indicator of the controller enclosure	<ul style="list-style-type: none"><li>● Steady red: The controller enclosure is out of service, or an alarm is generated on it.</li><li>● Off: The controller enclosure is working correctly.</li></ul>

Module	No.	Indicator	Status and Description
	5	Power indicator/Power button of the controller enclosure	<ul style="list-style-type: none"> <li>● Steady green: The controller enclosure is powered on.</li> <li>● Blinking green (0.5 Hz): The controller enclosure is being powered on.</li> <li>● Blinking green (1 Hz): The controller enclosure is in the burn-in test.</li> <li>● Blinking green (2 Hz): The controller enclosure is in the operating system boot process, or is being powered off.</li> <li>● Off: The controller enclosure is powered off or is in the standby state.</li> </ul>

## Indicators on the Rear Panel

[Figure 4-5](#) shows the indicators on the rear panel of a controller enclosure.

**Figure 4-5** Indicators on the rear panel of a controller enclosure



1	Power indicator of the interface module/Hot Swap button of the module	2	Link/Active/Mode indicator of the SmartIO port
3	Running/Alarm indicator of the power module	4	Link/Active indicator of the management network port

5	Speed indicator of the management network port	6	Running/Alarm indicator of the backup power module
7	Power indicator of the controller	8	Alarm indicator of the controller
9	Indicator of the mini SAS HD expansion port	10	Link/Active indicator of the GE electrical port
11	Speed indicator of the GE electrical port		

**Table 4-14** describes the indicators on the rear panel of a controller enclosure.

**Table 4-14** Description of the indicators on the rear panel of a controller enclosure

Module	No.	Indicator	Status and Description
Interface module	1	Power indicator of the interface module/Hot Swap button of the module	<ul style="list-style-type: none"><li>● Steady green: The interface module is running properly.</li><li>● Blinking green: The interface module receives a hot swap request.</li><li>● Steady red: The interface module is faulty.</li><li>● Off: The interface module is powered off or can be hot-swappable.</li></ul>

<b>Module</b>	<b>No.</b>	<b>Indicator</b>	<b>Status and Description</b>
	2	Link/Active/ Mode indicator of the SmartIO port	<ul style="list-style-type: none"> <li>● Blinking blue slowly (1 Hz): The interface module is working in FC mode, and the port link is down.</li> <li>● Blinking blue quickly (2 Hz): The interface module is working in FC mode, and data is being transmitted.</li> <li>● Steady blue: The interface module is working in FC mode, the port link is up, and no data is being transmitted.</li> <li>● Blinking green slowly (1 Hz): The interface module is working in ETH mode, and the port link is down.</li> <li>● Blinking green quickly (2 Hz): The interface module is working in ETH mode, and data is being transmitted.</li> <li>● Steady green: The interface module is working in ETH mode, the port link is up, and no data is being transmitted.</li> <li>● Steady red: The port is faulty.</li> <li>● Off: The port is not powered on.</li> </ul>
Power module	3	Running/ Alarm indicator of the power module	<ul style="list-style-type: none"> <li>● Steady green: The power supply is correct.</li> <li>● Blinking green: The power input is normal but the disk enclosure is powered off.</li> <li>● Steady red: The power module is faulty.</li> <li>● Off: No external power input is found.</li> </ul>
Controller	4	Link/Active indicator of the management network port	<ul style="list-style-type: none"> <li>● Steady green: The port is connected properly.</li> <li>● Blinking green: Data is being transferred.</li> <li>● Off: The port is connected abnormally.</li> </ul>
	5	Speed indicator of the management network port	<ul style="list-style-type: none"> <li>● Steady orange: Data is being transferred at the highest rate.</li> <li>● Off: The data transfer speed is lower than the highest speed.</li> </ul>
	6	Running/ Alarm indicator of the backup power module	<ul style="list-style-type: none"> <li>● Steady green: The backup power module is fully charged.</li> <li>● Blinking green (1 Hz): The backup power module is being charged.</li> <li>● Blinking green (4 Hz): The backup power module is being discharged.</li> <li>● Steady red: The backup power module is faulty.</li> </ul>

Module	No.	Indicator	Status and Description
	7	Power indicator of the controller	<ul style="list-style-type: none"> <li>● Steady green: The controller is powered on.</li> <li>● Blinking green (0.5 Hz): The controller enclosure is powered on and in the BIOS boot process.</li> <li>● Blinking green (2 Hz): The controller is in the operating system boot process, or the controller is in the power-off process.</li> <li>● Off: The controller is absent or powered off.</li> </ul>
	8	Alarm indicator of the controller	<ul style="list-style-type: none"> <li>● Steady red: An alarm is generated on the controller.</li> <li>● The Alarm indicator blinking red and the Power indicator blinking green: The controller is being located.</li> <li>● Off: The controller is working correctly.</li> </ul>
	9	Indicator of the mini SAS HD expansion port	<ul style="list-style-type: none"> <li>● Steady blue: Data is transferred to the downstream disk enclosure at the rate of 4 x 12 Gbit/s.</li> <li>● Steady green: Data is transferred to the downstream disk enclosure at the rate of 4 x 3 Gbit/s or 4 x 6 Gbit/s.</li> <li>● Steady red: The port is faulty.</li> <li>● Off: The link to the port is down.</li> </ul>
	10	Link/Active indicator of the GE electrical port	<ul style="list-style-type: none"> <li>● Steady green: The link to the application server is normal.</li> <li>● Blinking green: Data is being transferred.</li> <li>● Off: The link to the application server is down or no link exists.</li> </ul>
	11	Speed indicator of the GE electrical port	<ul style="list-style-type: none"> <li>● Steady orange: The data transfer rate between the storage system and the application server is 1 Gbit/s.</li> <li>● Off: The data transfer rate between the storage system and the application server is less than 1 Gbit/s.</li> </ul>

#### 4.2.3.2.2 Indicators on a 2 U Controller Enclosure (OceanStor 2000 Series)

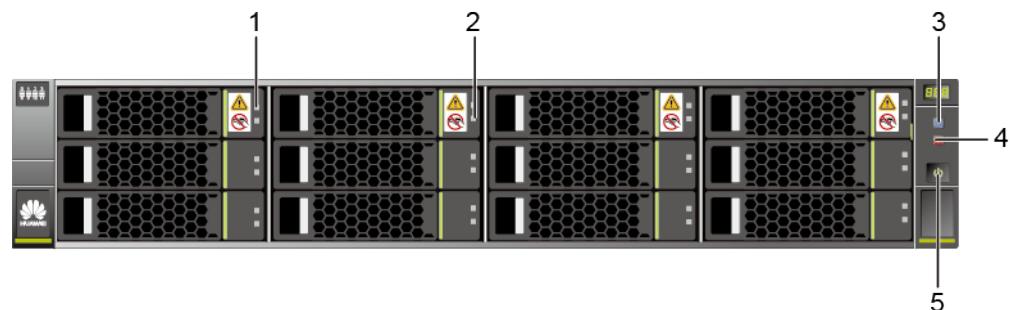
After a controller enclosure is powered on, you can check the current operating status of the controller enclosure by viewing its indicators.

#### Indicators on the Front Panel

[Figure 4-6](#) shows the indicators on the front panel of a 2 U 25-disk controller enclosure and [Figure 4-7](#) shows the indicators on the front panel of a 2 U 12-disk controller enclosure.

**Figure 4-6** Indicators on the front panel of a 2 U 25-disk controller enclosure

1	Running indicator of the disk module	2	Location/Alarm indicator of the disk module
3	Location indicator of the controller enclosure	4	Alarm indicator of the controller enclosure
5	Power indicator/ Power button of the controller enclosure		

**Figure 4-7** Indicators on the front panel of a 2 U 12-disk controller enclosure

1	Running indicator of the disk module	2	Location/Alarm indicator of the disk module
3	Location indicator of the controller enclosure	4	Alarm indicator of the controller enclosure
5	Power indicator/ Power button of the controller enclosure		

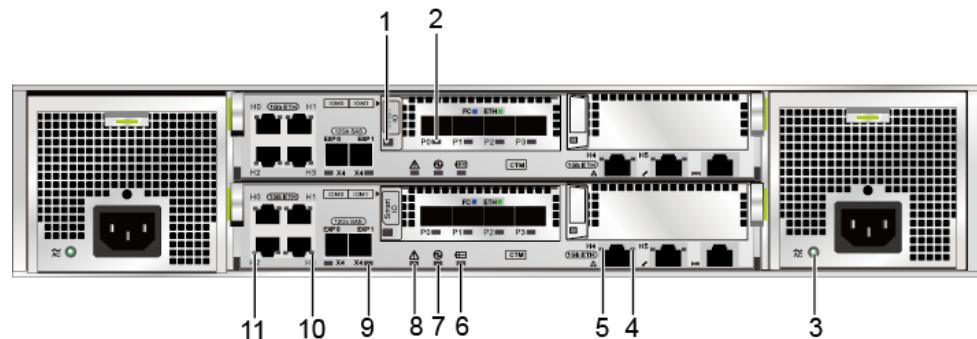
**Table 4-15** describes the indicators on the front panel of a controller enclosure.

**Table 4-15** Description of the indicators on the front panel of a controller enclosure

Module	No.	Indicator	Status and Description
Disk module	1	Running indicator of the disk module	<ul style="list-style-type: none"><li>● Steady green: The disk module is working correctly.</li><li>● Blinking green: Data is being read and written on the disk module.</li><li>● Off: The disk module is powered off or powered on incorrectly.</li></ul>
	2	Location/Alarm indicator of the disk module	<ul style="list-style-type: none"><li>● Steady red: The disk module is faulty.</li><li>● Blinking red: The disk module is being located.</li><li>● Off: The disk module is working correctly or hot swappable.</li></ul>
System subrack	3	Location indicator of the controller enclosure	<ul style="list-style-type: none"><li>● Blinking blue: The controller enclosure is being located.</li><li>● Off: The controller enclosure is not located.</li></ul>
	4	Alarm indicator of the controller enclosure	<ul style="list-style-type: none"><li>● Steady red: An alarm is generated on the controller enclosure.</li><li>● Off: The controller enclosure is working correctly.</li></ul>
	5	Power indicator/Power button of the controller enclosure	<ul style="list-style-type: none"><li>● Steady green: The controller enclosure is powered on.</li><li>● Blinking green (0.5 Hz): The controller enclosure is being powered on.</li><li>● Blinking green (1 Hz): The controller enclosure is in the burn-in test.</li><li>● Blinking green (2 Hz): The controller enclosure is in the operating system boot process, or is being powered off.</li><li>● Off: The controller enclosure is powered off or is in the standby state.</li></ul>

## Indicators on the Rear Panel

[Figure 4-8](#) shows the indicators on the rear panel of a controller enclosure.

**Figure 4-8** Indicators on the rear panel of a controller enclosure

1	Power indicator of the interface module/Hot Swap button of the module	2	Link/Active/Mode indicator of the SmartIO port
3	Running/Alarm indicator of the power module	4	Link/Active indicator of the management network port
5	Speed indicator of the management network port	6	Running/Alarm indicator of the backup power module
7	Power indicator of the controller	8	Alarm indicator of the controller
9	Indicator of the mini SAS HD expansion port	10	Link/Active indicator of the GE electrical port
11	Speed indicator of the GE electrical port		

**Table 4-16** describes the indicators on the rear panel of a controller enclosure.

**Table 4-16** Description of the indicators on the rear panel of a controller enclosure

<b>Module</b>	<b>No.</b>	<b>Indicator</b>	<b>Status and Description</b>
Interface module	1	Power indicator of the interface module/Hot Swap button of the module	<ul style="list-style-type: none"> <li>● Steady green: The interface module is running properly.</li> <li>● Blinking green: The interface module receives a hot swap request.</li> <li>● Steady red: The interface module is faulty.</li> <li>● Off: The interface module is powered off or can be hot-swappable.</li> </ul>
	2	Link/Active/Mode indicator of the SmartIO port	<ul style="list-style-type: none"> <li>● Blinking blue slowly (1 Hz): The interface module is working in FC mode, and the port link is down.</li> <li>● Blinking blue quickly (2 Hz): The interface module is working in FC mode, and data is being transmitted.</li> <li>● Steady blue: The interface module is working in FC mode, the port link is up, and no data is being transmitted.</li> <li>● Blinking green slowly (1 Hz): The interface module is working in ETH mode, and the port link is down.</li> <li>● Blinking green quickly (2 Hz): The interface module is working in ETH mode, and data is being transmitted.</li> <li>● Steady green: The interface module is working in ETH mode, the port link is up, and no data is being transmitted.</li> <li>● Steady red: The port is faulty.</li> <li>● Off: The port is not powered on.</li> </ul>
Power module	3	Running/Alarm indicator of the power module	<ul style="list-style-type: none"> <li>● Steady green: The power supply is correct.</li> <li>● Blinking green: The power input is normal but the disk enclosure is powered off.</li> <li>● Steady red: The power module is faulty.</li> <li>● Off: No external power input is found.</li> </ul>
Controller	4	Link/Active indicator of the management network port	<ul style="list-style-type: none"> <li>● Steady green: The port is connected properly.</li> <li>● Blinking green: Data is being transferred.</li> <li>● Off: The port is connected abnormally.</li> </ul>
	5	Speed indicator of the management network port	<ul style="list-style-type: none"> <li>● Steady orange: Data is being transferred at the highest rate.</li> <li>● Off: The data transfer speed is lower than the highest speed.</li> </ul>

<b>Module</b>	<b>No.</b>	<b>Indicator</b>	<b>Status and Description</b>
	6	Running/ Alarm indicator of the backup power module	<ul style="list-style-type: none"> <li>● Steady green: The backup power module is fully charged.</li> <li>● Blinking green (1 Hz): The backup power module is being charged.</li> <li>● Blinking green (4 Hz): The backup power module is being discharged.</li> <li>● Steady red: The backup power module is faulty.</li> </ul>
	7	Power indicator of the controller	<ul style="list-style-type: none"> <li>● Steady green: The controller is powered on.</li> <li>● Blinking green (0.5 Hz): The controller enclosure is powered on and in the BIOS boot process.</li> <li>● Blinking green (2 Hz): The controller is in the operating system boot process, or the controller is in the power-off process.</li> <li>● Off: The controller is absent or powered off.</li> </ul>
	8	Alarm indicator of the controller	<ul style="list-style-type: none"> <li>● Steady red: An alarm is generated on the controller.</li> <li>● The Alarm indicator blinking red and the Power indicator blinking green: The controller is being located.</li> <li>● Off: The controller is working correctly.</li> </ul>
	9	Indicator of the mini SAS HD expansion port	<ul style="list-style-type: none"> <li>● Steady blue: Data is transferred to the downstream disk enclosure at the rate of 4 x 12 Gbit/s.</li> <li>● Steady green: Data is transferred to the downstream disk enclosure at the rate of 4 x 3 Gbit/s or 4 x 6 Gbit/s.</li> <li>● Steady red: The port is faulty.</li> <li>● Off: The link to the port is down.</li> </ul>
	10	Link/Active indicator of the GE electrical port	<ul style="list-style-type: none"> <li>● Steady green: The link to the application server is normal.</li> <li>● Blinking green: Data is being transferred.</li> <li>● Off: The link to the application server is down or no link exists.</li> </ul>
	11	Speed indicator of the GE electrical port	<ul style="list-style-type: none"> <li>● Steady orange: The data transfer rate between the storage system and the application server is 1 Gbit/s.</li> <li>● Off: The data transfer rate between the storage system and the application server is less than 1 Gbit/s.</li> </ul>

#### 4.2.3.2.3 Indicators on a 2 U Controller Enclosure (OceanStor 5300 V3/5500 V3)

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

##### Indicators on the Front Panel

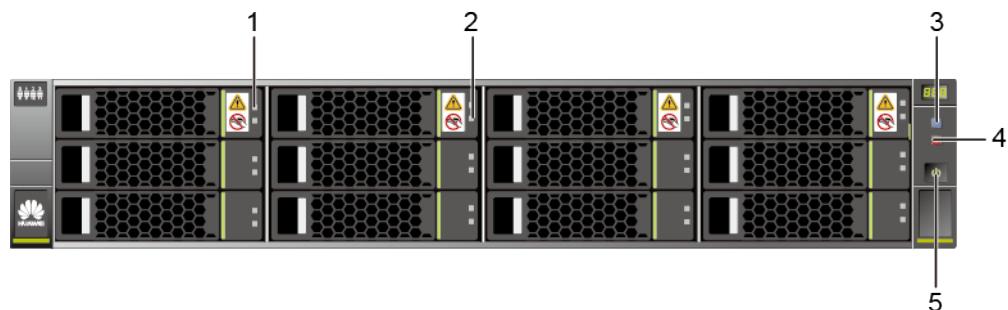
**Figure 4-9** shows the indicators on the front panel of a 2 U 25-disk controller enclosure and **Figure 4-10** shows the indicators on the front panel of a 2 U 12-disk controller enclosure.

**Figure 4-9** Indicators on the front panel of a 2 U 25-disk controller enclosure



1	Running indicator of the disk module	2	Location/Alarm indicator of the disk module
3	Location indicator of the controller enclosure	4	Alarm indicator of the controller enclosure
5	Power indicator/Power button of the controller enclosure		

**Figure 4-10** Indicators on the front panel of a 2 U 12-disk controller enclosure



1	Running indicator of the disk module	2	Location/Alarm indicator of the disk module
---	--------------------------------------	---	---

3	Location indicator of the controller enclosure	4	Alarm indicator of the controller enclosure
5	Power indicator/ Power button of the controller enclosure		

**Table 4-17** describes the indicators on the front panel of a controller enclosure.

**Table 4-17** Description of the indicators on the front panel of a controller enclosure

Module	No.	Indicator	Status and Description
Disk module	1	Running indicator of the disk module	<ul style="list-style-type: none"><li>● Steady green: The disk module is working correctly.</li><li>● Blinking green: Data is being read and written on the disk module.</li><li>● Off: The disk module is powered off or powered on incorrectly.</li></ul>
	2	Location/Alarm indicator of the disk module	<ul style="list-style-type: none"><li>● Steady red: The disk module is faulty.</li><li>● Blinking red: The disk module is being located.</li><li>● Off: The disk module is working correctly or hot swappable.</li></ul>
System subrack	3	Location indicator of the controller enclosure	<ul style="list-style-type: none"><li>● Blinking blue: The controller enclosure is being located.</li><li>● Off: The controller enclosure is not located.</li></ul>
	4	Alarm indicator of the controller enclosure	<ul style="list-style-type: none"><li>● Steady red: An alarm is generated on the controller enclosure.</li><li>● Off: The controller enclosure is working correctly.</li></ul>

Module	No.	Indicator	Status and Description
	5	Power indicator/Power button of the controller enclosure	<ul style="list-style-type: none"> <li>● Steady green: The controller enclosure is powered on.</li> <li>● Blinking green (0.5 Hz): The controller enclosure is being powered on.</li> <li>● Blinking green (1 Hz): The controller enclosure is in the burn-in test.</li> <li>● Blinking green (2 Hz): The controller enclosure is in the operating system boot process, or is being powered off.</li> <li>● Off: The controller enclosure is powered off or is in the standby state.</li> </ul>

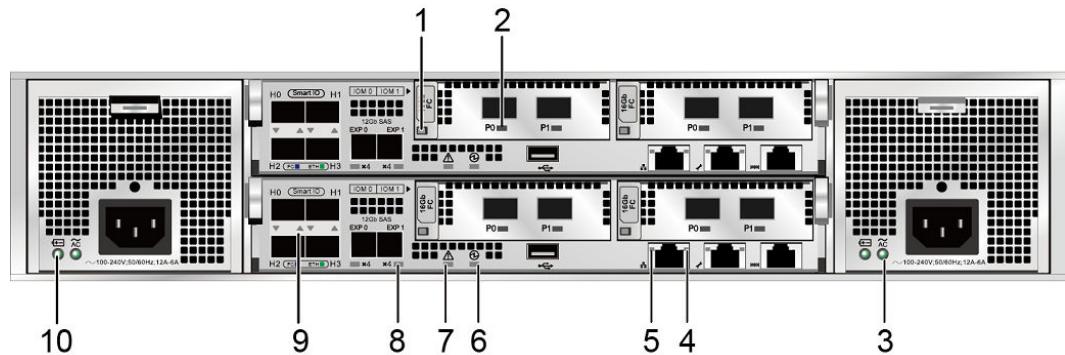
## Indicators on the Rear Panel

**Figure 4-11** shows the indicators on the rear panel of a controller enclosure.

 **NOTE**

The following figure shows the indicators on the OceanStor 5500 V3.

**Figure 4-11** Indicators on the rear panel of a controller enclosure



1	Power indicator/Hot Swap button on an interface module	2	Link/Speed indicator of the 16 Gbit/s Fibre Channel port
3	Running/Alarm indicator of the power module	4	Link/Active indicator of the management network port

5	Speed indicator of the management network port	6	Power indicator of the controller
7	Alarm indicator of the controller	8	Mini SAS HD expansion port indicator
9	Link/Active/Mode indicator of the SmartIO port	10	Running/Alarm indicator of the BBU

**Table 4-18** describes the indicators on the rear panel of a controller enclosure.**Table 4-18** Description of the indicators on the rear panel of a controller enclosure

Module	No.	Indicator	Status and Description
Interface module	1	Power indicator/Hot Swap button on an interface module	<ul style="list-style-type: none"> <li>● Steady green: The interface module is working correctly.</li> <li>● Blinking green: The interface module receives a hot swap request.</li> <li>● Steady red: The interface module is faulty.</li> <li>● Off: The interface module is not powered on or can be hot-swappable.</li> </ul>
	2	Link/Speed indicator of the 16 Gbit/s Fibre Channel port	<ul style="list-style-type: none"> <li>● Steady blue: The data transfer rate is 16 Gbit/s.</li> <li>● Blinking blue: Data is being transferred.</li> <li>● Steady green: The data transfer rate is 4 Gbit/s or 8 Gbit/s.</li> <li>● Blinking green: Data is being transferred.</li> <li>● Steady red: The port is faulty.</li> <li>● Off: The link to the port is down.</li> </ul>
Power-BBU module	3	Running/Alarm indicator of the power module	<ul style="list-style-type: none"> <li>● Steady green: The power supply is correct.</li> <li>● Blinking green: The power input is normal but the disk enclosure is powered off.</li> <li>● Steady red: The power module is faulty.</li> <li>● Off: No external power input is found.</li> </ul>
Controller	4	Link/Active indicator of the management network port	<ul style="list-style-type: none"> <li>● Steady green: The port is connected properly.</li> <li>● Blinking green: Data is being transferred.</li> <li>● Off: The port is connected abnormally.</li> </ul>

Module	No.	Indicator	Status and Description
	5	Speed indicator of the management network port	<ul style="list-style-type: none"><li>● Steady orange: Data is being transferred at the highest rate.</li><li>● Off: The data transfer speed is lower than the highest speed.</li></ul>
	6	Power indicator of the controller	<ul style="list-style-type: none"><li>● Steady green: The controller is powered on.</li><li>● The Power indicator blinking green and the Alarm indicator blinking red: The controller is being located.</li><li>● Blinking green (0.5 Hz): The controller enclosure is powered on and in the BIOS boot process.</li><li>● Blinking green (2 Hz): The controller is in the operating system boot process, or the controller is in the power-off process.</li><li>● Off: The controller is absent or powered off.</li></ul>
	7	Alarm indicator of the controller	<ul style="list-style-type: none"><li>● Steady red: An alarm is generated on the controller.</li><li>● The Alarm indicator blinking red and the Power indicator blinking green: The controller is being located.</li><li>● Off: The controller is working correctly.</li></ul>
	8	Mini SAS HD expansion port indicator	<ul style="list-style-type: none"><li>● Steady blue: Data is transferred to the downstream disk enclosure at the rate of 4 x 12 Gbit/s.</li><li>● Steady green: Data is transferred to the downstream disk enclosure at the rate of 4 x 3 Gbit/s or 4 x 6 Gbit/s.</li><li>● Steady red: The port is faulty.</li><li>● Off: The link to the port is down.</li></ul>

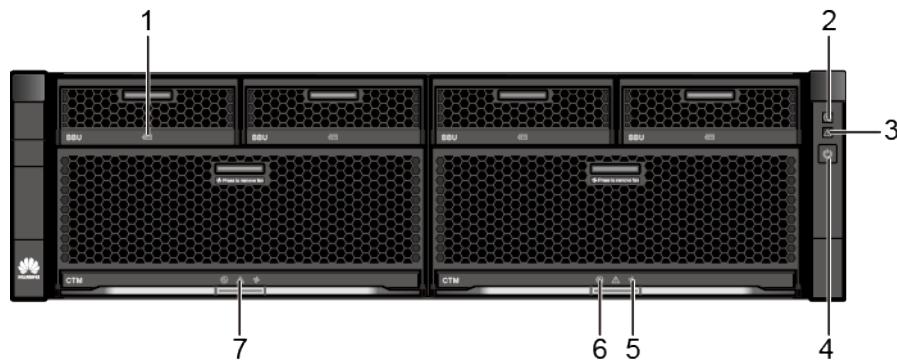
Module	No.	Indicator	Status and Description
	9 <sup>a</sup>	Link/Active/ Mode indicator of the SmartIO port	<ul style="list-style-type: none"><li>● Blinking blue slowly (1 Hz): The interface module is working in FC mode, and the port link is down.</li><li>● Blinking blue quickly (2 Hz): The interface module is working in FC mode, and data is being transmitted.</li><li>● Steady blue: The interface module is working in FC mode, the port link is up, and no data is being transmitted.</li><li>● Blinking green slowly (1 Hz): The interface module is working in ETH mode, and the port link is down.</li><li>● Blinking green quickly (2 Hz): The interface module is working in ETH mode, and data is being transmitted.</li><li>● Steady green: The interface module is working in ETH mode, the port link is up, and no data is being transmitted.</li><li>● Steady red: The port is faulty.</li><li>● Off: The port is not powered on.</li></ul>
Power-BBU module	10	Running/ Alarm indicator of the BBU	<ul style="list-style-type: none"><li>● Steady green: The BBU is fully charged.</li><li>● Blinking green (1 Hz): The BBU is being charged.</li><li>● Blinking green (4 Hz): The BBU is being discharged.</li><li>● Steady red: The BBU is faulty.</li></ul>
a: When the onboard port is a GE electrical port, the indicators on both sides of the port are the Speed indicator and Link/Active indicator. For details about these indicators, see No.4 and No.5.			

#### 4.2.3.2.4 Indicators on a 3 U Controller Enclosure

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

#### Indicators on the Front Panel

**Figure 4-12** shows the indicators on the front panel of a controller enclosure.

**Figure 4-12** Indicators on the front panel of a controller enclosure

1	Running/Alarm indicator on a BBU	2	Location indicator on the controller enclosure
3	Alarm indicator on the controller enclosure	4	Power indicator/Power button on the controller enclosure
5	Running/Alarm indicator of the fan module	6	Controller power indicator
7	Controller alarm indicator		

**Table 4-19** describes the indicators on the front panel of a controller enclosure.

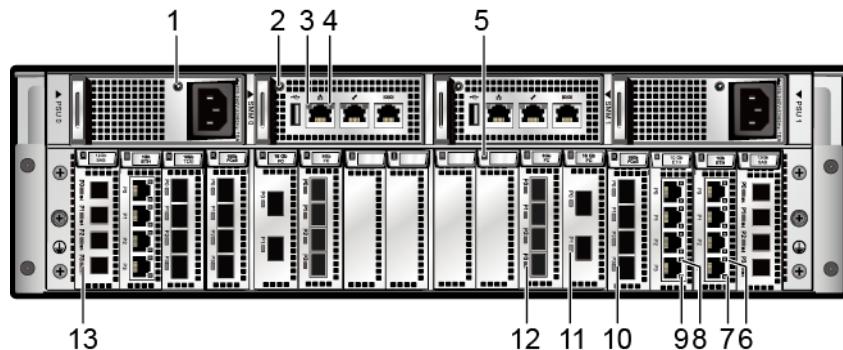
**Table 4-19** Indicators on the front panel of a controller enclosure

Module	No.	Indicator	Status and Description
BBU	1	Running/Alarm indicator on a BBU	<ul style="list-style-type: none"> <li>● Steady green: The BBU is fully charged.</li> <li>● Blinking green (1 Hz): The BBU is being charged.</li> <li>● Blinking green (4 Hz): The BBU is being discharged.</li> <li>● Steady red: The BBU is faulty.</li> </ul>
System subrack	2	Location indicator on the controller enclosure	<ul style="list-style-type: none"> <li>● Blinking blue: The controller enclosure is being located.</li> <li>● Off: The controller enclosure is not located.</li> </ul>

Module	No.	Indicator	Status and Description
Controller	3	Alarm indicator on the controller enclosure	<ul style="list-style-type: none"><li>● Steady red: An alarm about the controller enclosure is generated.</li><li>● Off: The controller enclosure is working properly.</li></ul>
	4	Power indicator/Power button on the controller enclosure	<ul style="list-style-type: none"><li>● Steady green: The controller enclosure is powered on.</li><li>● Blinking green (0.5 Hz): The controller enclosure is powered on for a short time.</li><li>● Blinking green (1 Hz): The controller enclosure is in the burn-in test.</li><li>● Blinking green (2 Hz): The controller enclosure is in the operating system boot process or in the power-off process.</li><li>● Off: The controller enclosure is powered off or powered by BBUs.</li></ul>
	5	Running/Alarm indicator of the fan module	<ul style="list-style-type: none"><li>● Steady green: Fan modules are working correctly.</li><li>● Steady red: The fan module is faulty.</li><li>● Off: Fan modules are powered off.</li></ul>
	6	Controller power indicator	<ul style="list-style-type: none"><li>● Steady green: The controller is powered on.</li><li>● Blinking green (0.5 Hz): The controller is powered on and in the BIOS boot process.</li><li>● Blinking green (2 Hz): The controller is in the operating system boot process.</li><li>● Off: The controller cannot be detected or is powered off.</li></ul>
	7	Controller alarm indicator	<ul style="list-style-type: none"><li>● Steady red: An alarm about the controller is generated.</li><li>● Off: The controller is working correctly.</li></ul>

## Indicators on the Rear Panel

Figure 4-13 shows the indicators on the rear panel of a controller enclosure.

**Figure 4-13** Indicators on the rear panel of a controller enclosure

1	Running/Alarm indicator on a power module	2	Power indicator on a management module
3	Speed indicator of the management network port	4	Link/Active indicator of the management network port
5	Power indicator/Hot Swap button on an interface module	6	Speed indicator of a GE electrical port
7	Link/Active indicator of a GE electrical port	8	Speed indicator of a GE electrical port
9	Link/Active indicator of a GE electrical port	10	Link/Speed indicator of a 10 Gbit/s FCoE port
11	Link/Speed indicator of a 16 Gbit/s Fibre Channel port	12	Link/Speed indicator of an 8 Gbit/s Fibre Channel port
13	Indicator of the mini SAS HD expansion port		

**Table 4-20** describes the indicators on the rear panel of a controller enclosure.

**Table 4-20** Indicators on the rear panel of a controller enclosure

Module	No.	Indicator	Status and Description
Power module	1	Running/ Alarm indicator on a power module	<ul style="list-style-type: none"><li>● Steady green: The power supply is normal.</li><li>● Blinking green: The power input is normal but the device is powered off.</li><li>● Steady red: The power module is faulty.</li><li>● Off: No external power input is available.</li></ul>
Management module	2	Power indicator on a management module	<ul style="list-style-type: none"><li>● Steady green: The module is working correctly.</li><li>● Blinking green: The module receives a hot swap request.</li><li>● Steady red: The module is faulty.</li><li>● Off: The module is powered off or hot swappable.</li></ul>
	3	Speed indicator of the management network port	<ul style="list-style-type: none"><li>● Steady orange: Data is being transferred at the highest rate.</li><li>● Off: The data transfer speed is lower than the highest speed.</li></ul>
	4	Link/Active indicator of the management network port	<ul style="list-style-type: none"><li>● Steady green: The port is connected properly.</li><li>● Blinking green: Data is being transferred.</li><li>● Off: The port is connected abnormally.</li></ul>
Interface module	5	Power indicator/Hot Swap button on an interface module	<ul style="list-style-type: none"><li>● Steady green: The interface module is working correctly.</li><li>● Blinking green: The interface module receives a hot swap request.</li><li>● Steady red: The interface module is faulty.</li><li>● Off: The interface module is powered off or can be hot-swappable.</li></ul>
	6	Speed indicator of a GE electrical port	<ul style="list-style-type: none"><li>● Steady orange: The data transfer rate between the controller enclosure and the application server is 1 Gbit/s.</li><li>● Off: The data transfer rate between the controller enclosure and the application server is lower than 1 Gbit/s.</li></ul>
	7	Link/Active indicator of a GE electrical port	<ul style="list-style-type: none"><li>● Steady green: The connection between the controller enclosure and the application server is correct.</li><li>● Blinking green: Data is being transferred.</li><li>● Off: The connection between the controller enclosure and the application server is incorrect.</li></ul>

Module	No.	Indicator	Status and Description
	8	Speed indicator of a 10 GE electrical port	<ul style="list-style-type: none"><li>● Steady orange: The data transfer rate between the controller enclosure and the application server is 10 Gbit/s.</li><li>● Off: The data transfer rate between the controller enclosure and the application server is lower than 10 Gbit/s.</li></ul>
	9	Link/Active indicator of a 10 GE electrical port	<ul style="list-style-type: none"><li>● Steady green: The connection between the controller enclosure and the application server is correct.</li><li>● Blinking green: Data is being transferred.</li><li>● Off: The connection between the controller enclosure and the application server is incorrect.</li></ul>
	10	Link/Speed indicator of a 10 Gbit/s FCoE port	<ul style="list-style-type: none"><li>● Steady blue: The data transfer rate between the storage system and the application server is 10 Gbit/s.</li><li>● Blinking blue: Data is being transferred.</li><li>● Steady red: The port is faulty.</li><li>● Off: The link to the port is down.</li></ul>
	11	Link/Speed indicator of a 16 Gbit/s Fibre Channel port	<ul style="list-style-type: none"><li>● Steady blue: The data transfer rate between the storage system and the application server is 16 Gbit/s.</li><li>● Blinking blue: Data is being transferred.</li><li>● Steady green: The data transfer rate between the storage system and the application server is 4 Gbit/s or 8 Gbit/s.</li><li>● Blinking green: Data is being transferred.</li><li>● Steady red: The port is faulty.</li><li>● Off: The link to the port is down.</li></ul>
	12	Link/Speed indicator of an 8 Gbit/s Fibre Channel port	<ul style="list-style-type: none"><li>● Steady blue: The data transfer rate is 8 Gbit/s.</li><li>● Blinking blue: Data is being transferred.</li><li>● Steady green: The data transfer rate is 2 Gbit/s or 4 Gbit/s.</li><li>● Blinking green: Data is being transferred.</li><li>● Steady red: The port is faulty.</li><li>● Off: The link to the port is down.</li></ul>

Module	No.	Indicator	Status and Description
	13	Indicator of the mini SAS HD expansion port	<ul style="list-style-type: none"> <li>● Steady blue: Data is transferred to the downstream disk enclosure at the rate of 4 x 12 Gbit/s.</li> <li>● Steady green: Data is transferred to the downstream disk enclosure at the rate of 4 x 3 Gbit/s or 4 x 6 Gbit/s.</li> <li>● Steady red: The port is faulty.</li> <li>● Off: The link to the port is down.</li> </ul>

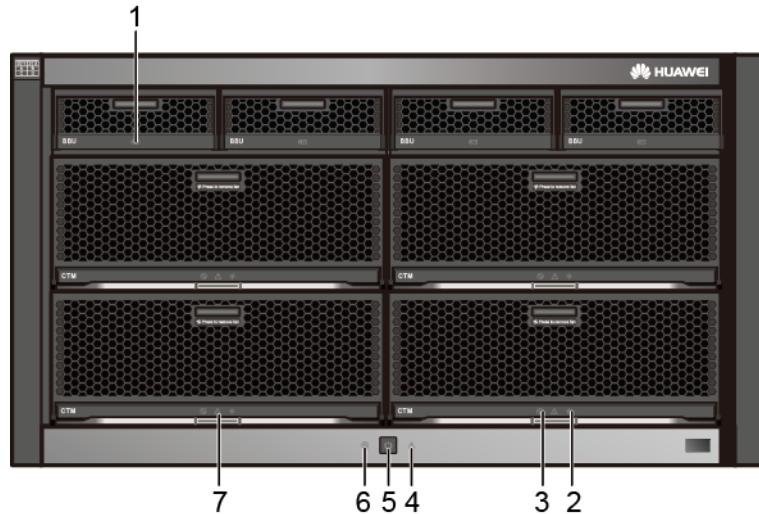
#### 4.2.3.2.5 Indicators on a 6 U Controller Enclosure

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

#### Indicators on the Front Panel

[Figure 4-14](#) shows the indicators on the front panel of a controller enclosure.

**Figure 4-14** Indicators on the front panel of a controller enclosure



1	Running/Alarm indicator on a BBU	2	Fan module Running/Alarm indicator
3	Controller power indicator	4	Alarm indicator on the controller enclosure
5	Power indicator/ Power button on the controller enclosure	6	Location indicator on the controller enclosure

7	Controller alarm indicator		
---	----------------------------	--	--

**Table 4-21** describes the indicators on the front panel of a controller enclosure.

**Table 4-21** Indicators on the front panel of a controller enclosure

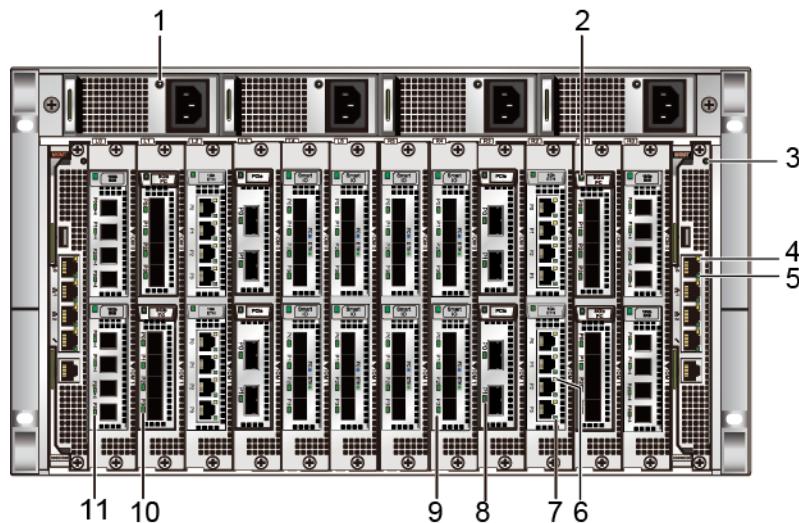
Module	No.	Indicator	Status and Description
BBU	1	Running/Alarm indicator on a BBU	<ul style="list-style-type: none"><li>● Steady green: The BBU is fully charged.</li><li>● Blinking green (1 Hz): The BBU is being charged.</li><li>● Blinking green (4 Hz): The BBU is being discharged.</li><li>● Steady red: The BBU is faulty.</li></ul>
Controller	2	Fan module Running/Alarm indicator	<ul style="list-style-type: none"><li>● Steady green: Fan modules are working correctly.</li><li>● Steady red: The fan module is faulty.</li><li>● Off: Fan modules are powered off.</li></ul>
	3	Controller power indicator	<ul style="list-style-type: none"><li>● Steady green: The controller is powered on.</li><li>● Blinking green (0.5 Hz): The controller is powered on and in the BIOS boot process.</li><li>● Blinking green (2 Hz): The controller is in the operating system boot process.</li><li>● Off: The controller cannot be detected or is powered off.</li></ul>
System subrack	4	Alarm indicator on the controller enclosure	<ul style="list-style-type: none"><li>● Steady red: An alarm about the controller enclosure is generated.</li><li>● Off: The controller enclosure is working properly.</li></ul>

Module	No.	Indicator	Status and Description
	5	Power indicator/Power button on the controller enclosure	<ul style="list-style-type: none"> <li>● Steady green: The controller enclosure is powered on.</li> <li>● Blinking green (0.5 Hz): The controller enclosure is powered on for a short time.</li> <li>● Blinking green (1 Hz): The controller enclosure is in the burn-in test.</li> <li>● Blinking green (2 Hz): The controller enclosure is in the operating system boot process, or is being powered off.</li> <li>● Off: The controller enclosure is powered off or powered by BBUs.</li> </ul>
	6	Location indicator on the controller enclosure	<ul style="list-style-type: none"> <li>● Blinking blue: The controller enclosure is being located.</li> <li>● Off: The controller enclosure is not located.</li> </ul>
Controller	7	Controller alarm indicator	<ul style="list-style-type: none"> <li>● Steady red: An alarm about the controller is generated.</li> <li>● Off: The controller is working correctly.</li> </ul>

## Indicators on the Rear Panel

[Figure 4-15](#) shows the indicators on the rear panel of a controller enclosure.

**Figure 4-15** Indicators on the rear panel of a controller enclosure



1	Running/Alarm indicator on a power module	2	Power indicator/Hot Swap button on an interface module
3	Power indicator on a management module	4	Speed indicator of the management network port
5	Link/Active indicator of the management network port	6	Speed indicator of a GE electrical port
7	Link/Active indicator of a GE electrical port	8	Link/Speed indicator of a 10 Gbit/s FCoE port
9	Link/Speed indicator of a 16 Gbit/s Fibre Channel port	10	Link/Speed indicator of an 8 Gbit/s Fibre Channel port
11	Indicator of the mini SAS HD expansion port		

**Table 4-22** describes the indicators on the rear panel of a controller enclosure.

**Table 4-22** Indicators on the rear panel of a controller enclosure

Module	No.	Indicator	Status and Description
Power module	1	Running/Alarm indicator on a power module	<ul style="list-style-type: none"> <li>● Steady green: The power supply is normal.</li> <li>● Blinking green: The power input is normal but the device is powered off.</li> <li>● Steady red: The power module is faulty.</li> <li>● Off: No external power input is available.</li> </ul>
Interface module	2	Power indicator/Hot Swap button on an interface module	<ul style="list-style-type: none"> <li>● Steady green: The interface module is working correctly.</li> <li>● Blinking green: The interface module receives a hot swap request.</li> <li>● Steady red: The interface module is faulty.</li> <li>● Off: The interface module is powered off or can be hot-swappable.</li> </ul>

Module	No.	Indicator	Status and Description
Management module	3	Power indicator on a management module	<ul style="list-style-type: none"><li>● Steady green: The module is working correctly.</li><li>● Blinking green: The module receives a hot swap request.</li><li>● Steady red: The module is faulty.</li><li>● Off: The module is powered off or hot swappable.</li></ul>
	4	Speed indicator of the management network port	<ul style="list-style-type: none"><li>● Steady orange: Data is being transferred at the highest rate.</li><li>● Off: The data transfer speed is lower than the highest speed.</li></ul>
	5	Link/Active indicator of the management network port	<ul style="list-style-type: none"><li>● Steady green: The port is connected properly.</li><li>● Blinking green: Data is being transferred.</li><li>● Off: The port is connected abnormally.</li></ul>
Interface module	6	Speed indicator of a GE electrical port	<ul style="list-style-type: none"><li>● Steady orange: The data transfer rate between the controller enclosure and the application server is 1 Gbit/s.</li><li>● Off: The data transfer rate between the controller enclosure and the application server is lower than 1 Gbit/s.</li></ul>
	7	Link/Active indicator of a GE electrical port	<ul style="list-style-type: none"><li>● Steady green: The connection between the controller enclosure and the application server is correct.</li><li>● Blinking green: Data is being transferred.</li><li>● Off: The connection between the controller enclosure and the application server is incorrect.</li></ul>
	8	Link/Speed indicator of a 10 Gbit/s FCoE port	<ul style="list-style-type: none"><li>● Steady blue: The data transfer rate between the storage system and the application server is 10 Gbit/s.</li><li>● Blinking blue: Data is being transferred.</li><li>● Steady red: The port is faulty.</li><li>● Off: The link to the port is down.</li></ul>

Module	No.	Indicator	Status and Description
	9	Link/Speed indicator of a 16 Gbit/s Fibre Channel port	<ul style="list-style-type: none"> <li>● Steady blue: The data transfer rate between the storage system and the application server is 16 Gbit/s.</li> <li>● Blinking blue: Data is being transferred.</li> <li>● Steady green: The data transfer rate between the storage system and the application server is 4 Gbit/s or 8 Gbit/s.</li> <li>● Blinking green: Data is being transferred.</li> <li>● Steady red: The port is faulty.</li> <li>● Off: The link to the port is down.</li> </ul>
	10	Link/Speed indicator of an 8 Gbit/s Fibre Channel port	<ul style="list-style-type: none"> <li>● Steady blue: The data transfer rate is 8 Gbit/s.</li> <li>● Blinking blue: Data is being transferred.</li> <li>● Steady green: The data transfer rate is 2 Gbit/s or 4 Gbit/s.</li> <li>● Blinking green: Data is being transferred.</li> <li>● Steady red: The port is faulty.</li> <li>● Off: The link to the port is down.</li> </ul>
	11	Mini SAS HD expansion port indicator	<ul style="list-style-type: none"> <li>● Steady blue: Data is transferred to the downstream disk enclosure at the rate of 4 x 12 Gbit/s.</li> <li>● Steady green: Data is transferred to the downstream disk enclosure at the rate of 4 x 3 Gbit/s or 4 x 6 Gbit/s.</li> <li>● Steady red: The port is faulty.</li> <li>● Off: The link to the port is down.</li> </ul>

#### 4.2.3.3 Checking Disk Enclosure Indicators

Disk enclosure indicators show the running status of a disk enclosure. By checking these indicators, you can quickly learn about the status of each component module.

 **NOTE**

- The 2 U disk enclosure is not supported by OceanStor 2600 V3 video surveillance edition storage system.
- The high-density disk enclosure is not supported by OceanStor 2200 V3 storage system.

##### 4.2.3.3.1 Indicators on a 2 U Disk Enclosure

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

#### Indicators on the Front Panel

**Figure 4-16** shows the indicators on the front panel of a disk enclosure.

**Figure 4-16** Indicators on the front panel of a disk enclosure

1	Running indicator of the disk module	2	Alarm/Location indicator of the disk module
3	Location indicator of the disk enclosure	4	Alarm indicator of the disk enclosure
5	Power indicator of the disk enclosure		

**Table 4-23** describes the indicators on the front panel of the disk enclosure.

**Table 4-23** Description of the indicators on the front panel of a disk enclosure

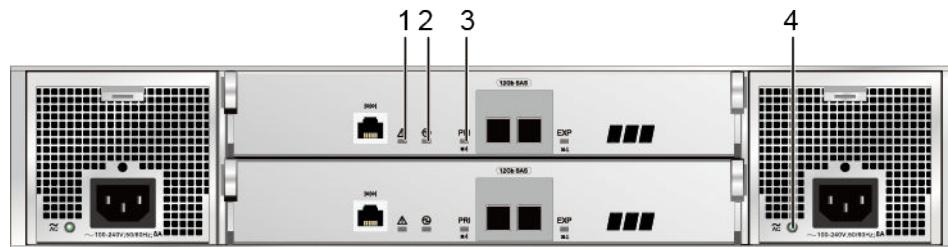
Module	No.	Indicator	Status and Description
Disk module	1	Running indicator of the disk module	<ul style="list-style-type: none"><li>● Steady green: The disk module is working correctly.</li><li>● Blinking green: Data is being read and written on the disk module.</li><li>● Off: The disk module is powered off or powered on incorrectly.</li></ul>
	2	Alarm/Location indicator of the disk module	<ul style="list-style-type: none"><li>● Steady red: The disk module is faulty.</li><li>● Blinking red: The disk module is being located.</li><li>● Off: The disk module is working correctly or hot swappable.</li></ul>
System subrack	3	Location indicator of the disk enclosure	<ul style="list-style-type: none"><li>● Blinking blue: The disk enclosure is being located.</li><li>● Off: The disk enclosure is not located.</li></ul>

Module	No.	Indicator	Status and Description
	4	Alarm indicator of the disk enclosure	<ul style="list-style-type: none"> <li>● Steady red: An alarm is generated in the disk enclosure.</li> <li>● Off: The disk enclosure is working correctly.</li> </ul>
	5	Power indicator of the disk enclosure	<ul style="list-style-type: none"> <li>● Steady green: The disk enclosure is powered on.</li> <li>● Off: The disk enclosure is powered off.</li> </ul>

## Indicators on the Rear Panel

[Figure 4-17](#) shows the indicators on the rear panel of a disk enclosure.

**Figure 4-17** Indicators on the rear panel of a disk enclosure



1	Alarm indicator of the expansion module	2	Power indicator of the expansion module
3	Indicator of the mini SAS HD expansion port	4	Running/Alarm indicator of the power module

[Table 4-24](#) describes the indicators on the rear panel of the disk enclosure.

**Table 4-24** Description of the indicators on the rear panel of a disk enclosure

Module	No.	Indicator	Status and Description
Expansion module	1	Alarm indicator of the expansion module	<ul style="list-style-type: none"> <li>● Steady red: An alarm is generated on the expansion module.</li> <li>● Off: The expansion module is working correctly.</li> </ul>

Module	No.	Indicator	Status and Description
	2	Power indicator of the expansion module	<ul style="list-style-type: none"> <li>● Steady green: The expansion module is powered on.</li> <li>● Off: The expansion module is powered off.</li> </ul>
	3	Indicator of the mini SAS HD expansion port	<ul style="list-style-type: none"> <li>● Steady blue: Data is transferred to the downstream disk enclosure at the rate of 4 x 12 Gbit/s.</li> <li>● Steady green: Data is transferred to the downstream disk enclosure at the rate of 4 x 3 Gbit/s or 4 x 6 Gbit/s.</li> <li>● Steady red: The port is faulty.</li> <li>● Off: The link to the port is down.</li> </ul>
Power module	4	Running/Alarm indicator of the power module	<ul style="list-style-type: none"> <li>● Steady green: The power supply is correct.</li> <li>● Blinking green: The power input is normal but the disk enclosure is powered off.</li> <li>● Steady red: The power supply is faulty.</li> <li>● Off: No external power input is found.</li> </ul>

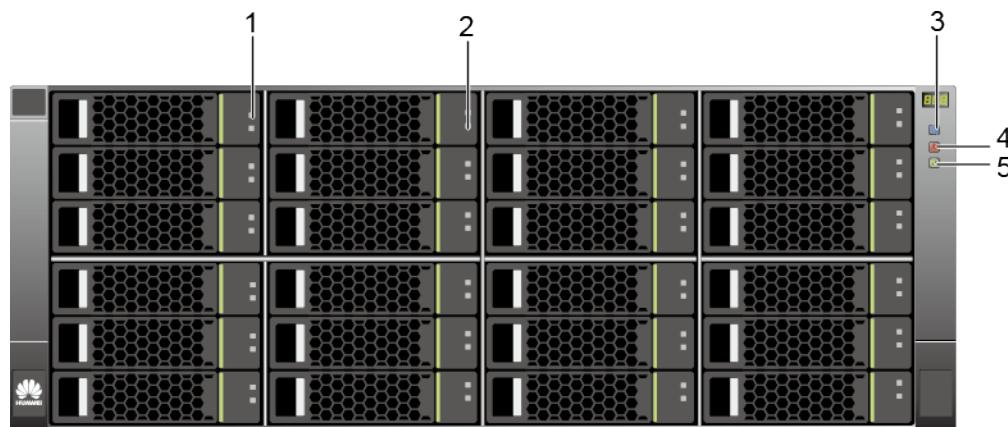
#### 4.2.3.3.2 Indicators on a 4 U Disk Enclosure

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

#### Indicators on the Front Panel

[Figure 4-18](#) shows the indicators on the front panel of a disk enclosure.

**Figure 4-18** Indicators on the front panel of a disk enclosure



1	Running indicator of the disk module	2	Location/Alarm indicator of the disk module
3	Location indicator of the disk enclosure	4	Alarm indicator of the disk enclosure
5	Power indicator of the disk enclosure		

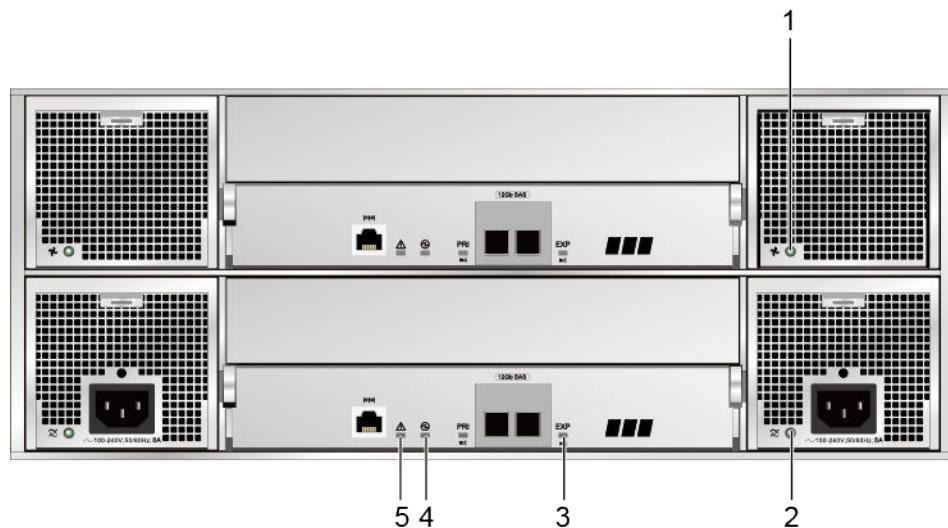
**Table 4-25** describes the indicators on the front panel of the disk enclosure.

**Table 4-25** Description of the indicators on the front panel of a disk enclosure

Module	No.	Indicator	Status and Description
Disk module	1	Running indicator of the disk module	<ul style="list-style-type: none"> <li>● Steady green: The disk module is working correctly.</li> <li>● Blinking green: Data is being read and written on the disk module.</li> <li>● Off: The disk module is powered off or powered on incorrectly.</li> </ul>
	2	Alarm/Location indicator of the disk module	<ul style="list-style-type: none"> <li>● Steady red: The disk module is faulty.</li> <li>● Blinking red: The disk module is being located.</li> <li>● Off: The disk module is working correctly or hot swappable.</li> </ul>
System subrack	3	Location indicator of the disk enclosure	<ul style="list-style-type: none"> <li>● Blinking blue: The disk enclosure is being located.</li> <li>● Off: The disk enclosure is not located.</li> </ul>
	4	Alarm indicator of the disk enclosure	<ul style="list-style-type: none"> <li>● Steady red: An alarm is generated in the disk enclosure.</li> <li>● Off: The disk enclosure is working correctly.</li> </ul>
	5	Power indicator of the disk enclosure	<ul style="list-style-type: none"> <li>● Steady green: The disk enclosure is powered on.</li> <li>● Off: The disk enclosure is powered off.</li> </ul>

## Indicators on the Rear Panel

**Figure 4-19** shows the indicators on the rear panel of a disk enclosure.

**Figure 4-19** Indicators on the rear panel of a disk enclosure

1	Running/Alarm indicator of the fan module	2	Running/Alarm indicator of the power module
3	Mini SAS HD expansion port indicator	4	Power indicator of the expansion module
5	Alarm indicator of the expansion module		

**Table 4-26** describes the indicators on the rear panel of the disk enclosure.

**Table 4-26** Description of the indicators on the rear panel of a disk enclosure

Module	No.	Indicator	Status and Description
Fan module	1	Running/Alarm indicator of the fan module	<ul style="list-style-type: none"><li>● Steady green: The fan module is working correctly.</li><li>● Steady red: The fan module is faulty.</li><li>● Off: The fan module is powered off.</li></ul>
Power module	2	Running/Alarm indicator of the power module	<ul style="list-style-type: none"><li>● Steady green: The power supply is correct.</li><li>● Blinking green: The power input is normal but the disk enclosure is powered off.</li><li>● Steady red: The power supply is faulty.</li><li>● Off: No external power input is found.</li></ul>

Module	No.	Indicator	Status and Description
Expansion module	3	Indicator of the mini SAS HD expansion port	<ul style="list-style-type: none"> <li>● Steady blue: Data is transferred to the downstream disk enclosure at the rate of 4 x 12 Gbit/s.</li> <li>● Steady green: Data is transferred to the downstream disk enclosure at the rate of 4 x 3 Gbit/s or 4 x 6 Gbit/s.</li> <li>● Steady red: The port is faulty.</li> <li>● Off: The link to the port is down.</li> </ul>
	4	Power indicator of the expansion module	<ul style="list-style-type: none"> <li>● Steady green: The expansion module is powered on.</li> <li>● Off: The expansion module is powered off.</li> </ul>
	5	Alarm indicator of the expansion module	<ul style="list-style-type: none"> <li>● Steady red: An alarm is generated on the expansion module.</li> <li>● Off: The expansion module is working correctly.</li> </ul>

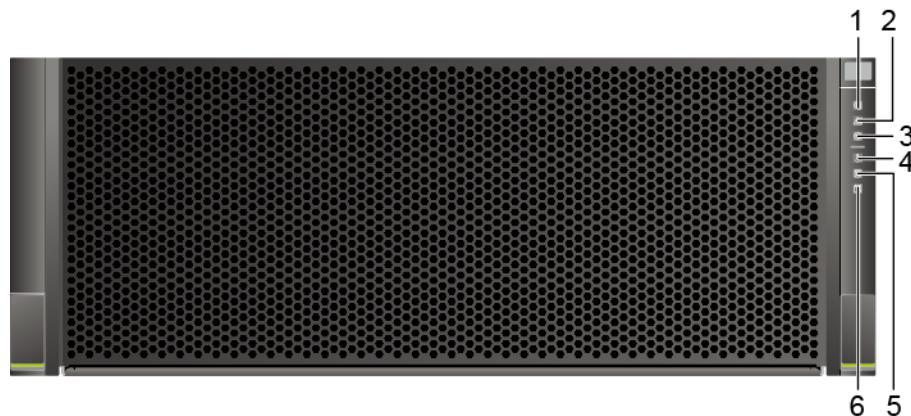
#### 4.2.3.3.3 Indicators on a High-Density Disk Enclosure

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

#### Indicators on the Front Panel

[Figure 4-20](#) shows the indicators on the front panel of a high-density disk enclosure.

**Figure 4-20** Indicators on the front panel of a high-density disk enclosure



1	Location indicator	2	Alarm indicator
---	--------------------	---	-----------------

3	Power indicator	4	Overtemperature Alarm indicator
5	Internal module Alarm indicator	6	Rear module Alarm indicator

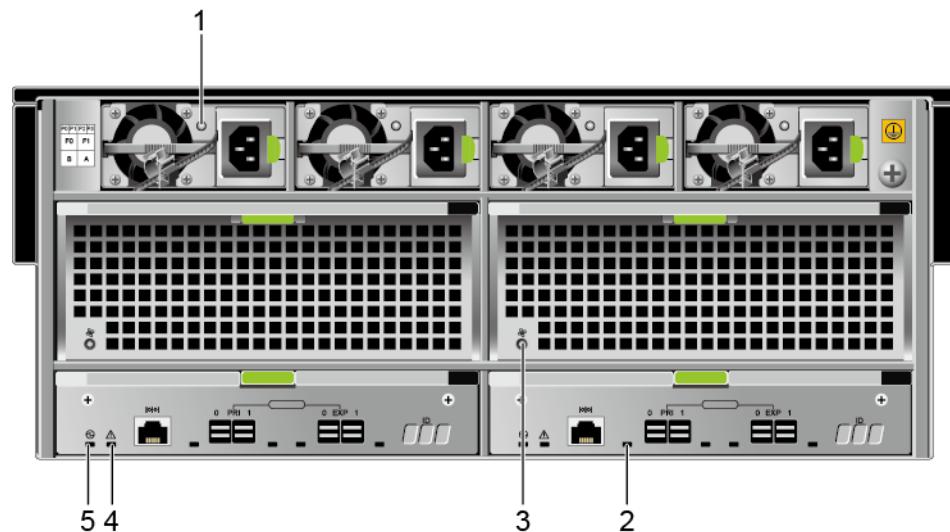
**Table 4-27** describes the indicators on the front panel of a high-density disk enclosure.

**Table 4-27** Description of the indicators on the front panel of a high-density disk enclosure

Module	No.	Indicator	Status and Description
System subrack	1	Location indicator	<ul style="list-style-type: none"> <li>● Blinking blue: The high-density disk enclosure has been located.</li> <li>● Off: The high-density disk enclosure is not located.</li> </ul>
	2	Alarm indicator	<ul style="list-style-type: none"> <li>● Steady red: An alarm is generated in the high-density disk enclosure.</li> <li>● Off: The high-density disk enclosure is running correctly.</li> </ul>
	3	Power indicator	<ul style="list-style-type: none"> <li>● Steady green: The high-density disk enclosure is powered on.</li> <li>● Off: The high-density disk enclosure is not powered on.</li> </ul>
	4	Overtemperature Alarm indicator	<ul style="list-style-type: none"> <li>● Steady red: The temperature of the high-density disk enclosure is too high.</li> <li>● Off: The temperature of the high-density disk enclosure is within the normal range.</li> </ul>
	5	Internal module Alarm indicator	<ul style="list-style-type: none"> <li>● Steady red: Internal disk modules of the high-density disk enclosure are faulty.</li> <li>● Off: Internal disk modules are running correctly.</li> </ul>
	6	Rear module Alarm indicator	<ul style="list-style-type: none"> <li>● Steady red: The number of rear field replaceable units (FRUs) is fewer than half of that in standard configuration or rear FRUs are faulty.</li> </ul> <p><b>NOTE</b> Modules on the rear of the high-density disk enclosure include power modules, fan modules, and expansion modules.</p> <ul style="list-style-type: none"> <li>● Off: Rear FRUs are running correctly.</li> </ul>

## Indicators on the Rear Panel

**Figure 4-21** shows the indicators on the rear panel of a high-density disk enclosure.

**Figure 4-21** Indicators on the rear panel of a high-density disk enclosure

1	Running/Alarm indicator of the power module	2	Indicator of the mini SAS HD expansion port
3	Fan module Running/Alarm indicator	4	Expansion module Alarm indicator
5	Expansion module Power indicator		

**Table 4-28** describes the indicators on the rear panel of a high-density disk enclosure.

**Table 4-28** Description of the indicators on the rear panel of a high-density disk enclosure

Module	No.	Indicator	Status and Description
Power module	1	Running/Alarm indicator of the power module	<ul style="list-style-type: none"><li>● Steady green: The power module is working correctly.</li><li>● Off: The power module is power off, or undervoltage, overvoltage, overtemperature, or short-circuit occurs.</li></ul>

Module	No.	Indicator	Status and Description
Expansion module	2	Indicator of the mini SAS HD expansion port	<ul style="list-style-type: none"><li>● Steady blue: The link is up and the data transfer rate is 4 x 12 Gbit/s.</li><li>● Steady green: The link is up and the data transfer rate is 4 x 6 Gbit/s.</li><li>● Steady red: The expansion port is faulty.</li><li>● Off: The link is down.</li></ul>
Fan module	3	Fan module Running/Alarm indicator	<ul style="list-style-type: none"><li>● Steady green: The fan module is running correctly.</li><li>● Steady red: The fan module is faulty.</li><li>● Off: The fan module is not powered on.</li></ul>
Expansion module	4	Expansion module Alarm indicator	<ul style="list-style-type: none"><li>● Steady red: An alarm is generated on the expansion module.</li><li>● Off: The expansion module is running correctly.</li></ul>
	5	Expansion module Power indicator	<ul style="list-style-type: none"><li>● Steady green: The expansion module is running correctly.</li><li>● Off: The expansion module is not powered on.</li></ul>

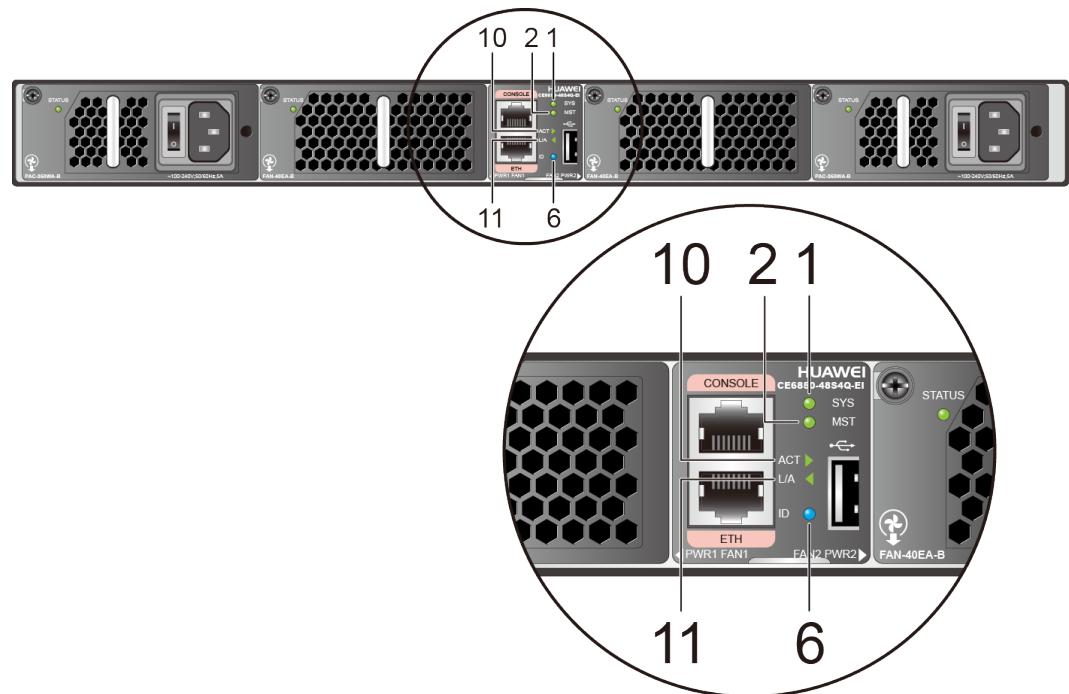
#### 4.2.3.4 Checking Status of Indicators on an IP Switch

Switch indicators reflect the current operating status of a switch. By observing these indicators, the status of each switch component can be quickly learned.

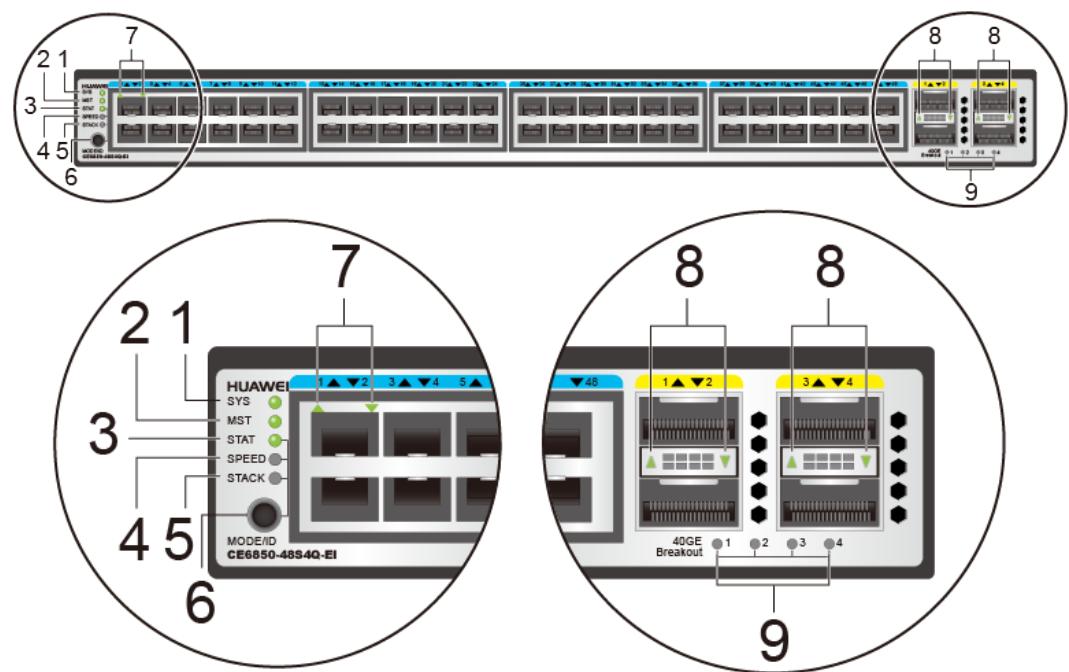
#### Reference Standard

Switch indicators are located on the front and rear panels of a switch.

**Figure 4-22** Indicators on a data switch panel (front view)



**Figure 4-23** Indicators on a data switch panel (rear view)



**Table 4-29** lists the states and their meanings of the switch indicators shown in [Figure 4-22](#) and [Figure 4-23](#).

**Table 4-29** Indicators on a data switch panel

No.	Indicator/Button	Color	Description
1	SYS: system status indicator	-	Off: The system is not running.
		Green	<ul style="list-style-type: none"> <li>● Fast blinking: The system is starting.</li> <li>● Slow blinking: The system is running properly.</li> </ul>
		Red	<p>Steady on:</p> <ul style="list-style-type: none"> <li>● The system failed to start.</li> <li>● One or more power supply modules have failed.</li> <li>● One or more fan modules have failed.</li> <li>● The card power consumption exceeds the rated power of the power module.</li> </ul>
2	MST: stack master/slave indicator	-	Off: The switch is not a stack master.
		Green	Steady on: The switch is a stack master or standalone switch.
		Amber	Steady on: An error has occurred during stack master election or another stack error has occurred.
3	STAT: STAT mode indicator	-	Off: The STAT mode is not selected.
		Green	Steady on: The STAT mode (default mode) is selected. If the STAT mode is selected, the service port indicator shows the port link or activity state.
4	SPEED: SPEED mode indicator	-	Off: The SPEED mode is not selected.
		Green	Steady on: The SPEED mode is selected. If the SPEED mode is selected, the service port indicator shows the port speed state.
5	STACK: STACK mode indicator	-	Off: The STACK mode is not selected.
		Green	Steady on: The STACK mode is selected. If the STACK mode is selected, the service port indicator shows the device stack ID.

No.	Indicator/Button	Color	Description
6	<b>MODE/ID:</b> mode switching button and ID indicator  <b>NOTE</b> The mode switching button on the rear panel is integrated with the ID indicator. There is only an ID indicator and no mode switching button on the front panel.	Mode switch ing button : -	<ul style="list-style-type: none"> <li>If you press the MODE button a first time, the SPEED indicator blinks green and the service port indicator shows the port speed state.</li> <li>If you press the MODE button a second time, the STACK indicator blinks green and the service port indicator shows the device stack ID.</li> <li>If you press the MODE button a third time, only the STAT indicator blinks green, indicating that the default mode is used. In addition, the service port indicator shows the port link or activity state.</li> </ul> <p>If you do not press the MODE button within 45 seconds, only the STAT indicator blinks green and the SPEED and STACK indicators are off.</p>
			ID indicator: - Off: The ID indicator is not used (default state).
			ID indicator: blue Steady on: The indicator identifies the device for maintenance. The ID indicator can be turned on or off remotely to help onsite engineers find the device to maintain.
7	<b>Service port indicator (10GE optical port)</b>  <b>NOTE</b> 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.		The meaning of the service port indicator varies with the current mode. For details, see <a href="#">Table 4-30</a> .
8	<b>Service port indicator (40GE optical port)</b>  <b>NOTE</b> 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.		The meaning of the service port indicator varies with the current mode. For details, see <a href="#">Table 4-30</a> .  When a 40GE port is configured as four 10GE ports, this indicator shows the status of a 10GE port. The sequence number of the indicated 10GE port is identified by indicators 40GE Breakout 1/2/3/4.  <b>NOTE</b> Each 40GE port has a single-color indicator, which shows the status of the 40GE port by default. When a 40GE port on the local device is not split and connects to four 10GE ports on the remote device through a one-to-four QSFP+ cable, the local 40GE port cannot go Up and the indicator is off.
9	10GE port sequence number indicators	-	Off: A 40GE port is not split into four 10GE ports.

No.	Indicator/Button	Color	Description
	(40GE Breakout 1/2/3/4) (10GE port converted from a 40GE port)  <b>NOTE</b> Indicators 1, 2, 3, 4 turn on in cyclic order, with each indicator keeping on for 5s.	Green	<p>Steady on: At least one 40GE port has been split into four 10GE ports.</p> <p>When one or more 40GE ports are configured as four 10GE ports, these indicators identify the sequence number of the 10GE ports. The port indicator (8 in <a href="#">Figure 4-23</a>) shows the status of a 10GE port converted from a 40GE port:</p> <ul style="list-style-type: none"> <li>● When Breakout indicator 1 is on, each 40GE interface indicator shows the status of the first 10GE interface derived from the corresponding 40GE interface.</li> <li>● When Breakout indicator 2 is on, each 40GE interface indicator shows the status of the second 10GE interface derived from the corresponding 40GE interface.</li> <li>● When Breakout indicator 3 is on, each 40GE interface indicator shows the status of the third 10GE interface derived from the corresponding 40GE interface.</li> <li>● When Breakout indicator 4 is on, each 40GE interface indicator shows the status of the fourth 10GE interface derived from the corresponding 40GE interface.</li> </ul> <p>The following is an example:</p> <p>The first 40GE interface shown in <a href="#">Figure 4-23</a> is split into four 10GE interfaces, and the second 40GE interface is not split.</p> <ul style="list-style-type: none"> <li>● When Breakout indicator 1 is on, the indicator of 40GE interface 1 shows the status of the first 10GE interface derived from 40GE interface 1, and the indicator of 40GE interface 2 shows the status of the second 40GE interface.</li> <li>● When Breakout indicator 2 is on, the indicator of 40GE interface 1 shows the status of the second 10GE interface derived from 40GE interface 1, and the indicator of 40GE interface 2 shows the status of the second 40GE interface.</li> </ul>
10	ACT: USB deployment status indicator	-	Off: USB-based deployment is disabled (default state).
		Green	<ul style="list-style-type: none"> <li>● Steady on: A USB-based deployment has been completed.</li> <li>● Blinking: The system is reading data from a USB flash drive.</li> </ul>

No.	Indicator/Button	Color	Description
		Red	Steady on: USB-based deployment has failed.
11	L/A: ETH port indicator	-	Off: No link is established on the port.
		Green	<ul style="list-style-type: none"> <li>● Steady on: A link is established on the port.</li> <li>● Blinking: The port is sending or receiving data.</li> </ul>

**Table 4-30** describes service interface indicators in various modes.**Table 4-30** Indicators in various modes

Display Mode	Port	Color	Description
STAT	40GE optical port	-	Off: The port is not connected or has been shut down.
		Green	<ul style="list-style-type: none"> <li>● Steady on: A link is established on the port.</li> <li>● Blinking: The port is sending or receiving data.</li> </ul>
	10GE optical port	-	Off: The port is not connected or has been shut down.
		Green	Steady on: A link is established on the port.
		Amber	Blinking: The port is sending or receiving data.
SPEED	10GE optical port	-	Off: The port is not connected or has been shut down.
		Green	<ul style="list-style-type: none"> <li>● Steady on: The port speed is 1000 Mbit/s.</li> <li>● Blinking: The port speed is 10GE.</li> </ul>
	40GE optical port	-	Off: The port is not connected or has been shut down.
		Green	<ul style="list-style-type: none"> <li>● Steady on: The 40GE port has split into four 10GE ports.</li> <li>● Blinking: The port is working as a 40GE port.</li> </ul>
STACK	Green <b>NOTE</b> This row describes the states and meanings of port indicator on a switch working in stack mode.		<ul style="list-style-type: none"> <li>● Off: Port indicators do not show stack IDs of corresponding devices.</li> <li>● Steady on: If the indicator of a port is steady on, the number of this port is the stack ID of the device.</li> </ul>

## Procedure

- Check front-panel and rear-panel indicators of the switch based on [Figure 4-22](#) and [Figure 4-23](#) and determine whether each module is working correctly.

## Exception Handling

If a module is faulty, rectify the fault. For details, see *CloudEngine 7800&6800&5800 V100R003C10 Product Documentation*. If the fault persists, contact technical support engineers.

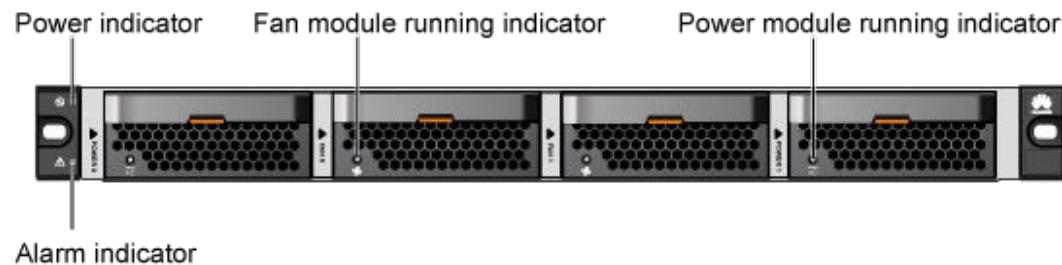
### 4.2.3.5 Checking Status of Indicators on a PCIe Switch

Data switch (DSW) indicators reflect the current running status of the DSW. By observing these indicators, you can learn about the status of each DSW component.

## Reference Standard

[Figure 4-24](#) shows the front-panel indicators and meanings of the DSW that has been correctly powered on.

**Figure 4-24** Powered-on DSW front-panel Indicators

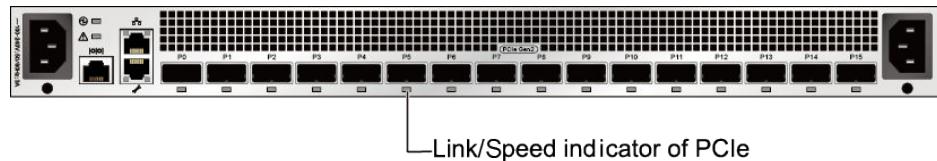


[Table 4-31](#) lists the states and meanings of the DSW front-panel indicators.

**Table 4-31** DSW front-panel indicator states and their meanings

Indicator	Normality	Abnormality
Power indicator	<ul style="list-style-type: none"><li>● Steady green</li><li>● Blinking green</li></ul>	Off
Alarm indicator	Off	Steady red
Fan module running indicator	Steady green	<ul style="list-style-type: none"><li>● Steady red</li><li>● Off</li></ul>
Power module running indicator	Steady green	<ul style="list-style-type: none"><li>● Steady red</li><li>● Off</li></ul>

[Figure 4-25](#) shows the rear-panel indicators and meanings of the DSW that has been correctly powered on.

**Figure 4-25** DSW rear-panel indicator states and their meanings

**Table 4-32** lists the states and meanings of the DSW rear-panel indicators.

**Table 4-32** DSW rear-panel indicator states and their meanings

Indicator	Normality	Abnormality
Link/Speed indicator of PCIe	<ul style="list-style-type: none"> <li>● Steady blue</li> <li>● Steady green</li> </ul>	<ul style="list-style-type: none"> <li>● Steady red</li> <li>● Off</li> </ul>

## Procedure

- Check DSW indicators by referring to [Figure 4-24](#) and [Figure 4-25](#).
- If the fault cannot be rectified, collect the fault information and report it to Huawei engineers.

## Exception Handling

If the DSW is abnormal, refer to the *Product Description* to locate the fault as reflected by indicators. Then troubleshoot the fault based on the detailed information.

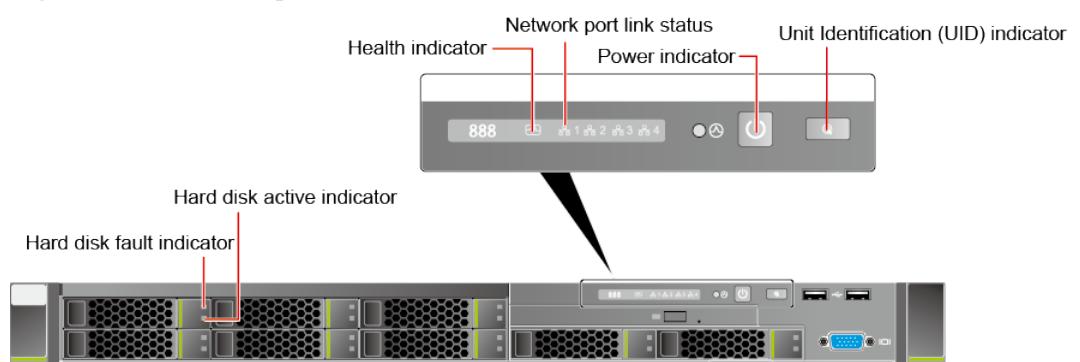
### 4.2.3.6 Checking the SVP Indicators (OceanStor 18000 Series)

SVP indicators show the running status of a controller enclosure. By checking these indicators, you can promptly learn about the status of each module.

## Reference Standard

SVP indicators are located on the front and rear panels of a controller enclosure.

[Figure 4-26](#) and [Figure 4-27](#) depict the front-panel and rear-panel indicators of the SVP that has been correctly powered on.

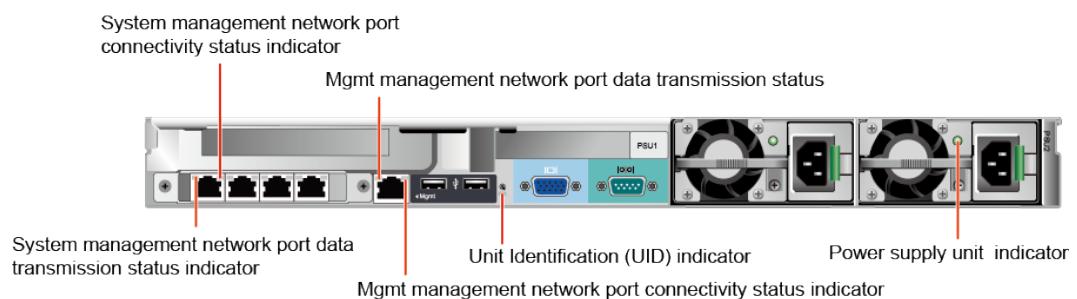
**Figure 4-26** SVP front-panel indicators

**Figure 4-26** lists the states and meanings of the SVP front-panel indicators shown in [Table 4-33](#).

**Table 4-33** SVP front-panel indicator states and their meanings

Indicator	Normality	Abnormality
Power indicator	<ul style="list-style-type: none"> <li>● Steady green</li> <li>● Steady yellow</li> <li>● Blinking yellow</li> </ul>	Off
Hard disk fault indicator	<ul style="list-style-type: none"> <li>● Off</li> <li>● Blinking yellow</li> </ul>	Steady yellow
Hard disk active indicator	<ul style="list-style-type: none"> <li>● Steady green</li> <li>● Blinking green</li> </ul>	Off
Health indicator	Steady green	Blinking red
Network port link status indicator	Steady green	Off
UID indicator	Steady blue	-

**Figure 4-27** SVP rear-panel indicators



**Figure 4-27** lists the states and their meanings of the SVP rear-panel indicators shown in [Table 4-34](#).

**Table 4-34** SVP rear-panel indicator states and their meanings

Indicator	Normality	Abnormality
Power supply unit (PSU) indicator	Steady green	Off
Mgmt management network port data transmission status indicator	Blinking orange	Off

Indicator	Normality	Abnormality
Mgmt management network port connectivity status indicator	Steady green	Off
System management network port data transmission status indicator	Blinking orange	Off
System management network port connectivity status indicator	Steady green	Off
Unit Identification (UID) indicator	Steady blue	-

## Procedure

- Check onsite SVP front-panel and rear-panel indicators according to [Figure 4-26](#) and [Figure 4-27](#). Predetermine whether all component modules on the SVP are working properly.

## Exception Handling

If an exception occurs on a device module, record the exception and log in to DeviceManager to locate alarms about engines. Alternatively, refer to the *Product Description* for the meanings of indicator states. If the fault cannot be rectified, collect the fault information and report it to Huawei engineers.

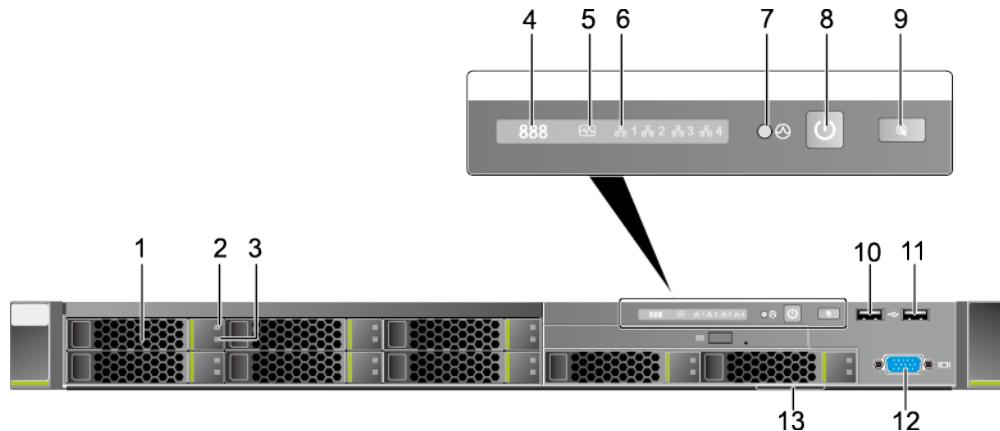
### 4.2.3.7 (Optional) Checking Quorum Server Indicators

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

## Front Panel of the Quorum Server

[Figure 4-28](#) shows the front panel of the quorum server.

**Figure 4-28** Front panel of the quorum server



1	Disk	2	Disk Fault indicator
3	Disk Active indicator	4	Fault diagnosis LED
5	Health indicator	6	Network port link indicator
7	NMI button	8	Power button/indicator
9	Unit Identification (UID) button/indicator	10	USB 2.0 port
11	USB 2.0 port	12	Video graphics array (VGA) port
13	Label (including ESN label)		

**Table 4-35** describes the indicators and buttons on the quorum server front panel.

**Table 4-35** Indicators and buttons on the front panel

Number	Meaning	Color	State Description
4	Fault diagnosis LED	None	<ul style="list-style-type: none"><li>● ---: The quorum server is operating properly.</li><li>● Error Code: A fault occurs in quorum server hardware.</li></ul>
8	Power button/indicator	Yellow and green	<ul style="list-style-type: none"><li>● Off: The quorum server is not powered on.</li><li>● Blinking yellow: The system is being started.</li><li>● Steady yellow: The system is in the standby state.</li><li>● Steady green: The system is properly powered on.</li></ul> <p><b>NOTE</b> You can hold down the power button for 6 seconds to power off the quorum server.</p>

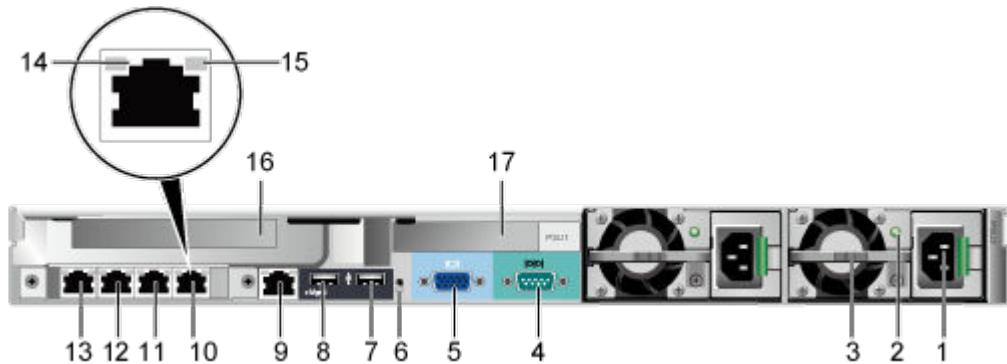
Number	Meaning	Color	State Description
9	UID button/indicator	Blue	<p>The UID button/indicator helps identify and locate a quorum server in a rack. You can turn on or off the UID indicator by manually pressing the UID button or remotely running a command on the CLI.</p> <ul style="list-style-type: none"><li>● Steady on: The quorum server is located.</li><li>● Off: The quorum server is not located.</li><li>● You can hold down the UID button for 4 to 6 seconds to reset the system.</li></ul>
5	Health indicator	Red and green	<ul style="list-style-type: none"><li>● Steady green: The quorum server is operating properly.</li><li>● Blinking red at 1 Hz: A major alarm is generated.</li><li>● Blinking red at 5 Hz: A critical alarm is generated.</li></ul>
7	NMI button	None	<p>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.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"><li>● Click the NMI button only when the OS is abnormal. Do not click this button when the quorum server is operating properly.</li><li>● 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.</li></ul>
3	Disk Active indicator	Green	<ul style="list-style-type: none"><li>● Off: The disk is not detected or is faulty.</li><li>● Blinking green: Data is being read from, written to the disk, or synchronized between disks.</li><li>● Steady green: The disk is inactive.</li></ul>

Number	Meaning	Color	State Description
2	Disk Fault indicator	Yellow	<ul style="list-style-type: none"> <li>● Off: The disk is working properly.</li> <li>● Blinking yellow: The disk is being located, or the RAID is being reconstructed.</li> <li>● Steady yellow: The disk is faulty, or member disks in the RAID group are abnormal.</li> </ul>
6	Network port Link status indicators	Green	<p>Each indicator shows the status of an Ethernet port on the network interface card (NIC).</p> <ul style="list-style-type: none"> <li>● Steady green: The port is properly connected.</li> <li>● Off: The port is not in use.</li> </ul> <p><b>NOTE</b> If the NIC provides only two network ports, network port indicators 1 and 2 on the front panel are used.</p>

## Rear View of the Quorum Server

[Figure 4-29](#) show the rear view of the quorum server.

**Figure 4-29** Rear view of the quorum server



1	Power socket for a power module	2	Power module indicator
3	Power module	4	Serial port
5	VGA port	6	UID indicator
7	USB 3.0 port	8	USB 3.0 port

9	Management network port of BMC	10	Management network port (Mgmt)
11	System management network port P3	12	System management network port P2
13	System management network port P1	14	Data transmission status indicator
15	Connectivity status indicator	16	Full-height PCIe slot <b>NOTE</b> This slot is reserved. Do not install PCIe card in this slot.
17	Half-height PCIe slot		

 **NOTE**

The default IP addresses of the management network port (Mgmt) on the quorum server is 192.168.128.200, and the default subnet mask is 255.255.255.0.

**Table 4-36** describes the indicators on the quorum server rear panel.

**Table 4-36** Indicators on the rear panel

Number	Indicator	Color	State
14	Data transmission status indicator	Yellow	<ul style="list-style-type: none"> <li>● Off: No data is being transmitted.</li> <li>● Blinking: Data is being transmitted.</li> </ul>
15	Connectivity status indicator	Green	<ul style="list-style-type: none"> <li>● Steady green: The port is properly connected.</li> <li>● Off: The port is not in use.</li> </ul>
6	Unit Identification (UID) indicator	Blue	<p>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 CLI.</p> <ul style="list-style-type: none"> <li>● Steady on: The quorum server is located.</li> <li>● Off: The quorum server is not located.</li> <li>● You can hold down the UID button for 4 to 6 seconds to reset the system.</li> </ul>

Number	Indicator	Color	State
2	Power module indicator	Green	<ul style="list-style-type: none"><li>● Steady green: Both the active output and the standby output are normal.</li><li>● Off: There is no AC power input; the input overvoltage or undervoltage occurs and the power module is not detected; the power module is abnormal.</li></ul>

## 4.2.4 Checking the Running Status of the Storage Device

You need to check the physical status of the storage device by examining its indicators and check the functional status of the device on DeviceManager. This allows you to detect device faults in a timely manner.

### 4.2.4.1 Checking Controller Enclosures or Disk Enclosures

You can learn about the health and running status of the controller enclosure or a disk enclosure by checking its status information on DeviceManager.

#### Impact on the System

A fault on the controller enclosure or disk enclosure may impair read/write performance, deteriorate reliability, disrupt services, and cause data loss on the enclosure.

#### Reference Standard

If the controller enclosure and disk enclosures are working properly, the following items are true on DeviceManager:

- All of the enclosures are in the **Normal** health status and **Online** running status.
- No enclosure alarm appears on the **Current Alarms** tab page.

#### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **System**.

**Step 3** Click the desired enclosure in the cabinet.



If a storage system has multiple cabinets, select a cabinet that you want to view.

**Step 4** Click the enclosure icon on the right.

The detailed information about the enclosure is displayed.

**Step 5** View the enclosure information in the group box that is displayed.

**Table 4-37** describes associated status parameters.

**Table 4-37** Enclosure statusparameters and their meanings

Parameter	Description
Health Status	Health status of an enclosure. The value can be: <ul style="list-style-type: none"><li>● <b>Normal:</b> The functionality and operating performance of the enclosure are normal.</li><li>● <b>Faulty:</b> The enclosure is working improperly.</li></ul>
Running Status	Running status of an enclosure. The value can be <b>Online</b> or <b>Offline</b> .

----End

## Follow-up Procedure

If an enclosure alarm appears on the **Current Alarms** tab page, select the alarm and diagnose the problem according to its details and repair suggestions.

### 4.2.4.2 Checking Controllers

Controllers of the storage device are responsible for running storage applications, implementing storage mechanisms (StoragePool, LUN mapping, and striping), and managing alarms. You can learn about the health and running status of a controller by checking its status information on DeviceManager.

## Impact on the System

A fault on a controller may impair read/write performance, deteriorate reliability, disrupt services, and cause data loss on the controller module.

## Reference Standard

If controllers are working properly, the following items are true on 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** Log in to DeviceManager.

**Step 2** Choose  **System**.

**Step 3** Click the desired controller module in the view.

The detailed information about the controller module is displayed.



If a storage system has multiple cabinets, select a cabinet that you want to view.

**Step 4** View the controller module information in the group box that is displayed.

**Table 4-38** describes associated status parameters.

**Table 4-38** Controller statusparameters and their meanings

Parameter	Description
Health Status	Health status of a controller module. The value can be: <ul style="list-style-type: none"><li>● <b>Normal:</b> The functionality and operating performance of the controller are normal.</li><li>● <b>Faulty:</b> The controller is working improperly.</li></ul>
Running Status	Running status of a controller module. The value can be <b>Online</b> or <b>Offline</b> .

----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.

### 4.2.4.3 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 DeviceManager.

## Impact on the System

- If a power module is faulty, data reliability deteriorates.
- If all of the power modules are faulty, service are interrupted and the storage device is powered off.

## Reference Standard

If power modules are working properly, the following items are true on 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** Log in to DeviceManager.

**Step 2** Choose  **System**.

**Step 3** Click  to switch to the rear view of the storage device.

 **NOTE**

If a storage system has multiple cabinets, select a cabinet that you want to view before performing the next step.

**Step 4** Click the desired power module.

The detailed information about the power module is displayed.

**Step 5** View the power module information in the group box that is displayed.

**Table 4-39** describes associated status parameters.

**Table 4-39** Power modulestatus parameters and their meanings

Parameter	Description
Health Status	Health status of a power module. The value can be: <ul style="list-style-type: none"><li>● <b>Normal:</b> The functionality and operating performance of the power module are normal.</li><li>● <b>Faulty:</b> The power module is working improperly.</li><li>● <b>No input:</b> The power module has been installed but does not supply power.</li></ul>
Running Status	Running status of a power module. The value can be <b>Online</b> or <b>Offline</b> .

----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.

### 4.2.4.4 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 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** Log in to DeviceManager.

**Step 2** Choose  **System**.

**Step 3** Click the desired BBU in the view.

The detailed information about the BBU is displayed.



If a storage system has multiple cabinets, select a cabinet that you want to view.

**Step 4** View the BBU information in the group box that is displayed.

**Table 4-40** describes associated status parameters.

**Table 4-40** BBU statusparameters and their meanings

Parameter	Description
Health Status	Health status of a BBU. The value can be: <ul style="list-style-type: none"><li>● <b>Normal</b>: The functionality and operating performance of the BBU are normal.</li><li>● <b>Faulty</b>: The BBU is working improperly.</li><li>● <b>Insufficient power</b>: The power level of the BBU is low though its operating performance is normal.</li></ul>
Running Status	Running status of a BBU. The value can be <b>Online</b> , <b>Charging</b> , or <b>Discharging</b> .

----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.

### 4.2.4.5 Checking Fan Modules

Fan modules in the controller enclosure or a disk enclosure provide a cyclic aeration system to ensure the reliable running of the storage device. You can learn about the health and running status of a fan module by checking its status information on DeviceManager.

## Impact on the System

When fan modules become faulty, the ambient temperature of the controller enclosure or a disk enclosure rises, hampering the proper running of the storage device.

## Reference Standard

If fan modules are working properly, the following items are true on 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** Log in to DeviceManager.

**Step 2** Choose  **System**.

**Step 3** Select the disk enclosure or controller enclosure.

- For disk enclosure, please click  to switch to the rear view of the storage device.
- For 3U controller enclosure, you can view the detailed information about the fan module from the front view of the storage device. For 2U controller enclosure, click  to switch to the rear view of the storage device.

**Step 4** Click the desired fan module in the view.

The detailed information about the fan module is displayed.

**Step 5** View the fan module information in the group box that is displayed.

**Table 4-41** describes associated status parameters.

**Table 4-41** Fan module statusparameters and their meanings

Parameter	Description
Health Status	Health status of a fan module. The value can be: <ul style="list-style-type: none"><li>● <b>Normal</b>: The functionality and operating performance of the fan module are normal.</li><li>● <b>Fault</b>: The fan module is working improperly.</li></ul>
Running Status	Running status of a fan module. The value can be <b>Running</b> or <b>Not running</b> .

----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.

### 4.2.4.6 Checking Hard Disks

Hard 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 hard disk by checking its status information on DeviceManager.

## Impact on the System

Faulty hard disks may impair read/write performance and cause data loss on the storage device.

## Reference Standard

If hard 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** Log in to DeviceManager.

**Step 2** Choose  **System**.

**Step 3** Click the desired disk in the view.

The detailed information about the hard disk is displayed.

 **NOTE**

If a storage system has multiple cabinets, select a cabinet that you want to view before performing the next step.

**Step 4** View the disk information in the group box that is displayed.

**Table 4-42** describes associated status parameters.

**Table 4-42** Hard disk statusparameters and their meanings

Parameter	Description
Health Status	Health status of a hard disk. The value can be: <ul style="list-style-type: none"><li>● <b>Normal</b>: The functionality and operating performance of the hard disk are normal.</li><li>● <b>Fault</b>: The hard disk is working improperly.</li><li>● <b>Failing</b>: The hard disk is about to fail.</li></ul>
Running Status	Running status of a hard disk. The value can be <b>Online</b> or <b>Offline</b> .

----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.

#### 4.2.4.7 Checking Host Ports

Host ports enable service communication between the storage device and application servers. You can learn about the health and running status of a host port by checking its status information on DeviceManager.

#### Impact on the System

Faulty host ports may disable service communication between the storage device and application servers.

#### Reference Standard

If front-end host ports are working properly, the following items are true on DeviceManager:

- All of the host ports are in the **Normal** health status and **Link Up** running status.
- No host port alarm appears on the **Current Alarms** tab page.

#### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **System**.

**Step 3** Click  to switch to the rear view of the storage device.

 **NOTE**

If a storage system has multiple cabinets, select a cabinet that you want to view before performing the next step.

**Step 4** Click the desired host port in the view.

The detailed information about the host port is displayed.

**Step 5** View the host port information in the group box that is displayed.

**Table 4-43** describes associated status parameters.

**Table 4-43** Host port statusparameters and their meanings

Parameter	Description
Health Status	Health status of a host port. The value can be: <ul style="list-style-type: none"><li>● <b>Normal</b>: The functionality and operating performance of the host port are normal.</li><li>● <b>Faulty</b>: The host port is working improperly.</li></ul>
Running Status	Running status of a host port. The value can be <b>Link up</b> or <b>Link down</b> .

----End

## Follow-up Procedure

If a host port alarm appears on the **Current Alarms** tab page, select the alarm and diagnose the problem according to its details and repair suggestions.

### 4.2.4.8 Checking Interface Modules

Interface modules are used to house host ports 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 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** Log in to DeviceManager.

**Step 2** Choose  **System**.

**Step 3** Click  to switch to the rear view of the storage device.

 **NOTE**

If a storage system has multiple cabinets, select a cabinet that you want to view.

**Step 4** Click the desired interface module in the view.

The detailed information about the interface module is displayed.

**Step 5** View the interface module information in the group box that is displayed.

**Table 4-44** describes associated status parameters.

**Table 4-44** Interface modulestatus parameters and their meanings

Parameter	Definition
Health Status	Health status of an interface module. The value can be: <ul style="list-style-type: none"><li>● <b>Normal</b>: The functionality and operating performance of the interface module are normal.</li><li>● <b>Faulty</b>: The interface module is working improperly.</li></ul>
Running Status	Running status of an interface module. The value can be <b>Running</b> or <b>Powered off</b> .

----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.

### 4.2.4.9 Checking Remote Devices

You can learn about the health and running status of a remote device connecting to the storage device by using 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 DeviceManager.

## Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Data Protection** >  **Remote Device**.

**Step 3** On the **Remote Device** page, view the detailed information about the desired remote device.

**Table 4-45** describes associated status parameters.

**Table 4-45** Remote devicestatus parameters and their meanings

Parameter	Description
Health Status	Health status of a remote device. The value can be: <ul style="list-style-type: none"><li>● <b>Normal</b>: The remote device is working properly.</li><li>● <b>Faulty</b>: The remote device is working improperly.</li></ul>
Running Status	Running status of a remote device. The value can be <b>Link up</b> or <b>Link down</b> .

----End

## Follow-up Procedure

For a remote device, if its **Health Status** is **Fault** 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 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.

The remote replication function, consistency group function, clone function, snapshot function, LUN copy function, HyperMirror function, file system function and optimization features are not supported by OceanStor 2600 V3 video surveillance edition.

### 4.2.5.1 Checking Disk Domains

By checking the status of a disk domain, you can understand its health status and running status. The running status of a disk domain directly affects that of a storage pool.

#### Impact on the System

A faulty or degraded disk domain may impair read/write performance, interrupt services, and cause data loss on the storage device.

#### Reference Standard

If disk domains are working properly, the following items are true on DeviceManager:

- All of the disk domains are in the **Normal** health status and **Online** running status.
- No disk domain alarm appears on the **Current Alarms** tab page.

#### Precaution

None

#### Procedure

**Step 1** On the navigation bar of DeviceManager, click  **Provisioning**.

**Step 2** In the function pane, click **Disk Domain**.

The **Disk Domain** page is displayed.

**Step 3** On the **Disk Domain** page, view the information about the desired disk domain.

**Table 4-46** describes associated status parameters.

**Table 4-46** Disk domain status parameters and their meanings

Parameter	Description
Health Status	Health status of a disk domain. The value can be: <ul style="list-style-type: none"><li>● <b>Normal</b>: The functionality and operating performance of the disk domain are normal.</li><li>● <b>Degraded</b>: The disk domain is working in a poor performance.</li><li>● <b>Faulty</b>: The disk domain is working improperly.</li></ul>

Parameter	Description
Running Status	Running status of a disk domain. The value can be <b>Online</b> , <b>Reconstruction</b> , <b>Precopy</b> , <b>Initializing</b> , <b>Deleting</b> or <b>Offline</b> .

----End

## Exception Handling

If a disk domain 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 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, disrupt 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.

## Precaution

None

## Procedure

**Step 1** On the navigation bar of DeviceManager, click  **Provisioning**.

**Step 2** In the function pane, click **Storage Pool**.

The **Storage Pool** page is displayed.

**Step 3** On the **Storage Pool** page, view the information about the desired storage pool.

**Table 4-47** describes associated status parameters.

**Table 4-47** Storage pool status parameters and their meanings

Parameter	Description
Health Status	Health status of a storage pool. The value can be: <ul style="list-style-type: none"><li>● <b>Normal:</b> The functionality and operating performance of the storage pool are normal.</li><li>● <b>Degraded:</b> The storage pool is working in a poor performance.</li><li>● <b>Faulty:</b> The storage pool is working improperly.</li></ul>
Running Status	Running status of a storage pool. The value can be <b>Online</b> , <b>Reconstruction</b> , <b>Precopy</b> , <b>Initializing</b> , <b>Deleting</b> or <b>Offline</b> .

----End

## Exception Handling

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.

### 4.2.5.3 Checking LUNs

Logical unit numbers (LUNs) are basic storage resources of the storage device accessible to application servers. 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.
- No LUN alarm appears on the **Current Alarms** tab page.

## Precaution

None

## Procedure

-  **Step 1** On the navigation bar of DeviceManager, click **Provisioning**.
- Step 2** In the function pane, click **LUN**.  
The **LUN** page is displayed.
- Step 3** On the **LUN** page, view the information about the desired LUN.

**Table 4-48** describes associated status parameters.

**Table 4-48** LUN status parameters and their meanings

Parameter	Description
Health Status	Health status of a LUN. The value can be: <ul style="list-style-type: none"><li>● <b>Normal:</b> The functionality and operating performance of the LUN are normal.</li><li>● <b>Fault:</b> The LUN is working improperly.</li></ul>
Running Status	Running status of a LUN. The value can be <b>Online</b> or <b>Offline</b> .

----End

## Exception Handling

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.

### 4.2.5.4 Checking Host Status

You can view host information to understand host status.

## Impact on the System

A host fault may interrupt system services and cause data loss.

## Reference Standard

If the host status is normal, on the DeviceManager management page:

- The **Status** of the host is **Normal**.
- No alarm about the host is displayed on the **Current Alarms** tab page.

## Precaution

None

## Procedure

**Step 1** On the navigation bar of DeviceManager, click  **Provisioning**.

**Step 2** In the function pane on the left, click **Host**.

The **Host** page is displayed.

**Step 3** On the **Host** tab of the **Host** page, view detailed information about the host.

----End

## Exception Handling

If a new alarm about the host is displayed on the **Current Alarms** tab page, select the alarm, and troubleshoot the fault according to the alarm details and repair suggestions.

### 4.2.5.5 Viewing Mapping Status

You can learn the component mapping relationship on the mapping view.

#### Impact on the System

A faulty mapping may interrupt system services and cause data loss.

#### Precaution

None

#### Procedure

**Step 1** On the navigation bar of DeviceManager, click  **Provisioning**.

**Step 2** In the function pane on the left, click **Mapping View**.

The **Mapping View** page is displayed.

**Step 3** On the **Mapping View** page, select a mapping you want to view.

**Step 4** Click **Properties** and view LUN group, host group, and port group information in the mapping.

----End

## Exception Handling

If a new alarm about the host is displayed on the **Current Alarms** tab page, select the alarm, and troubleshoot the fault according to the alarm details and repair suggestions.

### 4.2.5.6 Checking Remote Replication Tasks

The remote replication function is critical to a disaster recovery system. It can implement real-time disaster recovery over long distance and can protect application continuity and data reliability. You can learn about the health and running status of a remote replication task by checking its status information.

#### Impact on the System

Faulty remote replication tasks may interrupt data backup services and cause data loss.

#### Prerequisites

A license file is required for enabling the remote replication function.

## Reference Standard

If remote replication tasks are running properly, the following items are true on DeviceManager:

- All of the remote replication tasks are in the **Normal** health status and **Normal** running status.
- No remote replication alarm appears on the **Current Alarms** tab page.

## Precaution

None

## Procedure



**Step 1** On the navigation bar of DeviceManager, click **Data Protection**.

**Step 2** In the function pane, click **Remote Replication**.

The **Remote Replication** page is displayed.

**Step 3** On the **Remote Replication** page, view the information about the desired remote replication task.

**Table 4-49** describes associated status parameters.

**Table 4-49** Remote replication status parameters and their meanings

Parameter	Definition
Pair Health Status	Health status of a remote replication task. The value can be: <ul style="list-style-type: none"><li>● <b>Normal</b>: The functionality and operating performance of the remote replication task are normal.</li><li>● <b>Faulty</b>: One or more replication pairs for the remote replication task are abnormal.</li></ul>
Pair Running Status	Running status of a remote replication task. The value can be <b>Normal</b> , <b>Synchronizing</b> , <b>To be recovered</b> , <b>Interrupted</b> , <b>Split</b> , or <b>Invalid</b> .

----End

## Exception Handling

If a remote replication alarm appears on the **Current Alarms** tab page, select the alarm and diagnose the problem according to its details and repair suggestions.

### 4.2.5.7 Checking Consistency Groups

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.

## Precaution

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, click  **Data Protection**.

**Step 2** In the function pane, click **Remote Replication**.

The **Remote Replication** page is displayed.

**Step 3** On the **Consistency Group** tab, view the information about the desired consistency group.

**Table 4-50** describes associated status parameters.

**Table 4-50** Consistency group status parameters and their meanings

Parameter	Definition
Health Status	Health status of a consistency group. The value can be: <ul style="list-style-type: none"><li>● <b>Normal</b>: The functionality and operating performance of the consistency group are normal.</li><li>● <b>Faulty</b>: One or more replication pairs for the consistency group are abnormal.</li></ul>
Running Status	Running status of a consistency group. The value can be <b>Normal</b> , <b>Synchronizing</b> , <b>To be recovered</b> , <b>Interrupted</b> , <b>Split</b> , or <b>Invalid</b> .

----End

## Exception Handling

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.

### 4.2.5.8 Checking Clone Tasks

The clone function is mainly used for data backup. It can generate point-in-time complete physical copies or consistent duplicates for the data on the storage device. You can learn about the health and running status of a clone task by checking its status information.

## Impact on the System

Faulty clone tasks may interrupt clone services and cause data loss.

## Prerequisites

A license file is required for enabling the clone function.

## Reference Standard

If clone tasks are running properly, the following items are true on DeviceManager:

- All of the clone tasks are in the **Normal** health status and **Normal** running status.
- No clone alarm appears on the **Current Alarms** tab page.

## Precaution

None

## Procedure



**Step 1** On the navigation bar of DeviceManager, click **Data Protection**.

**Step 2** In the function pane, click **Clone**.

The **Clone** page is displayed.

**Step 3** On the **Clone** page, view the information about the desired clone task.

**Table 4-51** describes associated status parameters.

**Table 4-51** Clone status parameters and their meanings

Parameter	Definition
Health Status	Health status of a clone task. The value can be: <ul style="list-style-type: none"><li>● <b>Normal:</b> The functionality and operating performance of the clone task are normal.</li><li>● <b>Faulty:</b> One or more clone pairs for the clone task are abnormal.</li></ul>
Running Status	Running status of a clone task. The value can be <b>Normal</b> , <b>Synchronizing</b> , <b>Reversely synchronizing</b> , <b>To be recovered</b> , <b>Interrupted</b> , <b>Split</b> , <b>Queueing</b> , or <b>Unknown</b> .

----End

## Exception Handling

If a clone alarm appears on the **Current Alarms** tab page, select the alarm and diagnose the problem according to its details and repair suggestions.

### 4.2.5.9 Checking Snapshot Tasks

Snapshots can provide continuous data protection with quick data backup and recovery. You can learn about the health and running status of a snapshot task by checking its status information on DeviceManager.

## Impact on the System

Faulty snapshot tasks may interrupt snapshot services and impair data security.

## Prerequisites

A license file is required for enabling the snapshot function.

## Reference Standard

If snapshot tasks are working properly, the following items are true on DeviceManager:

- All of the snapshot tasks are in the **Normal** health status.
- No snapshot alarm appears on the **Current Alarms** tab page.

## Precaution

None

## Procedure

**Step 1** On the navigation bar of DeviceManager, click  **Data Protection**.

**Step 2** In the function pane, click **Snapshot**.

The **Snapshot** page is displayed.

**Step 3** On the **Snapshot** page, view the information about the desired snapshot task.

**Table 4-52** describes associated status parameters.

**Table 4-52** Snapshot status parameters and their meanings

Parameter	Description
Health Status	Health status of a snapshot task. The value can be: <ul style="list-style-type: none"><li>● <b>Normal:</b> The functionality and operating performance of the snapshot task are normal.</li><li>● <b>Faulty:</b> The snapshot task is running improperly.</li></ul>
Running Status	Running status of a snapshot task. The value can be <b>Activated</b> , <b>Unactivated</b> , <b>Deleting</b> , <b>Initializing</b> or <b>Restore</b> .

----End

## Exception Handling

If a snapshot alarm appears on the **Current Alarms** tab page, select the alarm and diagnose the problem according to its details and repair suggestions.

### 4.2.5.10 Checking LUN Copy Tasks

The LUN copy function can copy data from a source LUN to a target LUN to implement storage tiering and remote backup. You can learn about the health and running status of a LUN copy task by checking its status information.

## Impact on the System

Faulty LUN copy tasks may interrupt LUN copy services and cause data loss.

## Prerequisites

A license file is required for enabling the LUN copy function.

## Reference Standard

If LUN copy tasks are running properly, the following items are true on DeviceManager:

- All of the LUN copy tasks are in the **Normal** health status.
- No LUN copy alarm appears on the **Current Alarms** tab page.

## Precaution

None

## Procedure

 **Step 1** On the navigation bar of DeviceManager, click **Data Protection**.

**Step 2** In the function pane, click **LUN Copy**.

The **LUN Copy** page is displayed.

**Step 3** On the **LUN Copy** page, view the information about the desired LUN copy task.

**Table 4-53** describes associated status parameters.

**Table 4-53** LUN copy status parameters and their meanings

Parameter	Definition
Health Status	Health status of a LUN copy task. The value can be: <ul style="list-style-type: none"><li>● <b>Normal:</b> The functionality and operating performance of the LUN copy task are normal.</li><li>● <b>Faulty:</b> The LUN copy task is running improperly.</li></ul>
Running Status	Running status of a LUN copy task. The value can be <b>Not start, Stopped, Copying, Paused, Queuing, or Completed</b> .

----End

## Exception Handling

If a LUN copy alarm appears on the **Current Alarms** tab page, select the alarm and diagnose the problem according to its details and repair suggestions.

### 4.2.5.11 Checking HyperMirror Status

HyperMirror provides mirror copies for LUNs and continuously protects LUNs without affecting applications running on the host. By checking HyperMirror information, you can learn about its health status and running status.

## Prerequisites

A license file is required for enabling the HyperMirror function.

## Reference Standard

If the status of HyperMirror is normal, the following items are true on the DeviceManager:

- **Health Status is Normal.**
- No alarms about HyperMirror are displayed on the **Current Alarms** tab page.

## Precaution

None

## Procedure

 **Step 1** On the navigation bar of DeviceManager, click **Data Protection**.

**Step 2** In the function pane, click **HyperMirror**.

The **HyperMirror** page is displayed.

**Step 3** On the **HyperMirror** page, view details about HyperMirror.

**Table 4-54** describes related parameters.

**Table 4-54** HyperMirror status parameters

Parameter	Description
Health status	Health status of HyperMirror. The value can be: <ul style="list-style-type: none"><li>● <b>Normal</b>: The functions and running performance of HyperMirror are normal.</li><li>● <b>Degraded</b>: The functions of HyperMirror are normal but its running performance deteriorates.</li><li>● <b>Faulty</b>: The functions and running performance of HyperMirror are abnormal.</li></ul>
Running status	Running status of volume mirroring. The status can be <b>Normal</b> , <b>Initializing</b> , <b>Queuing</b> , <b>Synchronizing</b> , <b>Split</b> , <b>Interrupted</b> , or <b>Invalid</b> .

----End

## Exception Handling

If a new alarm about HyperMirror is displayed on the **Current Alarms** tab page, select the alarm, and troubleshoot the fault according to the alarm details and repair suggestions.

### 4.2.5.12 Checking File System Status

Normal running of the file system services depends on the file system functionality. You can obtain the health status and operating status of a file system by checking the file system information.

## Impact on the System

A malfunctioning file system may interrupt system services and cause data loss.

## Reference Standard

If the status of a file system is normal, the following items are true on DeviceManager:

- **Health Status** of the file system is **Normal**, and **Running Status** is **Online**.
- No alarms about the file system are displayed on the **Current alarms** tab page.

## Precaution

None

## Procedure

**Step 1** On the navigation bar of DeviceManager, click  **Provisioning**.

The **Provisioning** page is displayed.

**Step 2** In the **File Storage Service** area, click **File System**.

The **File System** page is displayed.

**Step 3** Check file system status.

**Table 4-55** describes related parameters.

**Table 4-55** File system status parameters

Parameter	Description
Health Status	Health status of the file system. Possible values are: <ul style="list-style-type: none"><li>● <b>Normal</b>: The functions and running performance of the file system are normal.</li><li>● <b>Faulty</b>: The functions and running performance of the file system are abnormal.</li></ul>
Running Status	Operating status of the file system. Possible values are <b>Online</b> and <b>Offline</b> .

----End

## Exception Handling

If a new alarm about the file system is displayed on the **Current Alarms** tab page, select the alarm, and troubleshoot the fault according to the alarm details and repair suggestions.

### 4.2.5.13 Checking Optimization Feature Status

Optimization features directly affect the storage system performance and therefore need to be periodically checked.

## Prerequisites

Log in to DeviceManager as a read-only user.

## Procedure

**Step 1** In the navigation tree on the right, click  **Provisioning**.

The **Provisioning** page is displayed.

**Step 2** In the **Storage Configuration and Optimization** area, click **Resource Performance Tuning**.

The **Resource Performance Tuning** page is displayed.

**Step 3** Click an optimization feature that you want to view and check its status. If a fault occurs, report it to maintenance personnel for handling.

**Table 4-56** provides items for checking optimization features.

**Table 4-56** Items for checking optimization features

Optimization Feature	Feature Status Check Method
SmartTier	Check <b>Migration Status</b> , <b>Migration Triggering Mode</b> , <b>To Be Moved Up</b> , <b>To Be Moved Down</b> , and <b>Estimated Duration</b> of all storage pools for which SmartTier is configured.
SmartQoS	<ul style="list-style-type: none"><li>● On the <b>Priority Control</b> tab page, check <b>I/O Priority</b>, <b>Health Status</b>, and <b>Running Status</b> of LUNs, file systems, or snapshots.</li><li>● On the <b>Traffic Control</b> tab page, check <b>Status</b> and <b>Control Type</b> of a SmartQoS policy.</li></ul>
SmartPartition	View <b>Type</b> and <b>Read Partition Size</b> of a SmartPartition and check <b>Health Status</b> and <b>Running Status</b> of LUNs and file systems in the SmartPartition.
SmartCache	<ul style="list-style-type: none"><li>● On the <b>SmartCache Pool</b> tab page, view <b>Total Capacity</b> and <b>Used Capacity</b> of a SmartCache pool and check <b>Health Status</b> and <b>Running Status</b> of disks in the SmartCache pool.</li><li>● On the <b>SmartCache Partition</b> tab page, view <b>Expected Capacity</b> and <b>Used Capacity</b> of a SmartCache partition.</li></ul>
SmartMigration	Check <b>Running Status</b> of SmartMigration, including <b>Migrating</b> , <b>Migration completed</b> , <b>Migration fault</b> , <b>Normal</b> , and <b>Queuing</b> .

To view details, click  next to the table heading. From the drop-down list, select indicators you are concerned with.

----End

## 4.3 Collecting Storage System Information

After a fault occurs, find the cause and remove the fault by quickly collecting and reporting basic information, fault information, storage device information, network information, and application server information. Note that you must obtain the customer's prior 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 4-57** and send them to maintenance engineers.

**Table 4-57** 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.  <b>NOTE</b> You can log in to DeviceManager and query the serial number and version of the storage device in the <b>General</b> area.
	Customer information	Provide 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.
	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 status of the storage device indicators, especially the indicators in orange or red.  For details about indicator status, see the <i>Product Description</i> of the corresponding product model.
	System data	Manually export the operating data, and system logs of the storage device.
	Alarms and events	Manually export the alarms and events of the storage device.

Information Type	Item	Action
Network information	Connection mode	Describe the networking mode between application servers and the storage device, for example, Fibre Channel or iSCSI networking.
	Switch model	Record the switch models if any switches exist on the network.
	Switch diagnosis information	Manually export switch diagnosis information, including startup configurations, current configurations, interface information, time, and system versions. <b>NOTE</b> You must use the serial port to log in to the CLI and run the <b>display diagnostic-information</b> command to collect switch information. For details about this command, see the <i>CloudEngine 7800&amp;6800&amp;5800 Product Documentation</i> .
	Network topology	Describe the network topology or provide the network diagram.
	IP address information	Describe the IP address allocation principle or provide an IP address allocation list 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 port rate, see <i>Help</i> .
	Operating system logs	View and export the operating system logs.

### 4.3.2 Collecting Information on DeviceManager

You can use DeviceManager to collect system data, alarms, and events in the storage system.

#### 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 prevent the damage to the storage system caused by system faults and unexpected disasters. When a system failure occurs, the exported system data can be used to locate and analyze the failure. The system data to be exported includes running data, system logs, disk logs, storage resource, and diagnostic file.

#### Context

- Running data indicates the real-time running status of a storage system, such as, the configuration information of LUN. The running data file is in \*.txt format.

- System logs record the information about the running data, 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.
- DHA runtime log is the daily runtime log of disk. It mainly includes daily disk health status, I/O information, and disk service life. The DHA runtime log file is in \*.tgz format.
  - DHA logs collect the SMART/LogPage (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), and generate a package (1 KB) each day. A disk on a single controller can generate a maximum of 74 packages within a year (some old log packages will be deleted during the collection). Packages of a disk on a single controller and an information file will be exported each time.

 **NOTE**

You can run the **change dha policy collect\_start\_time=?** command in developer mode in the CLI to change the collection start time of DHA logs.

- Recommended times of export during routine maintenance are listed in the following table. The analysis of DHA logs is only performed on samples instead of all logs. To prevent the analysis of DHA logs from affecting the entire routine maintenance, take the recommended values only for reference.

Disk Quantity in an Array	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 log is working log of HSSD, such as, the S.M.A.R.T information and run logs of the disk. The HSSD log file is in \*.tgz format.
- Diagnostic files collect the device faults. The diagnostic files are in \*.tgz format.

Before the download of system logs, DHA runtime logs, or HSSD logs, the system collects those logs of controllers and shows the collection progress. 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.

---

## Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  Settings >  Export Data.

**Step 3** Export data.

- In **Running Data** area, click **Download**. 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 running data is exported.
- In **System Log** area, select **Recent logs** or **All logs**, and click **Log List**. Confirm the information in the security alert dialog box and 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 **Disk Log** area, click **DHA Runtime Log List**. Confirm the information in the security alert dialog box and 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 **Disk Log** area, click **HSSD Log List**. Confirm the information in the security alert dialog box and 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 **Diagnostic File** area, click **Export**. Confirm the information in the security alert dialog box, select **I have read and understood the consequences associated with performing this operation**, and click **OK**.  
The device faults are exported.

 **NOTE**

- In the **System Log** area, if **Recent logs** is selected, the system exports recent logs that have been generated by the current point in time. The logs include the latest one power-on and power-off log and a maximum of six messages logs. If **All logs** is selected, the system exports all logs on the current node. Note that historical messages logs are saved to the **/OSM/coffer\_log/log/his\_debug** directory.
- If you export the data using the Internet Explorer browser with the default settings, the data will be saved in the download path which the user has selected. For example, you can choose **Save > Save as** in the displayed file download dialog box and select the download path in Internet Explorer 9 browser.
- If you export the 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** and click the **General > Browser** in the **Options** dialog box to view the default download path.
- If you export the 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 **Customize and Control Google Chrome > Settings** and view the default download path in the **Download Content** area of the **Settings** page.
- When using Chrome to export for the first time, click **Allow** if the **This site is attempting to download multiple files. Do you want to allow this message?** message is displayed. Otherwise, at the upper right corner of the browser, choose **Customise and control Google Chrome > Settings > Privacy > Content Settings... > Automatic downloads > Manage exceptions**, select **Allow** in **Behaviour**, and click **Finished**. Then, reopen the web page and you can successfully download multiple files. Alternatively, delete **Block** from **Behaviour** and click **Finished**. Then, reopen the web page again and you can download multiple files. In such a case, a message asking whether to allow multiple files to be downloaded will be displayed.
- If the exported logs cannot be viewed, export the logs again. If the new logs still cannot be viewed, contact Huawei technical support.

**Step 4** Click **Close**.

----End

### 4.3.2.2 Exporting Alarms and Events

Alarms and events record the faults and events that occur during storage system operation. When 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 logs are saved in \*.xls files. After they are exported, do not modify the file content.

#### Procedure

**Step 1** Go to the **Alarms and Events** page.

1. On the right navigation bar of DeviceManager, click  **Monitor**.

2. On the left side, click **Alarms 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.
- On the **All Events** tab page, alarms of all severities are displayed. Alarms on the **Current Alarms** tab page are exported to **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 **Save As**. In the drop-down list, select **Save Selected** or **Save All**, and follow instructions to save alarms and events.

----End

### 4.3.3 Collecting Information in 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 when the upgrade or capacity expansion fails.

#### Prerequisites

- The FTP server or SFTP server is accessible to the storage system.
- The FTP service 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 configuration files need to be imported when anomalies occur, contact technical support.

## Procedure

- Step 1** Log in to the CLI of the storage system as the 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 server or SFTP server.

**Table 4-58** Parameter description

Parameter	Description	Value
<b>ip=?</b>	IP address of a File Transfer Protocol (FTP) server or a Secure File Transfer Protocol (SFTP) server to which you want to import a configuration file.	[Example] -
<b>user=?</b>	User name for logging in to an FTP server or an SFTP server.	[Example] The value contains 1 to 64 characters.
<b>password=?</b>	Password for logging in to an FTP server or an SFTP server.	[Example] The value contains 1 to 63 characters.
<b>db_file=?</b>	File name of and path to a configuration file on an FTP server or an SFTP server.	[Example] The file name extension must be <b>.dat</b> . If you specify a file name, the file name cannot contain any of the following characters: \ / : * ? " < >  .
<b>port=?</b>	ID of the employed port on an FTP server or an SFTP server.	[Example] The value ranges from 1 to 65535. <ul style="list-style-type: none"><li>● If the protocol is= FTP, the default value is 21.</li><li>● If the protocol is= SFTP, the default value is 22.</li></ul>
<b>protocol=?</b>	Protocol type.	[Example] The value can be <b>FTP</b> or <b>SFTP</b> . The default value is <b>SFTP</b> . To ensure the security of data transfer, you are advised to use SFTP.

Parameter	Description	Value
<b>clean_device_file=?</b>	Whether to delete a configuration file in the storage system memory after the configuration file has been exported to an FTP or SFTP server.	[Example] The value can be <b>yes</b> or <b>no</b> , where: <ul style="list-style-type: none"><li>● <b>yes</b>: The configuration file that resides in the storage system memory will be deleted after the configuration file is exported to an FTP server or an SFTP server.</li><li>● <b>no</b>: The configuration file that resides in the storage system memory will not be deleted after the configuration file is exported to an FTP server or an SFTP server.</li></ul> The default value is <b>yes</b> .

----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 correct and has been backed up.

##### Context

Storage system configuration information can be imported only on the command-line interface (CLI).

##### Precautions

- The type of configuration files to be imported is **\*.dat**. Do not modify exported configuration file contents.
- Do not perform any operation when importing configuration files.

##### 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 configuration files from the FTP server to the storage system.

 **NOTE**

For details about this command, see *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 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 the **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 ... > **MyTools** > **Storage** > **Routine Maintenance** > **Information Collection**.

The **Information Collection** dialog box is displayed.

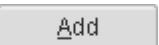
2. In the device list, select the device whose information you want to collect and click **Setting**.

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**.

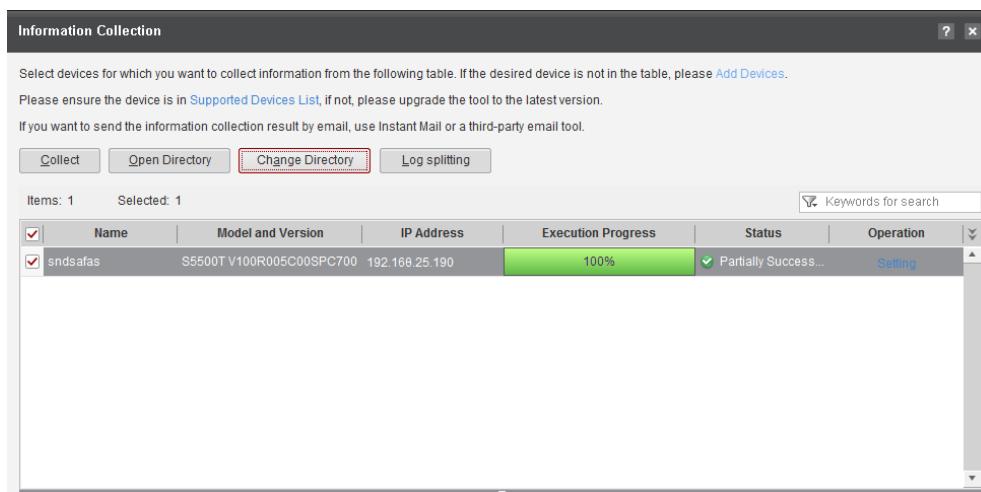
The device information collection setting is complete.

 **NOTE**

- The storage system can collect information such as system logs, alarm logs, operation data, disks, and electronic labels.
- 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 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

The 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 ... > **MyTools** > **Storage** > **Routine Maintenance** > **Collect Device Archives**.

The device archive information collection page is displayed.

**Step 3** For details about archive information collection operations, click  in the upper-right corner to obtain help.

----End

#### 4.3.4.3 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

- The 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.

##### Context

To use the information collection tool, you have two methods with the same function: directly using the tool or importing the tool to SmartKit. The following uses the latter method as an example to describe how to use the information collection tool.

- When the information collection tool is imported to SmartKit for utilization, installing JRE is not required.
- When directly using the information collection tool, install JRE first.

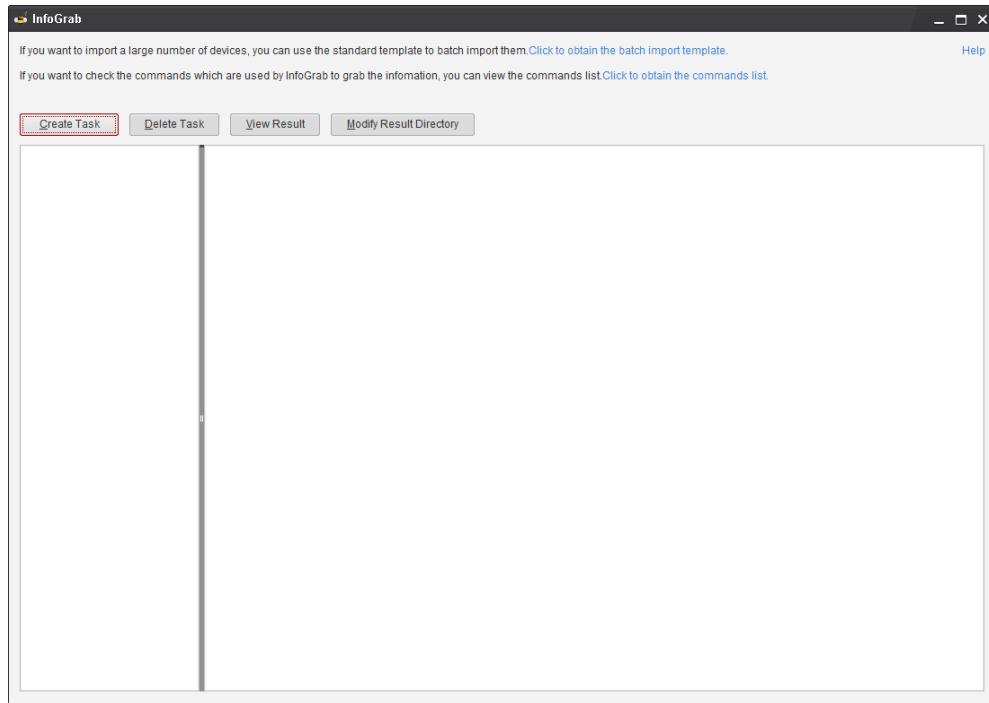
For details about how to download JRE, see *MigrationDirector InfoGrab Tool Operation Guide*.

##### Procedure

**Step 1** Start SmartKit.

**Step 2** Choose ... > **MyTools** > **Storage** > **Planning and Design** > **InfoGrab**.

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

#### 4.3.4.4 Analyzing Log Files Using SmartKit

When SmartKit is installed on a storage system and a log analysis tool is loaded, you can use the log analysis tool to analyze system logs exported from DeviceManager and results from an information collection tool, and have solutions to problems.

#### Prerequisites

- SmartKit has been installed on a maintenance terminal and a log analysis tool has been loaded.
- System log files have been exported from DeviceManager and related information files have been collected using the SmartKit information collection tool.

#### Procedure

**Step 1** Start SmartKit.

**Step 2** Choose ... > **MyTools** > **Storage** > **Routine Maintenance** > **Analyze Log**.

The log analysis tool page is displayed.

**Step 3** For details about log analysis operations, click **?** in the upper-right corner to obtain help.

----End

#### 4.3.5 Using a Script File to Collect Logs (OceanStor 18000 Series)

A script file can be used to collect system logs and Windows system logs in SVP.

### 4.3.5.1 Using a Script File to Collect System Logs

A script file can be used to collect system logs in SVP.

#### Prerequisites

- CLI and DeviceManager cannot be used to collect storage system logs.
- The storage system is working properly and can be connected using PuTTY.

#### Procedure

**Step 1** On the desktop, double-click the **export\_device\_log\_manually.bat** file.

The system starts the script that is used to collect system logs.

**Step 2** In **Please enter the IP address of the storage array whose log files you want to obtain:**, type the IP address of the storage system (for example **192.168.128.101**), and press **Enter**.

**Step 3** In **login as:**, type the user name for logging in to the storage system and press **Enter**.

**Step 4** In **password:**, type the password for logging in to the storage system and press **Enter**.

The script file automatically obtains system logs from the storage system. After system logs are collected, the following information is displayed:

```
"export log finished!"  
=====  
export log to "D:\log\192.168.128.101\20141223173923"
```

The **D:\log\192.168.128.101\20141223173923** is the location of the system logs.

**Step 5** Press any key to exit the script.

----End

### 4.3.5.2 Using a Script File to Collect Windows System Logs

A script file can be used to collect Windows system logs on the SVP. When the Windows operating system is working incorrectly or the management software deployed on the Windows operating system is working incorrectly, collect Windows system logs for troubleshooting.

#### Prerequisites

- You can log in to the Windows operating system running on the SVP using the maintenance terminal.
- Only administrators can execute the script.

#### Procedure

**Step 1** On the desktop of the Windows operating system, double-click the **WindowsInfoTool.bat** file.

The system starts the script that is used to collect system logs.

**Step 2** The script file automatically obtains log files. The following is displayed after the collection is complete:

```
Collect windows log successfully
=====
"export log to D:\SVP_Windows_log.rar"
=====
```

The **D:\SVP\_Windows\_log.rar** is the location of the system logs.

**Step 3** Press any key to exit the script.

**----End**

# 5 Routine Management

This chapter describes the routine management items for the storage system.

- [5.1 Powering on or off the Storage Device \(OceanStor 2000, 5000, and 6000 Series\)](#)
- [5.2 Powering on or off the Storage Device \(OceanStor 18000 Series\)](#)
- [5.3 Managing Access Permission of a Storage System](#)
- [5.4 Managing Alarm Notifications](#)
- [5.5 Enabling and Managing the Call Home Service \(Applicable to V300R006C10 and later\)](#)
- [5.6 Monitoring Storage System Performance](#)
- [5.7 Managing Basic Information About a Storage System](#)
- [5.8 Managing License Files](#)
- [5.9 Reclaiming Space of a Storage System](#)
- [5.10 Obtaining System Version Information](#)
- [5.11 Interconnecting Storage Devices with a Third-Party NMS](#)
- [5.12 Connection Change Between the Storage System and an Application Server](#)
- [5.13 Managing VMs \(OceanStor 18000 Series\)](#)
- [5.14 Expanding Storage Space](#)

## 5.1 Powering on or off the Storage Device (OceanStor 2000, 5000, and 6000 Series)

Powering on or off a storage device 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 a Device

This topic guides you through the process of re-powering on the storage device that has been powered off.

## Prerequisites

The storage device contains a disk enclosure with coffer disks.

## Precautions

- Before powering on the storage system for the first time or after clearance of the system configurations, ensure that controller A is correctly connected and inserted in the controller enclosure. Otherwise, the storage system cannot be correctly powered on.
- Do not wear any ESD wrist straps during a power-on to avoid electric shocks.
- Do not remove or insert any optical fibers, network cables, coffer disks, and interface modules during a power-on to avoid data loss.
- Do not online modify any expansion cable connections after the storage device has been powered on; otherwise, device failures may occur.
- Complete expansion cable connections for a newly added disk enclosure before you power on the enclosure. Also, do not modify any expansion cable connections after the new disk enclosure has been powered on; otherwise, device failures may occur.

Always respect the following power-on sequence:

1. Switch on external power supplies of the hardware components.
2. Press the power button on the controller enclosure.
3. Switch on Ethernet switches or Fibre Channel switches (If the Ethernet or fiber switch is configured, but not powered on).
4. Switch on application servers (If the application server is not powered on).

## Procedure

**Step 1** Check that all of the power cables have snapped into place.

**Step 2** Check the labels on the power cables and identify the power switches corresponding to those cables in the power distribution unit (PDU).

**Step 3** Sequentially switch on the identified power switches.

**Step 4** Switch on the controller enclosure.

### NOTE

- 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.
- During the power-on, the power indicator of the controller enclosure blinks until the storage device is fully powered on in 15 to 30 minutes.

----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 **Checking the Running Status of the Storage Device**. If you find an anomaly for any indicator, try to rectify it by referring to the *Event Reference* or *Troubleshooting*.

## 5.1.2 Powering off the Storage Device

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

The correct power-off sequence is: stopping services running on the storage device → holding down the power button for 5 seconds for the controller enclosure to be powered off → disconnecting the controller enclosure and disk enclosures from their external power supplies.

#### NOTE

When you want to power off a storage system with four or more controllers, press the Power button of any controller enclosure that houses the first four controllers for five seconds to power off the entire system.

To power off the storage device, you can either press and hold the controller enclosure's power button for 5 seconds or execute power-off operations on DeviceManager. This document exemplifies how to power off the storage device using DeviceManager.

### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  Settings >  Power Off Device.

**Step 3** Confirm the information in the displayed **security alert** dialog box and enter the password of the currently logged in user. 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.

---

**Step 4** Click **OK**.

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

**Step 5** Click **OK**. You have powered off the storage device.

**Step 6** Disconnect all power supplies from the controller enclosures and disk enclosures to power off the storage system.

----End

## 5.1.3 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  **Settings** >  **Restart System**.

**Step 3** Confirm the information in the displayed security alert dialog box and enter the password of the currently logged in user. 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 succeeded.

**Step 5** Click **OK**. You have restarted the storage device.

----End

## 5.1.4 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 human safety and prevent devices from damages.

---



#### NOTICE

Powering off the storage device in an irregular way may cause data loss or disrupt the services for other clients.

---

Follow the electricity guidelines for your equipment room when you power off the storage device.

## 5.1.5 Re-Powering on the Storage Device After an Emergency Power-off

Re-power on the storage device that was powered off upon 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.

## 5.1.6 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.

**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 succeeded.

**Step 6** Click **OK**. The interface module is powered on.

----End

## 5.1.7 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**.

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

**Step 8** Click **OK**. The interface module is powered off.

----End

## 5.1.8 Powering off a Disk Enclosure (Applicable to V300R006C20 and later)

If you want to power off a disk enclosure, perform operations described in this section.

### Context

This operation will power off all disks in the disk enclosure. Before performing this operation, determine whether the operation is necessary.

### Procedure

**Step 1** Log in to a storage system as the super administrator and run **change user\_mode current\_mode user\_mode=engineer**.

```
admin:/>change user_mode current_mode user_mode=engineer  
engineer:/>
```

**Step 2** Run **poweroff enclosure enclosure\_number=?** to power off a disk enclosure.

 **NOTE**

**enclosure\_number** is ID of a disk enclosure with the prefix DAE. You can run **show enclosure** command to query details of disk enclosures.

Power off the disk enclosure whose ID is **DAE000**. The command output varies depending on a specific product.

```
engineer:/>poweroff enclosure enclosure_number=DAE000  
DANGER: You are about to power off a disk enclosure.  
This operation will power off all disks in the disk enclosure.  
Suggestion: Before performing this operation, determine whether the operation is necessary.  
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

## Follow-up Procedure

Run **poweron enclosure enclosure\_number=?** command to power on the disk enclosure.

# 5.2 Powering on or off the Storage Device (OceanStor 18000 Series)

Powering on or off a storage device includes powering on or off interface modules and other hardware components. A correct procedure effectively avoids device damage caused by misoperations.

## 5.2.1 Powering on the Storage Device

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.



The service processor (SVP) starts automatically upon system power-on. You are not required to power on SVP independently.



### 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. Your PDUs can be either European standard or North American standard. Choose the correct power-on sequence according to the type of PDUs configured.

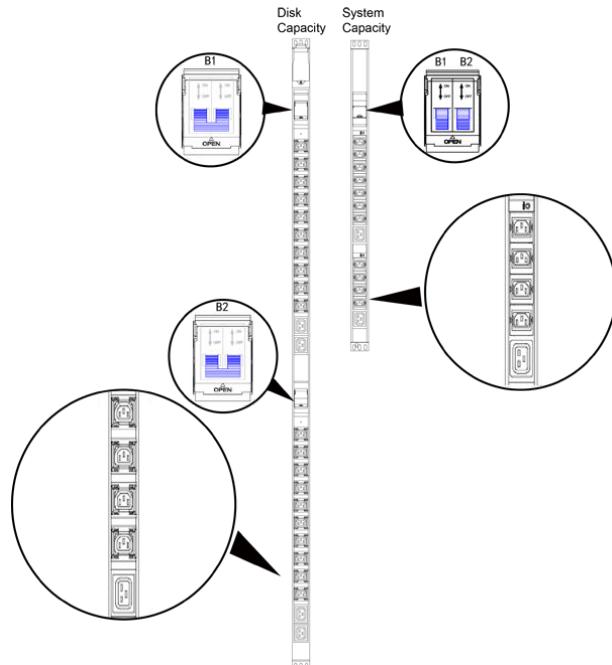
## Power-On Sequence for Systems Configured with European Standard PDUs

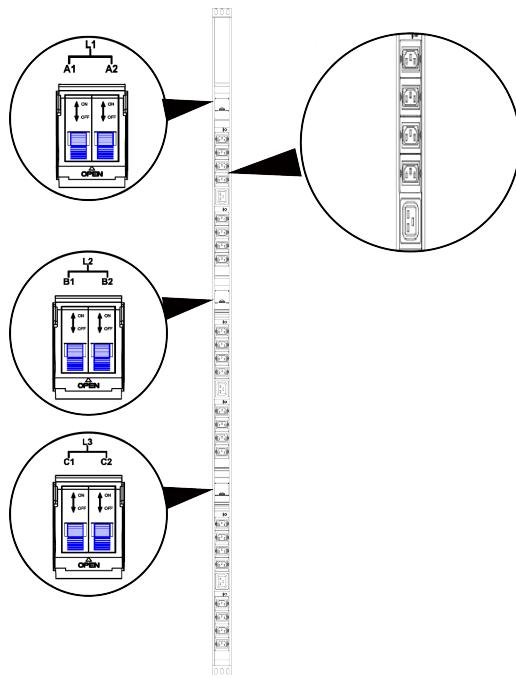
For a system configured with European standard PDUs, the correct power-on sequence is as follows:

1. Turn on switches of all disk bays without the necessity to follow any sequence.
  - For European standard PDU switches (single-phase, 220 V, 32 A), turn on the switches in a sequence of **B1 > B2**.
  - 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**.
2. 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**.
  - 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 5-1](#) and [Figure 5-2](#) shows the switches on a European standard PDU.

**Figure 5-1** Switches on a European standard PDU (single-phase 220 V, 32 A)



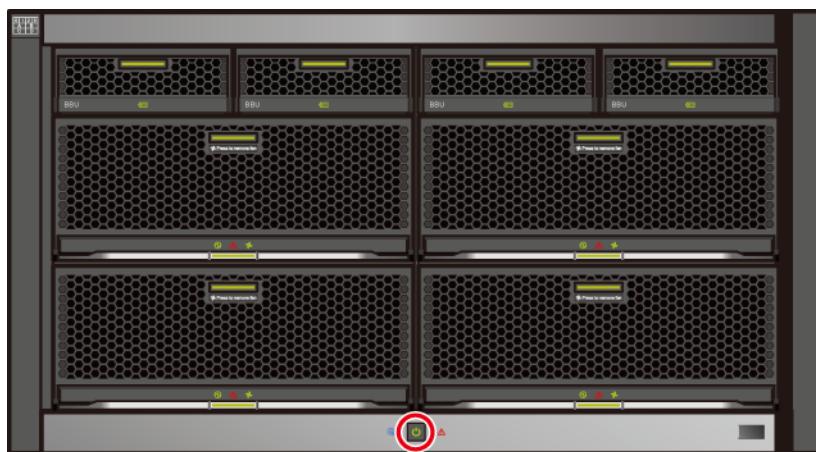
**Figure 5-2** Switches on a European standard PDU (three-phase 380 V, 32 A)

3. Press the power button of all engines, as shown in **Figure 5-3**.

**NOTE**

In a scenario with multiple controllers, all the controllers must be powered on within three minutes. If the engines 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 5-3** Power button on an engine

4. (Optional) If the KVM is not powered on, switch on the power button on the rear panel of the KVM to power on it.
5. After the KVM is powered on, enter your user name and password to log in to the KVM console. The default user name and password are empty. That is, you can log in to the

system by pressing **Enter** twice. After the login, select the channel that connects to the SVP to go to the Windows system (the default channel is 1).

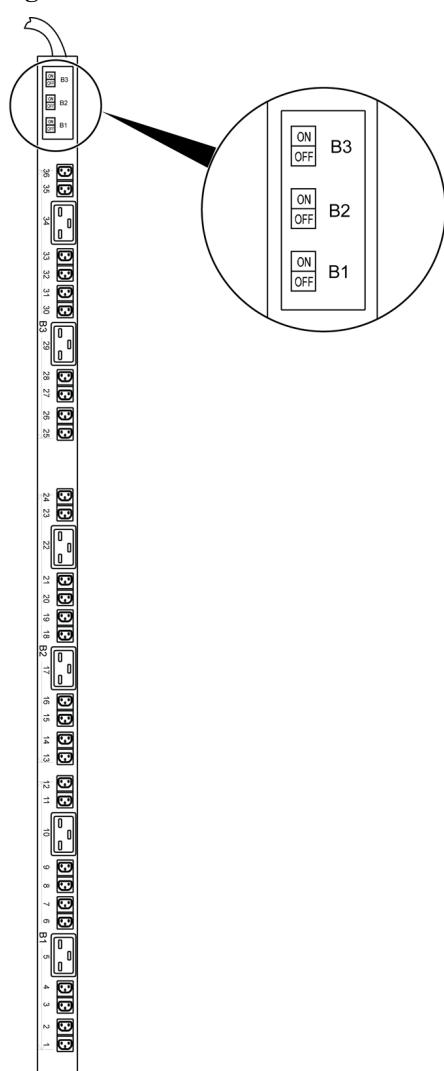
## Power-On Sequence for Systems Configured with North American Standard PDUs

For a system configured with North American standard PDUs, the correct power-on sequence is as follows:

1. Turn on switches of all disk bays without the necessity to follow any sequence.  
For North American standard PDU switches, turn on the switches in a sequence of **B1 > B2**.
2. Turn on PDU switches of the system bays from system bay 0 to system bay  $n$  in sequence.  
For North American standard PDU switches, turn on the switches in a sequence of **B1 > B2 > B3**.

**Figure 5-4** shows the switches on a North American standard PDU.

**Figure 5-4** Switches on a North American standard PDU



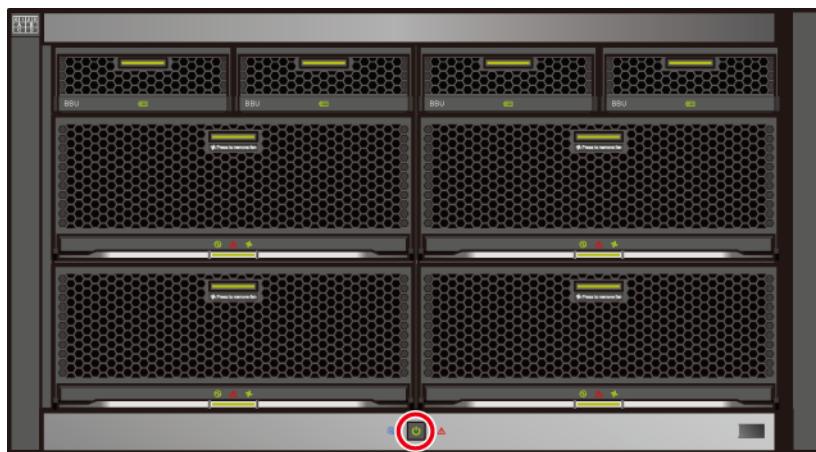
3. Press the power button of all engines, as shown in [Figure 5-5](#).

 **NOTE**

In a scenario with multiple controllers, all the controllers must be powered on within three minutes. If the engines 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 5-5** Power button on an engine



4. (Optional) If the KVM is not powered on, switch on the power button on the rear panel of the KVM to power on it.
5. After the KVM is powered on, enter your user name and password to log in to the KVM console. The default user name and password are empty. That is, you can log in to the system by pressing **Enter** twice. After the login, select the channel that connects to the SVP to go to the Windows system (the default channel is 1).

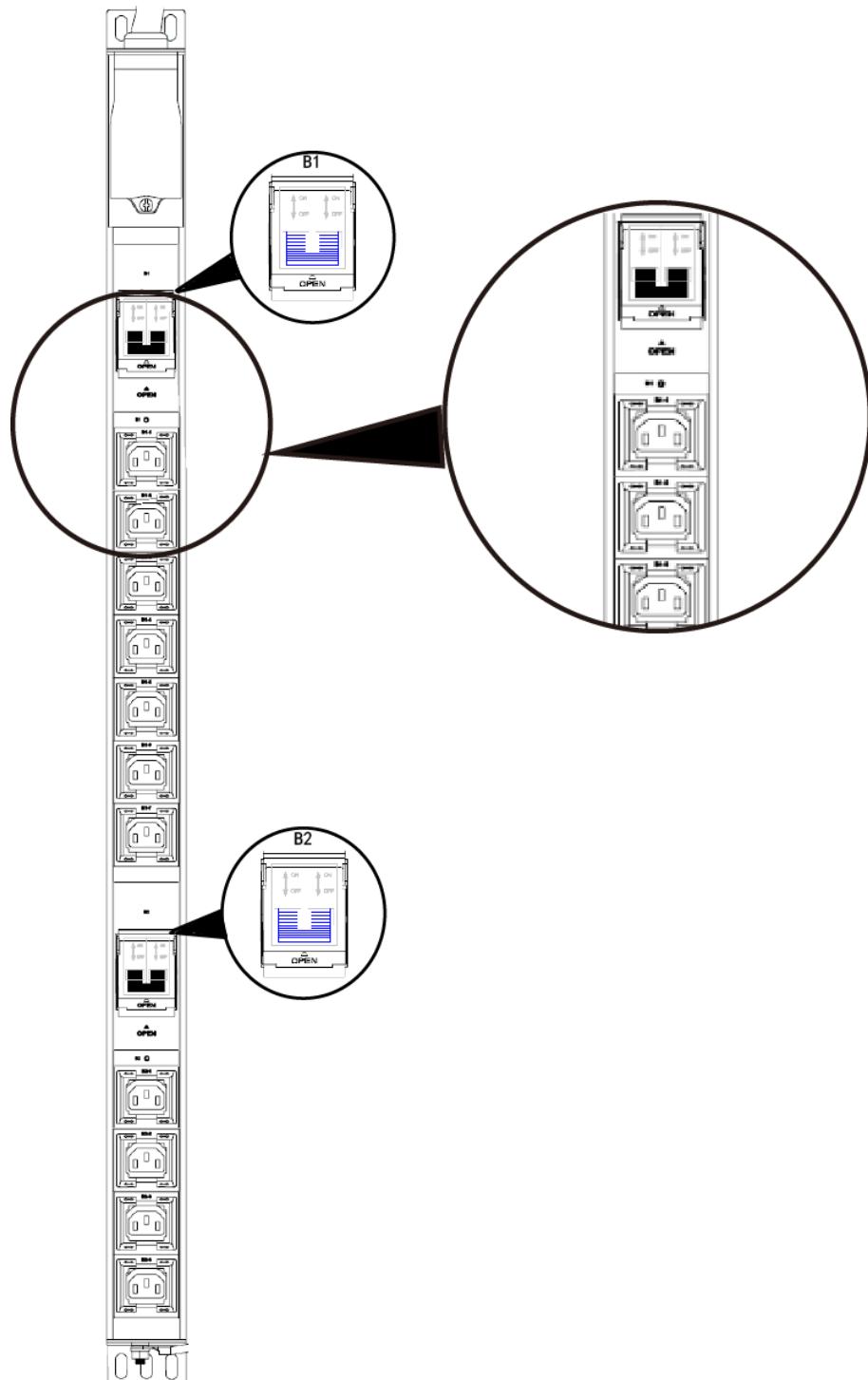
## Power-On Sequence for Systems Configured with High Voltage DC PDUs

For a system configured with high voltage DC PDUs, the correct power-on sequence is as follows:

1. Turn on switches of all disk bays without the necessity to follow any sequence.  
For HVDC PDU switches, turn on the switches in a sequence of **B1 > B2**.
2. Turn on switches of all system bays.  
For HVDC PDU switches, turn on the switches in a sequence of **B1 > B2**.

[Figure 5-6](#) shows the switches on a high voltage DC PDU.

**Figure 5-6** Switches on a high voltage DC PDU (240 V, 32 A)



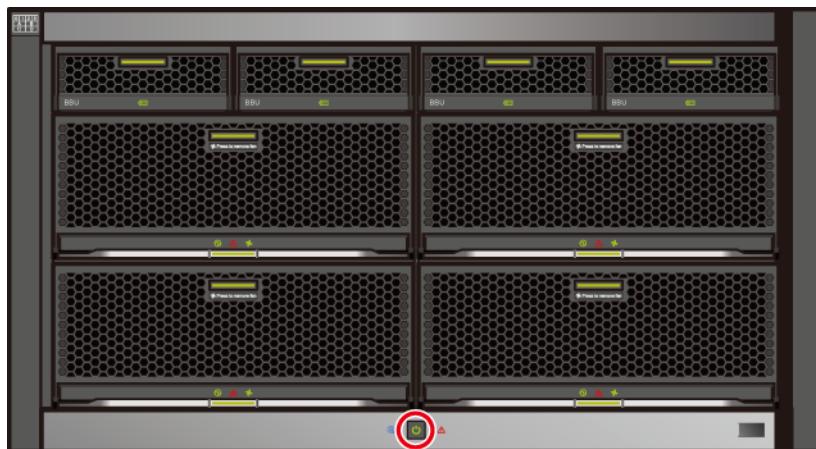
3. Press the power button of all engines, as shown in [Figure 5-7](#).

**NOTE**

In a scenario with multiple controllers, all the controllers must be powered on within three minutes. If the engines 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 5-7** Power button on an engine



4. (Optional) If the KVM is not powered on, switch on the power button on the rear panel of the KVM to power on it.
5. After the KVM is powered on, enter your user name and password to log in to the KVM console. The default user name and password are empty. That is, you can log in to the system by pressing **Enter** twice. After the login, select the channel that connects to the SVP to go to the Windows system (the default channel is 1).

## Sequence for Powering on DC PDBs (Four Controllers)

Power supplied to the entire storage system can be controlled using switches on the DC PDBs. Each bay has two DC PDBs. One is located between 36 U and 37 U, and the other one is located between 39 U and 40 U.

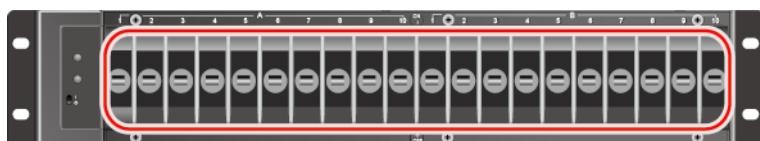
**NOTE**

OceanStor 18000 series storage systems support DC power modules.

1. Turn on the switches of each DC PDB in all disk bays. There is no sequence requirement.

**Figure 5-8** shows the switches of a DC PDB.

**Figure 5-8** Switches of a DC PDB



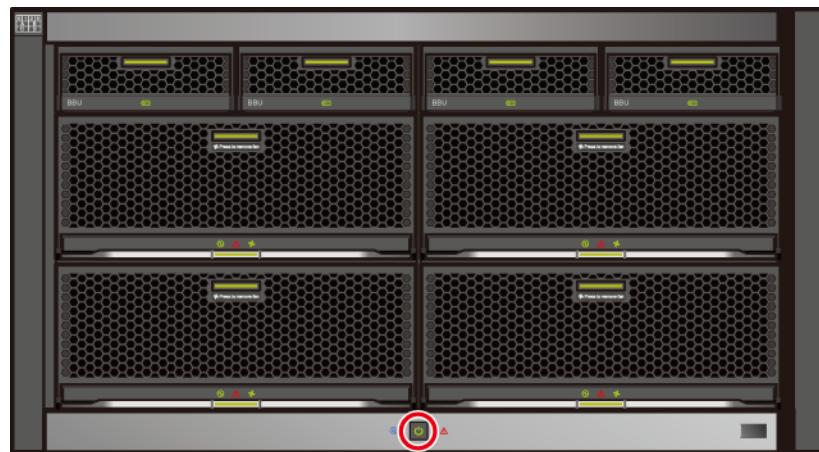
2. Turn on the switches of each DC PDB in all system bays.
3. Press the power button of all engines, as shown in [Figure 5-9](#).

 **NOTE**

In a scenario with multiple controllers, all the controllers must be powered on within three minutes.

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 5-9** Power button on an engine



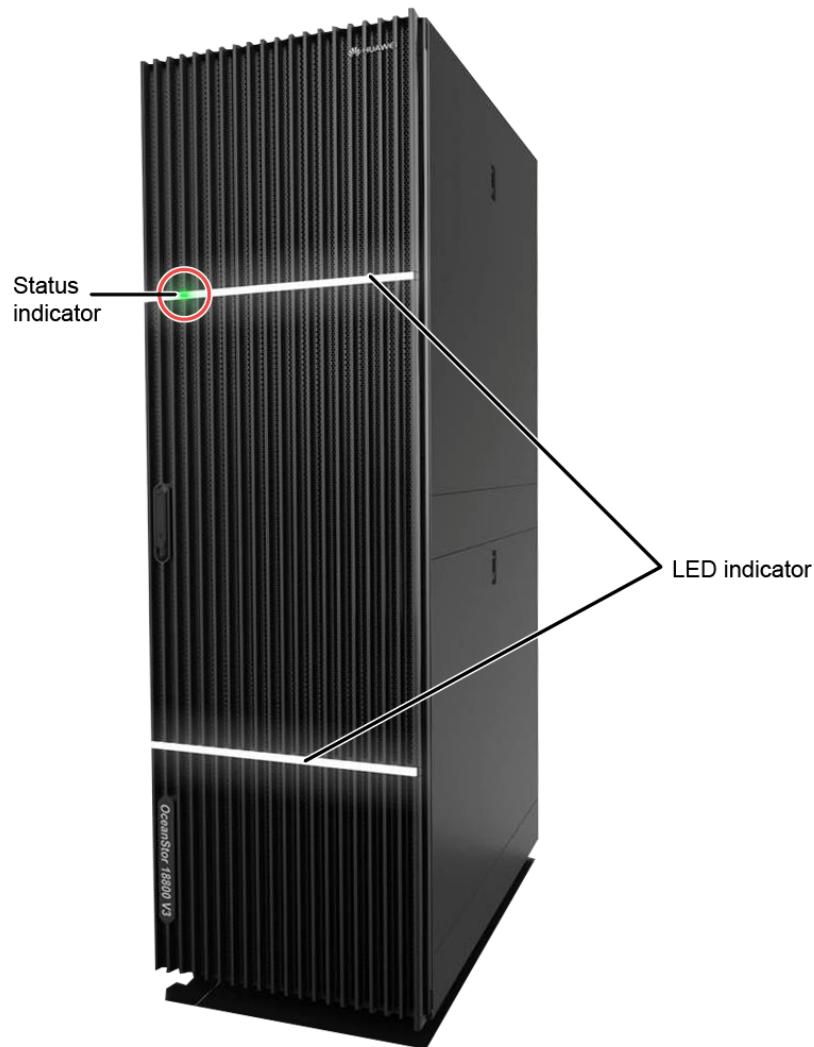
 **NOTE**

The power-on of the storage system takes 15 to 30 minutes.

## Power-On Check

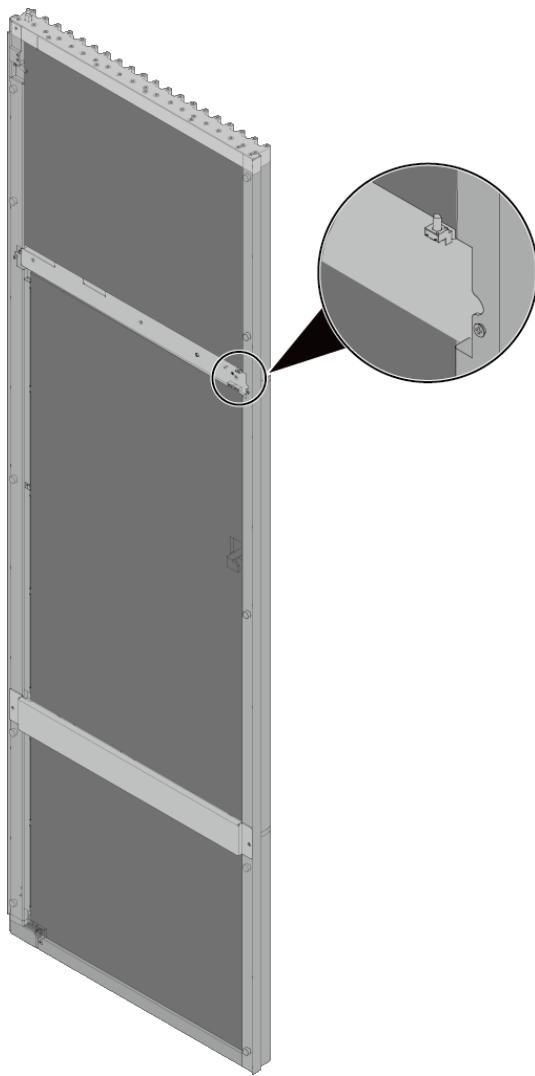
When the system is successfully powered on, the status indicator on the front door of system bay 0 is steady green, as shown in [Figure 5-10](#).

**Figure 5-10** Bay indicator



The LED indicator is for decoration only. If you want to turn off the LED indicator, you can turn off the LED indicator switch on the back of the bay's front door, as shown in [Figure 5-11](#).

**Figure 5-11** LED indicator switch



## 5.2.2 Powering off the Storage System

The storage system power-off sequence is to first power off storage devices and then turn off PDU switches. Respect the power-off sequence when you power off storage devices for not using them, replacing cabinet enclosures, or responding power link failures. The storage system power-off sequence is to first power off storage devices and then turn off PDU switches.

### Prerequisites

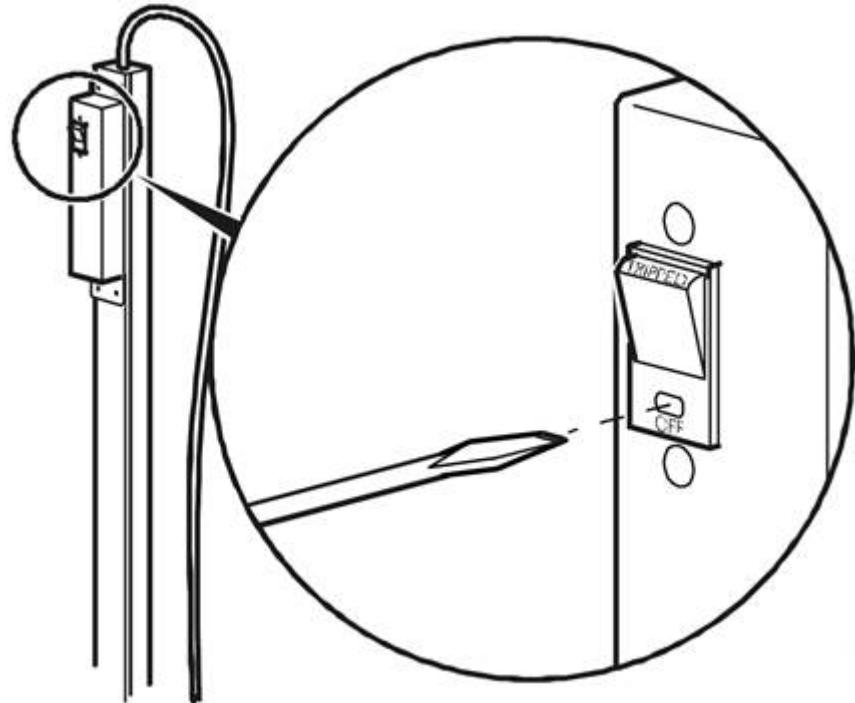
No service is running on the storage system.

### Context

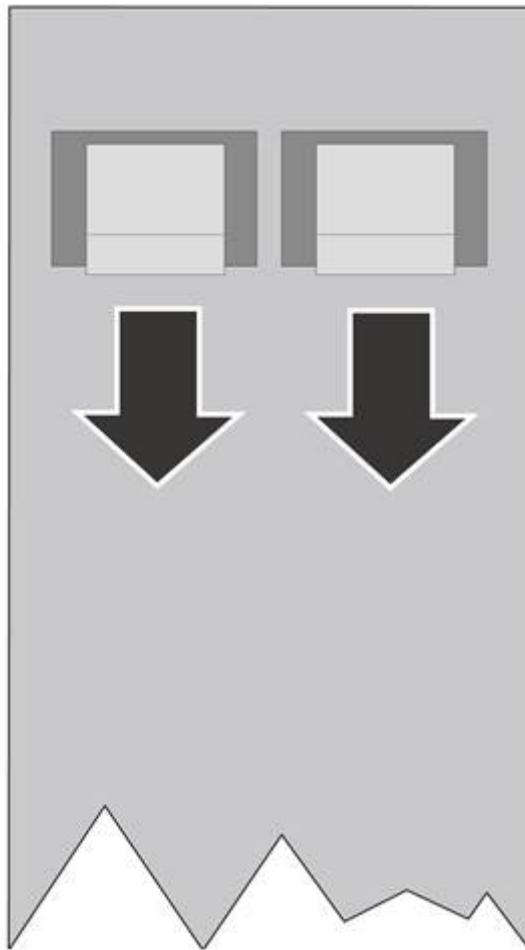
The operation of turning off PDU switches varies based on types of PDUs configured.

- 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 **Settings** > **Power Off Device**.
3. Confirm the information in the displayed **Danger** dialog box, enter the password of the currently logged on user, and then select **I have read and understand the consequences associated with performing this operation**.



## WARNING

If you enter the wrong password three times in succession within 5 minutes, the current user will be logged out and exit DeviceManager.

1. Click **OK**.

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

2. Click **OK**. You have powered off the storage device.

**Step 2** Turn off the PDU switches in every bay in the right sequence.

- The sequence to turn off the PDU switches is as follows:
  - When the system is equipped with disk bays, first turn off the PDU switches on the system bays, then on the disk bays.
  - Turn off the PDU switch on all system bays from system bay 0 to system bay *n* in sequence.

### NOTE

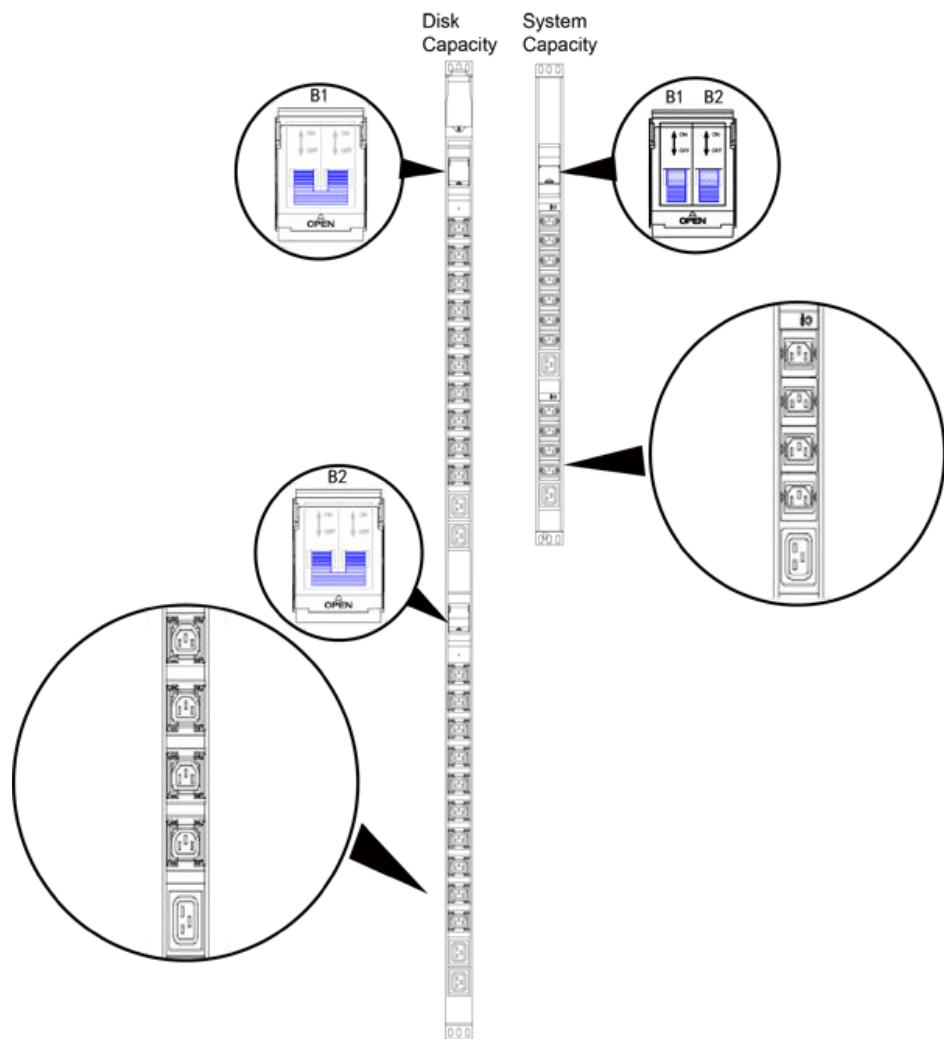
For details about turning off PDU switches, refer to context.

- You can turn off the storage system that is configured with European standard PDU switches as follows:
  - a. 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**.
  - b. Turn off PDU switches of the disk bays.
    - 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**.

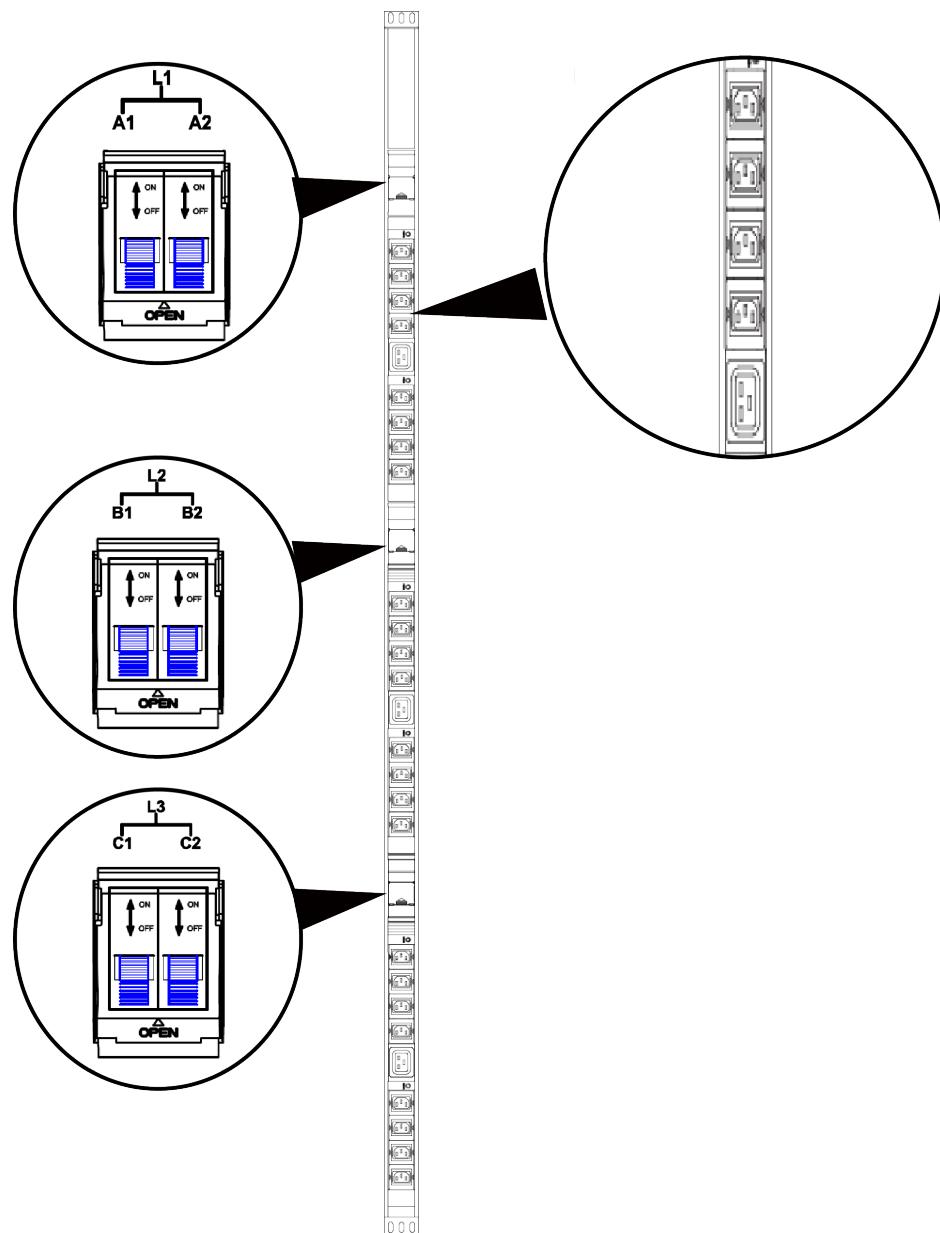
[Figure 5-12](#) and [Figure 5-13](#) shows switches on a European standard PDU switches.

----End

**Figure 5-12** Switches on a European standard PDU (single phase, 220 V, 32 A)

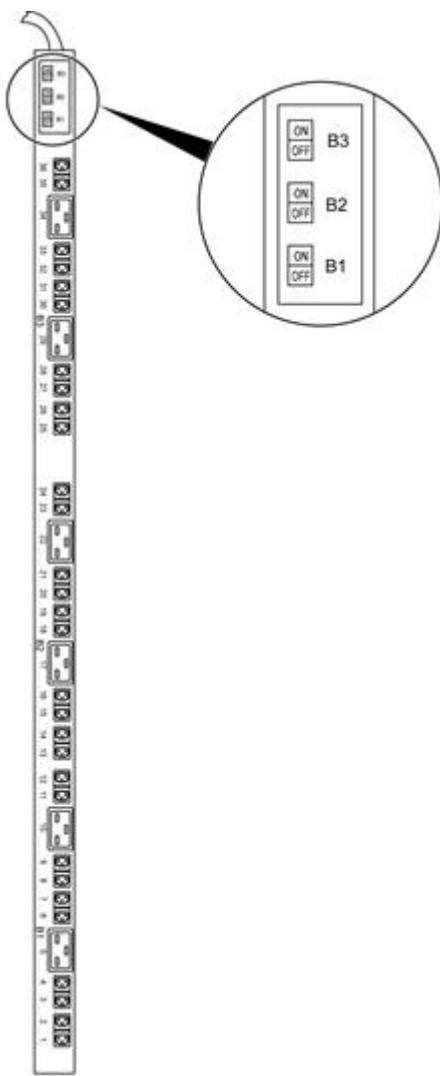


**Figure 5-13** Switches on a European standard PDU (three-phase, 380 V, 32 A)



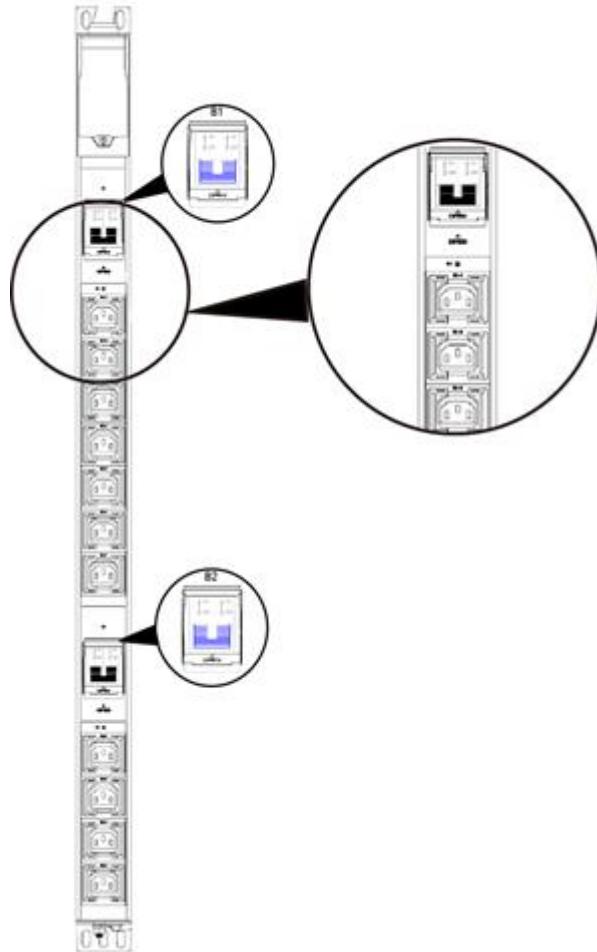
- You can turn off the storage system that is configured with North American standard PDU switches.
    - a. Turn off PDU switches of the system bays from system bay 0 to system bay n in sequence.  
For North American standard PDU switches, turn off the switches in a sequence of **B3 > B2 > B1**.
    - b. Turn off PDU switches of the disk bays.  
For North American standard PDU switches, turn off the switches in a sequence of **B3 > B2 > B1**.
- North American standard PDU switches are as shown in Figure 5-14.

**Figure 5-14** Switches on a North American standard PDU



- You can turn off the storage system that is configured with HVDC PDU switches as follows:
  - a. 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**.
  - b. Turn off PDU switches of the disk bays.  
For HVDC PDU switches, turn off the switches in a sequence of **B2 > B1**.HVDC PDU switches are as shown in Figure 5-15.

**Figure 5-15** Switches on an HVDC PDU (240 V, 32 A)



----End

### 5.2.3 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   **Settings** >  **Restart Device**.

- Step 3** Confirm the information in the displayed security alert dialog box and enter the password of the currently logged in user. 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 succeeded.

- Step 5** Click **OK**. You have restarted the storage device.

----End

### 5.2.4 Restarting the SVP

If you want to restart the SVP, perform operations described in this section.

#### Procedure

- Step 1** Log in to DeviceManager.

- Step 2** Choose **Settings** > **Restart SVP**.

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

- Step 4** Click **OK**.

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

- Step 5** Click **OK**. You have restarted the storage device.

----End

### 5.2.5 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 human safety and prevent devices from damages.



## NOTICE

Powering off the storage device in an irregular way may cause data loss or disrupt the services for other clients.

---

Follow the electricity guidelines for your equipment room when you power off the storage device.

## 5.2.6 Re-Powering on the Storage Device After an Emergency Power-off

Re-power on the storage device that was powered off upon 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.

## 5.2.7 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.

**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 succeeded.

**Step 6** Click **OK**. The interface module is powered on.

----End

## 5.2.8 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**.

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

**Step 8** Click **OK**. The interface module is powered off.

----End

## 5.2.9 Powering off a Disk Enclosure (Applicable to V300R006C20 and later)

If you want to power off a disk enclosure, perform operations described in this section.

### Context

This operation will power off all disks in the disk enclosure. Before performing this operation, determine whether the operation is necessary.

### Procedure

**Step 1** Log in to a storage system as the super administrator and run **change user\_mode current\_mode user\_mode=engineer**.

```
admin:/>change user_mode current_mode user_mode=engineer  
engineer:/>
```

**Step 2** Run **poweroff enclosure enclosure\_number=?** to power off a disk enclosure.



**enclosure\_number** is ID of a disk enclosure with the prefix DAE. You can run **show enclosure** command to query details of disk enclosures.

Power off the disk enclosure whose ID is **DAE000**. The command output varies depending on a specific product.

```
engineer:/>poweroff enclosure enclosure_number=DAE000  
DANGER: You are about to power off a disk enclosure.  
This operation will power off all disks in the disk enclosure.  
Suggestion: Before performing this operation, determine whether the operation is necessary.  
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

## Follow-up Procedure

Run **poweron enclosure enclosure\_number=?** command to power on the disk enclosure.

## 5.3 Managing Access Permission of a Storage System

To ensure device and service data security, the storage systems support security policy adjustment, IP address access control, and user management.

### 5.3.1 Configuring a Security Policy for System User

You can set the username and password policies to control the username and password complexity of new accounts. The login policy enables the system to lock the accounts with security exceptions.

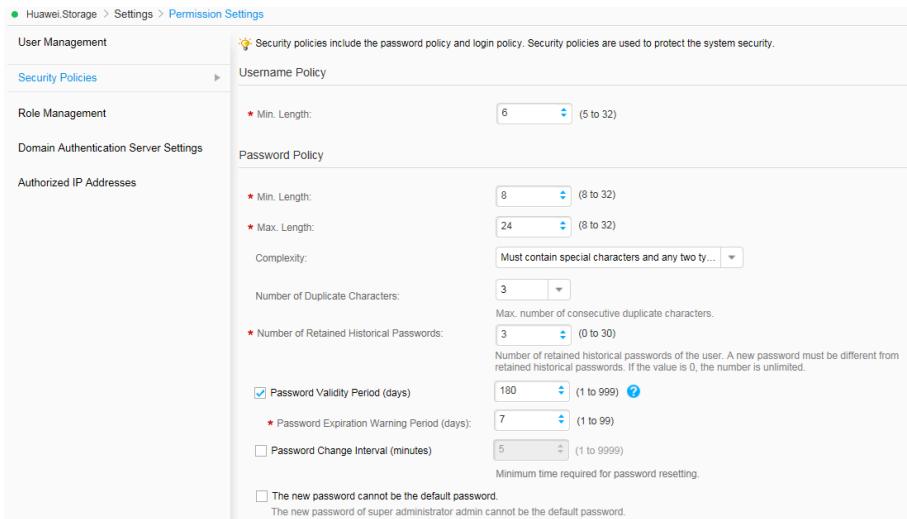
#### Context

The storage system supports the following password policies to ensure account security.

- The storage system supports strong password complexity to prevent brute-force password cracking.
- Passwords must be encrypted before they are stored and transferred.
- Passwords can be changed only after authentication and users can only change their own passwords.

#### Procedure

1. Log in to DeviceManager.
2. Choose  **Settings** >  **Permission Settings** > **Security Policies**.
  - a. On the right navigation bar, click  **Settings**.
  - b. In the **Basic Service Settings** area on the function pane, click  **Permission Settings**.  
The **Security Policies** page is displayed.
  - c. In the left navigation tree, select **Security Policies**.  
The **Security Policies** page is displayed.



3. **Table 5-1**, **Table 5-2**, **Table 5-3**, and **Table 5-4** describe the parameters related to configuration of user name, password, login, and account audit policies.

**Table 5-1** User name policy

Parameter	Description	Value
Min. length	Minimum length of a user name. The user name cannot be too simple.	[Value range] The value is an integer ranging from 5 to 32. [Example] 6

**Table 5-2** Password policies

Parameter	Description	Value
Min. Length	Minimum length of a password, avoiding too short passwords.	[Value range] The value is an integer ranging from 8 to 32. [Example] 8
Max. Length	Maximum length of a password, avoiding too long passwords.	[Value range] The value is an integer ranging from 8 to 32. [Example] 16

Parameter	Description	Value
Complexity	Complexity of the password, avoiding too simple passwords.	[Value range] The password must contain special characters and at least two types among uppercase letters, lowercase letters, and digits, or the password must contain special characters, uppercase letters, lowercase letters, and digits. [Example] The password must contain special characters and at least two types among uppercase letters, lowercase letters, and digits.
Number of Duplicate Characters	Maximum number of consecutive same characters in a password.	[Value range] The value is not restricted or the value is an integer ranging from 1 to 9. [Example] 3
Number of Retained Historical Passwords	Number of historical passwords retained for a user. The new password must be different from the historical passwords. If the value is 0, there is no restriction.	[Value range] The value is an integer ranging from 0 to 30. [Example] 3
Password Validity Period (days)	Setting of a password's validity period.  <b>After Password Validity Period (days)</b> is enabled, you must set the days in which a password is valid. After the validity period of the password expires, the system prompts you to change the password in a timely manner.  <b>NOTE</b> If this parameter is not selected, the password will never expire. To ensure storage system security, you are advised to select and set this parameter.	[Value range] The value is an integer ranging from 1 to 999. [Example] 90

Parameter	Description	Value
Password Expiration Warning Period (days)	Number of days prior to password expiration that the administrator receives a warning message.	[Value range] The value is an integer ranging from 1 to 99.  [Example] 7
Min. Password Lifespan (minutes)	Minimum lifespan of a new password.	[Value range] The value is an integer ranging from 1 to 9999.  [Example] 5
The new password cannot be the default password.	The new password of the super administrator admin cannot be the default password.	[Value range] Enable or Disable  [Example] Enable

**Table 5-3** Login policies

Parameter	Description	Value
Session Timeout Duration (minutes)	Duration after which the system indicates timeout if a logged-in administrator performs no operations during the period. After you click <b>OK</b> in the event of timeout, the system returns to the login page.	[Value range] The value is an integer ranging from 1 to 100.  [Example] 30
Password Lock	Locks a user if the count of consecutively inputting incorrect passwords by the user exceeds Number of Incorrect Passwords within 10 minutes.	[Value range] Enable or Disable  [Example] Enable

Parameter	Description	Value
Number of Incorrect Passwords	<p>Times allowed for consecutively entering incorrect passwords. The system automatically locks a user if the times of consecutively inputting incorrect passwords by the user exceed <b>Number of Incorrect Passwords</b>.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>● This parameter is available only when <b>Password Lock</b> is enabled.</li> <li>● After a user is locked, the super administrator can manually unlock the user. If <b>Lock Mode</b> is set to <b>Temporary</b>, the user will be automatically unlocked when the unlock time arrives.</li> </ul>	<p>[Value range] The value is an integer ranging from 1 to 9. [Example] 3</p>
Lock Mode	<p>Mode of automatically locking a user.</p> <ul style="list-style-type: none"> <li>● In <b>Permanent</b> mode, administrators and read-only users are locked permanently. The super administrator will be automatically unlocked after 15 minutes.</li> <li>● In <b>Temporary</b> mode, you can set a duration of locking administrators and read-only users.</li> </ul>	<p>[Value range] Temporary or Permanent [Example] Temporary</p>
Automatic Lock Duration (minutes)	<p>Duration of locking a user. After the lock duration expires, the locked user is automatically unlocked.</p> <ul style="list-style-type: none"> <li>● This parameter is available only when <b>Password Lock</b> is enabled and <b>Lock Mode</b> is <b>Temporary</b>.</li> <li>● This parameter is available to automatic lock only. This parameter is unavailable if a user is manually locked. The user can be manually unlocked only.</li> <li>● Automatic unlock is only applicable to administrators and read-only users. The super administrator will be automatically unlocked after 15 minutes in both <b>Permanent</b> and <b>Temporary</b> modes.</li> </ul>	<p>[Value range] The value is an integer ranging from 3 to 2000. [Example] 15</p>
Lock Account When Idle	A system account will be locked if it is not used for login and the idle period exceeds the specified days.	<p>[Value range] Enable or Disable [Example] Enable</p>

Parameter	Description	Value
Idle Period (days)	Idle days of a system account.	[Value range] The value is an integer ranging from 1 to 999. [Example] 60
Login Security Info	After a user login, information about the last login (including the login time and IP address) is displayed.	[Value range] Enable or Disable [Example] Enable
User-Defined Info	After an account's successful login, an alarm is displayed indicating the preset information.	[Value range] Enable or Disable [Example] Enable
Info	The information to prompt the successful login of user account.	[Value range] The information contains 1 to 511 characters. [Example] Login successful

**Table 5-4** Account audit policies

Parameter	Description	Value
User Account Audit	Periodically audits the number and permission of user accounts to ensure account security.	[Value range] Enable or Disable [Example] Enable
Audit Period (Days)	Period of auditing the user accounts.	[Value range] The value is an integer ranging from 0 to 999. [Default] 120

4. Confirm the security policy configuration.
  - a. Click **Save**.  
The **Execution Results** dialog box is displayed, indicating that the security policy configuration succeeds.
  - b. Click **Close**.

## 5.3.2 Configuring Authorized IP Addresses

You can specify the IP addresses that can access the device from DeviceManager to prevent unauthorized access.

### Prerequisites

You are a super administrator. Only super administrators have the permission to perform this operation.

### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Settings** >  **Permission Settings** > **Authorized IP Addresses**.

**Step 3** Authorize IP addresses.

1. Select **Enable**.
2. Click **Add**.

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



3. Enter the IP segment or IP address that can access the storage device.
  - To authorize an IP address segment, select **IP address segment** and set **Start IP Address** and **End IP Address**. IP addresses included in the IP address segment are allowed to access the storage device.
  - To authorize IP addresses, select **IP address** and set **IP Address**.
4. Click **OK**. The specified IP segment or IP address is added to the IP address segment/IP address list.



After this function is enabled, if you want to prevent one IP address or IP address segment from accessing devices, select the IP address or IP address segment from the IP address/IP address segment list and click **Remove**. Note that at least one IP address or IP address segment must be allowed access.

5. Click **Save**, read and confirm the prompt information.

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

**Step 4** Click **Close**.

----End

## 5.3.3 Managing Users and Their Access Permissions

To prevent misoperations from affecting device stability and service data security, the storage device defines three user levels, each with certain permission.

### 5.3.3.1 Creating a Local User

To ensure device stability and service data security, a super administrator can create different levels of users based on service requirements.

#### Context

- For the user levels and roles, see [1 User Levels, Roles, and Permission](#).
- The storage system supports a maximum of 32 system users, among which a maximum of two super administrators can be created.

#### Procedure

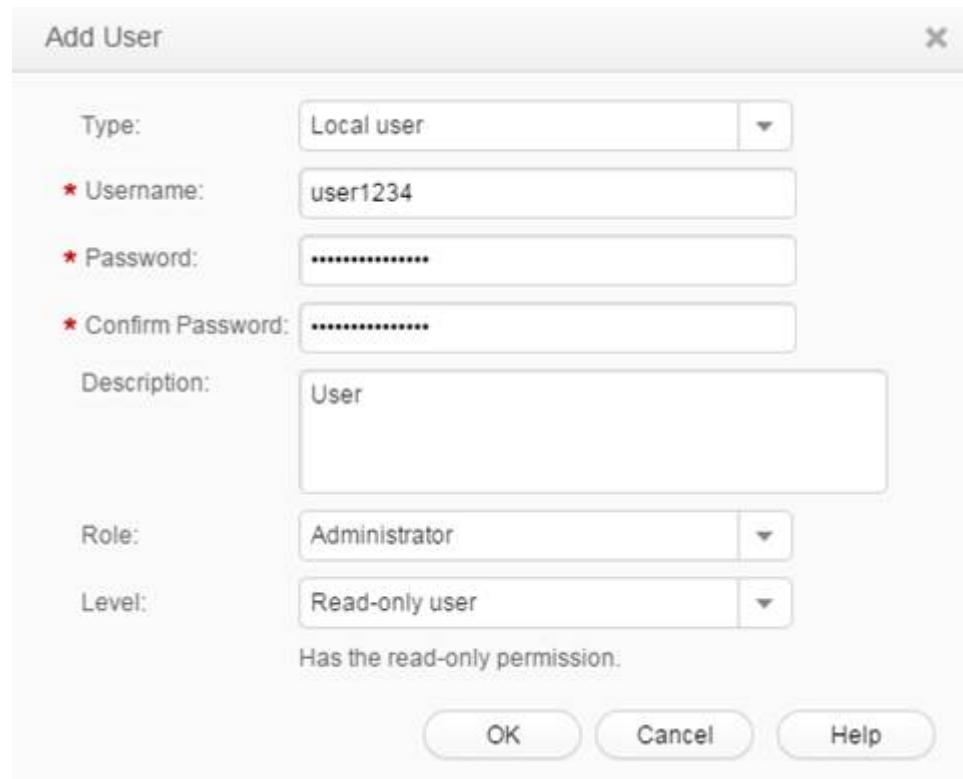
**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Settings** >  **Permission Settings** > **User Management**.

**Step 3** In the right function pane, click **Add**.

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

**Step 4** Set user information. Select **Local user** in **Type** and configure relevant parameters.



**Table 5-5** describes the local user parameters.

**Table 5-5** Local user parameters

Parameter	Description	Value
Username	Name of a newly created user.  <b>NOTE</b> You can modify the username policy in <b>Permission Settings &gt; Security Policies</b> .  <b>[Example]</b> user1234	[Value range] <ul style="list-style-type: none"><li>● The name contains 5 to 32 characters.</li><li>● The name can only contain letters, digits, and underscores (_) and must start with a letter.</li><li>● The username must be unique.</li></ul>

Parameter	Description	Value
Password	Password of a newly created user.	[Value range] <ul style="list-style-type: none"><li>● The password contains 8 to 32 characters.</li><li>● The password must contain special characters. Special characters include !"#\$%&amp;'()*+,-./;:&lt;=&gt;?@[\\]^`{_{_}}~ and spaces.</li><li>● The password must contain any two types of uppercase letters, lowercase letters and digits.</li><li>● The maximum number of consecutive same characters cannot exceed 3.</li><li>● The password cannot be the same as the username or the username typed backward.</li></ul> <p><b>NOTE</b></p> <ul style="list-style-type: none"><li>● You can modify the password policy in <b>Permission Settings &gt; Security Policies</b>.</li><li>● Keep your password safe.</li></ul> <p>[Example]</p> <p>a#123456</p>
Confirm password	Password for confirmation.	[Value range] The value must be the same as that of <b>Password</b> . <p>[Example]</p> <p>a#123456</p>
Description	Description of a newly created user.	[Example] User
Role	Set permissions for users. You can select a built-in role or create a self-defined role.	[Example] Administrator

Parameter	Description	Value
Level	<p>Level of a user. Possible values are as follows:</p> <ul style="list-style-type: none"><li>● Super administrator: has full administrative permissions on the storage device, and is able to create the users at all user levels.</li><li>● Administrator: has partial system administration permissions. Specifically, they cannot manage users, upgrade storage devices, modify system time, restart devices, or power off devices.</li><li>● Read-only user: has only the access permission for the storage system and can perform queries only.</li></ul>	[Example] Read-only user

**Step 5** Confirm the user account creation.

1. Click **OK**.

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

2. Click **OK**.

----End

### 5.3.3.2 Creating a Domain User

DeviceManager allows users to log in to the storage system using the Lightweight Directory Access Protocol (LDAP) server authentication mode to centrally manage user information.

#### Context

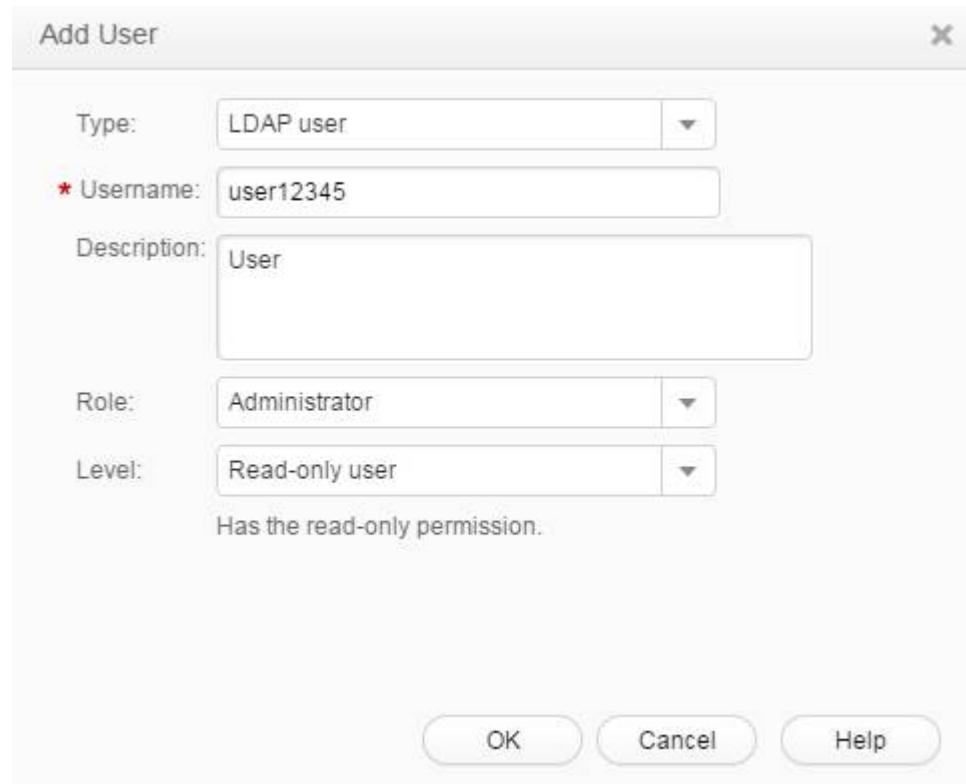
- For the user levels and roles, see [1 User Levels, Roles, and Permission](#).
- The storage system supports a maximum of 32 system users, among which a maximum of two super administrators can be created.

#### Procedure

**Step 1** Log in to DeviceManager.**Step 2** Choose **Settings** > **Permission Settings** > **User Management**.**Step 3** In the right function pane, click **Add**.

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

**Step 4** Set user information. Select **LDAP user** or **LDAP user group** in **Type** and configure the relevant parameters. **Table 5-6** describes the parameters.



**Table 5-6** LDAP user or LDAP user group parameters

Parameter	Description	Value
Username	Name of a newly created LDAP user or LDAP user group. <b>NOTE</b> The LDAP user or LDAP user group to be created must reside on the LDAP domain server. Otherwise, the login will fail.	[Value range] ● The username contains 1 to 64 characters. ● The username must be unique. [Example] user12345
Description	Description of a newly created user.	[Example] User
Role	Set permissions for users. You can select a built-in role or create a self-defined role.	[Example] Administrator

Parameter	Description	Value
Level	<p>Level of a newly created LDAP user or LDAP user group. Possible values are as follows:</p> <ul style="list-style-type: none"><li>● <b>Administrator:</b> has partial system administration permissions. Specifically, they cannot manage users, upgrade storage devices, modify system time, restart devices, or power off devices.</li><li>● <b>Read-only user:</b> has only the access permission for the storage system and can perform queries only.</li></ul>	[Example] Read-only user

**Step 5** Confirm the user account creation.

1. Click **OK**.

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

2. Click **OK**.

----End

### 5.3.3.3 Managing User Levels

A super administrator can change the level of a read-only user or an administrator according to the actual requirements.

#### Prerequisites

- Only super administrators have the right to perform this operation.
- The super administrator can modify the level and initiate the password only for users whose **Status** is **Offline**.

#### Context

User levels include:

- **Administrator:** has permission to control the storage device and modify password of administrator, but cannot manage users, upgrade the storage device, modify system time, activate license files, restart device, or power off device. Administrator cannot import or export license files.
- **Read-only user:** has permission to access the storage device and change its password. After logging in to the storage device, the read-only user can only query device information but cannot perform other operations.

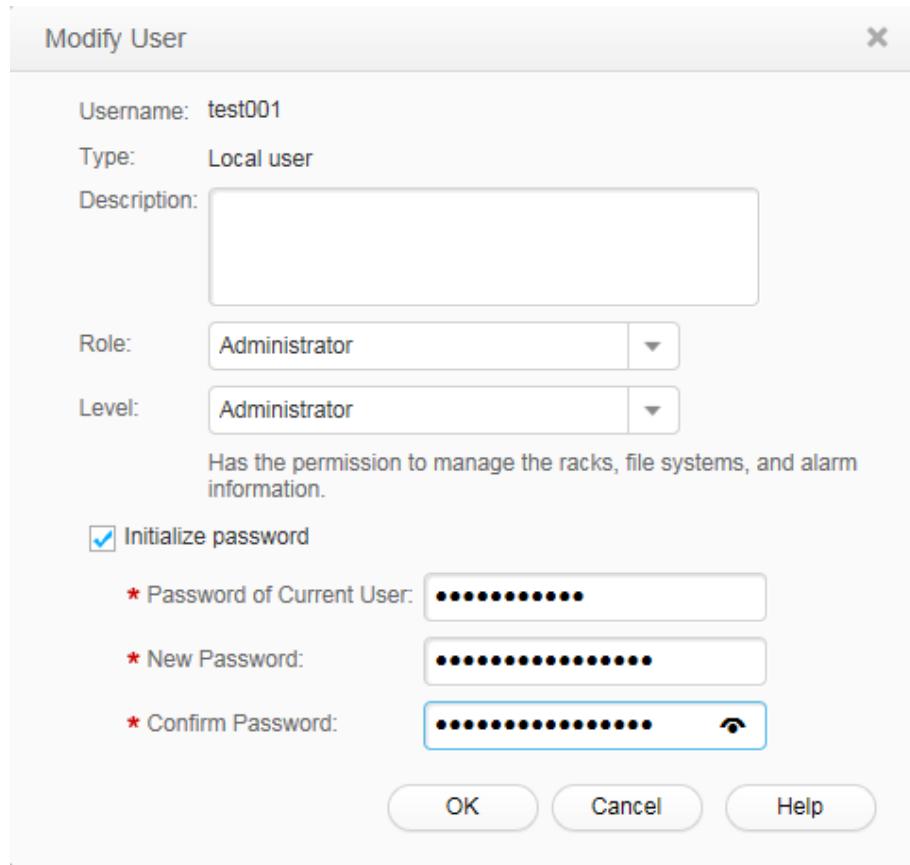
## Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose   **Permission Settings** > **User Management**.

**Step 3** In the middle function pane, select a user that you want to modify and click **Modify**.

The **Modify User** dialog box is displayed.



**Step 4** Select a desired user level from the **Level** drop-down list.

 **NOTE**

The user level determines whether a user has operation or read-only permission. For details on how to modify the scope of permission, see **Customizing User Roles**.

**Step 5** Confirm the user modification.

1. Click **OK**.

The security alert dialog box is displayed. Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation**.

2. Click **OK**.

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

3. Click **Close**.

**----End**

### 5.3.3.4 Customizing User Roles

User roles control the scopes of permission for users. A super administrator can change the role of a read-only user or an administrator to adjust the user's scope of permission according to the actual requirements. After a role is assigned to a user, the user has the permission to access or operate the objects specified by the role.

#### Prerequisites

The super administrator can modify the level and role and initiate the password only for users whose **Status** is **Offline**.

#### Context

The storage system provides typical default roles. If the default roles cannot meet your requirements, you can create roles.

#### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** (Optional) Choose  **Settings** >  **Permission Settings** > **Role Management** and manage user-defined roles. [Table 5-7](#) details the operations.

 **NOTE**

- You can create roles if the system's default roles do not meet your requirements.
- You can modify existing user-defined roles as required.
- You can delete user-defined roles that are not needed any more.

**Table 5-7** Managing user-defined roles

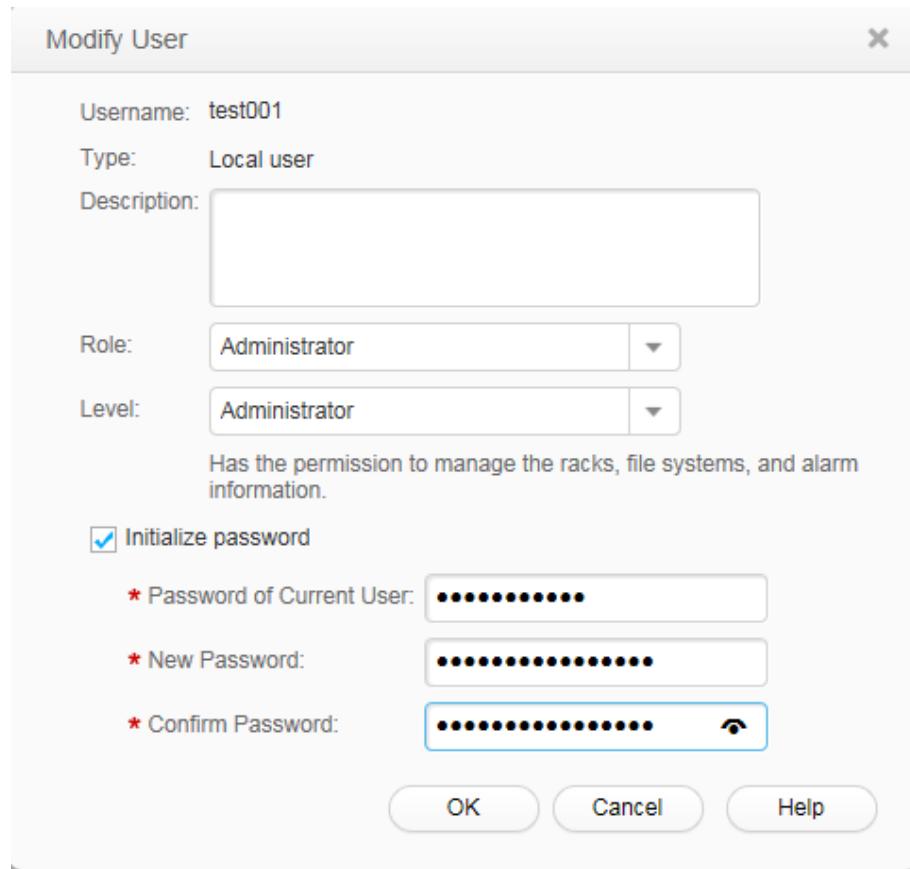
Operation	Procedure
Adding a user-defined role	<ol style="list-style-type: none"><li>1. In the function pane, click <b>Add</b>. The <b>Add Role</b> dialog box is displayed.</li><li>2. Set relevant parameters and click <b>Finish</b>. <a href="#">Table 5-8</a> describes the parameters.</li><li>3. On the <b>Execution Result</b> page, click <b>Close</b>.</li></ol>
Modifying a user-defined role	<ol style="list-style-type: none"><li>1. In the function pane, select a role and click <b>Modify</b>. The <b>Modify Permission</b> dialog box is displayed.</li><li>2. On the <b>General</b> and <b>Permission</b> tab pages, modify the parameters as required. <a href="#">Table 5-8</a> describes the parameters.</li><li>3. Click <b>OK</b>.</li></ol>
Deleting a user-defined role	<ol style="list-style-type: none"><li>1. In the function pane, select a role and click <b>Delete</b>.</li><li>2. The <b>Success</b> dialog box is displayed.</li><li>3. Click <b>OK</b>.</li></ol>

**Table 5-8** User-defined role parameters

Parameter	Description
Name	Name of a role.
Owning group	The value can be <b>System Group</b> or <b>vStore Group</b> . <ul style="list-style-type: none"><li>● If a role belongs to <b>System Group</b>, its permissions are valid in the system view.</li><li>● If a role belongs to <b>vStore Group</b>, its permissions are valid in the vStore view.</li></ul>
Description	Description of a role.
Object	Required object. For the object functions, see <a href="#">A Permission Matrix for Self-defined Roles (Applicable to V300R006C20 and Earlier Versions)</a> or <a href="#">B Permission Matrix for Self-defined Roles (Applicable to V300R006C30)</a> .
Read/Write Permission	Read/write permission of the selected object. The value can be <b>Read-only</b> or <b>Readable and writable</b> .

**Step 3** Change the user role.

1. Choose  **Settings** >  **Permission Settings** > **User Management**.
2. In the middle function pane, select a user that you want to modify and click **Modify**.  
The **Modify User** dialog box is displayed.



3. Select a desired role from the **Role** drop-down list.

**NOTE**

You can select a built-in or user-defined role based on your actual requirements.

**Step 4** Confirm the user modification.

1. Click **OK**.

The security alert dialog box is displayed. Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation**.

2. Click **OK**.

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

3. Click **Close**.

**----End**

### 5.3.3.5 Locking or Unlocking a User

A super administrator can prevent a user from logging in to the storage device by locking the user. Locked users online at the time they are locked can continue using DeviceManager but will not be able to log in again after they log out.

#### Prerequisites

- Only super administrators have the permission to perform this operation.

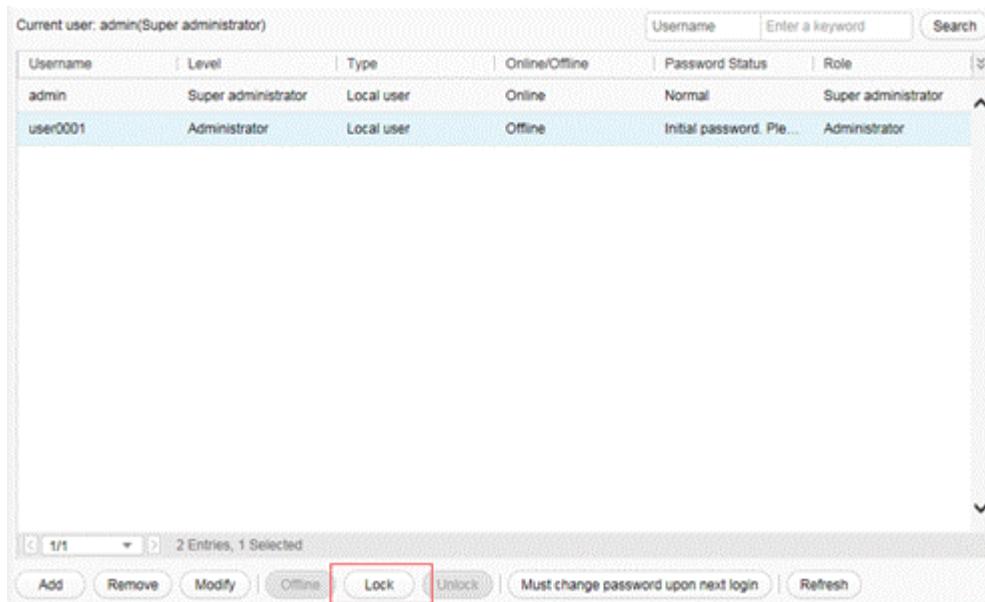
- Lock Status of the user to be locked is **Unlock**.

## Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Settings** >  **Permission Settings** > **User Management**.

**Step 3** In the middle function pane, choose a user that you want to lock and click **Lock**.



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

 **NOTE**

You can also right-click the user that you want to lock and choose **Lock**.

**Step 4** Click **OK**.

----End

### 5.3.3.6 Logging Out a User

A super administrator can prevent a logged-in user from using the storage device by forcibly logging the user out of DeviceManager.

## Prerequisites

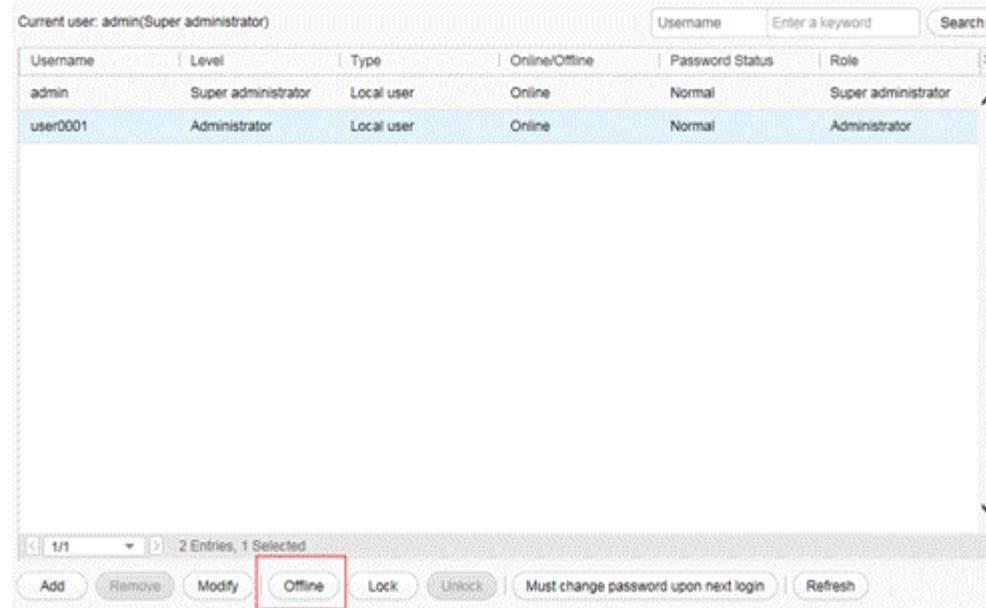
- Only super administrators have the permission to perform this operation.
- Users whose **Status** is **Online** can be logged out.

## Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Settings** >  **Permission Settings** > **User Management**.

**Step 3** In the function pane, select a user that you want to log out and click **Offline**.



The security alert dialog box is displayed.

**NOTE**

You can also right-click the user, and then choose **Offline**.

**Step 4** Confirm the logout of the user.

1. Carefully read the content in the dialog box and select **I have read and understand the consequences associated with performing this operation** to confirm the information.
2. Click **OK**.  
The **Success** dialog box is displayed, indicating that the operation succeeded.
3. Click **OK**.

----End

### 5.3.3.7 Changing Password

To ensure storage system security, periodically change the password used for logging in to the storage system.

#### Precautions

- Super administrators, administrators, and read-only users only have the permission to change their own passwords. Super administrators have the permission to initialize the passwords of administrators and read-only users.
- If your password has expired or been 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, administrators, and read-only users need to change their default password after logging in to the storage system the first time and change their password later regularly.

- 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.

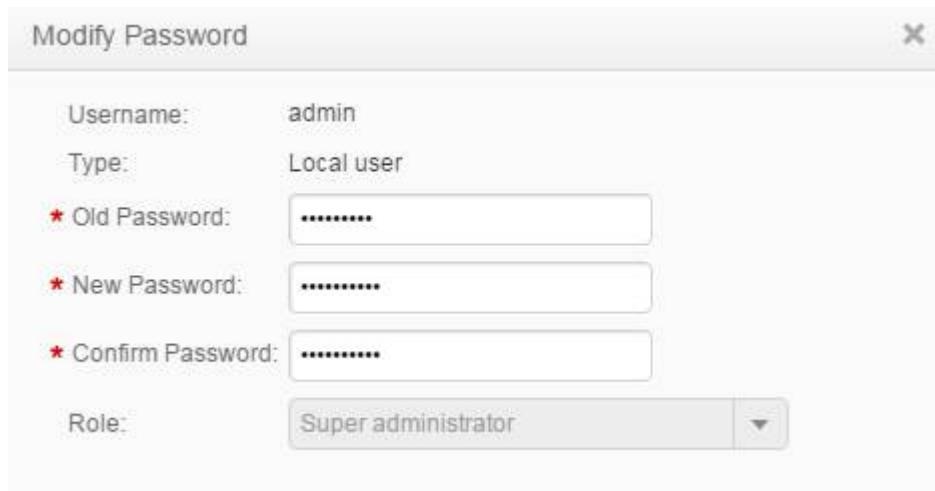
## Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Settings** >  **Permission Settings** > **User Management**.

**Step 3** In the function pane, click the name of the super administrator and click **Modify**.

The **Modify Password** dialog box is displayed.



**Step 4** Enter **Old Password**, **New Password** and **Confirm Password**.

 **NOTE**

- To ensure account security, change the default password after you log in to the storage system for the first time.
- To ensure account security, change your password regularly.

**Step 5** Click **OK**.

----End

### 5.3.3.8 Resetting the Password of an Administrator or a Read-Only User

This section describes how to retrieve or reset user passwords.

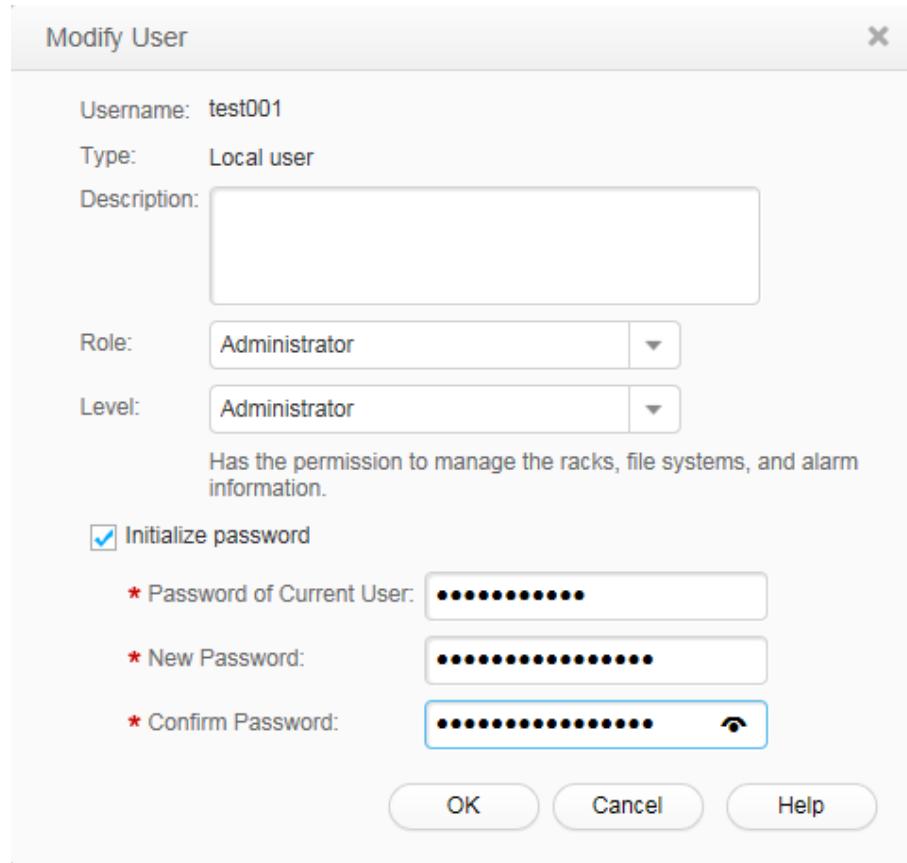
If an administrator or a read-only user forgets the password, the super administrator **admin** can reset the password on DeviceManager or the CLI.

- Resetting user passwords on DeviceManager
  - Log in to DeviceManager as the super administrator.

 **NOTE**

The default super administrator name is **admin** and its password is **Admin@storage**.

1. Choose  **Settings** >  **Permission Settings** > **User Management**.
2. In the middle function pane, select a user that you want to modify and click **Modify**.  
The **Modify User** dialog box is displayed.



3. Select **Initialize password**. Input **Password of Current Login User**, **New Password**, and **Confirm Password**.

 **NOTE**

The passwords of LDAP users cannot be initialized.

4. Confirm the password initialization.
  - a. Click **OK**.  
The security alert dialog box is displayed. Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation**.
  - b. Click **OK**.  
The **Execution Result** dialog box is displayed indicating that the operation succeeded.
  - c. Click **Close**.
    - Resetting user passwords on the CLI
5. Log in to the CLI as the super administrator.

 **NOTE**

The default super administrator name is **admin** and its password is **Admin@storage**.

6. Run the **change user user\_name=? action=reset\_password** command to reset the password.

For example, to reset the password of **testuser**, run the following command:

```
admin:/>change user user_name=testuser action=reset_password
New password:*****
Reenter password:*****
Password:*****
Command executed successfully.
```

### 5.3.3.9 Resetting the Password of a Super Administrator

This section describes how to reset the password of a super administrator.

If the password of the super administrator **admin** is lost, another super administrator **\_super\_admin** can log in to the CLI via a serial port and run **initpasswd** to reset the password. The procedure is as follows:

1. Use **\_super\_admin** to log in to the CLI via a serial port.

 **NOTE**

The default password of the super administrator **\_super\_admin** is **Admin@revive**.

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
```

### 5.3.3.10 Setting User Passwords to Never Expire

This section describes how to set user passwords to never expire.

## Procedure

You can set user passwords to never expire in **Security Policies** or **User Management**.

 **NOTE**

- In **Security Policies**, you can set passwords of all users in a storage system to never expire.
  - In **User Management**, you can only set the password of a specified user to never expire. This applies to V300R006C30 and later.
- Configuring Password Validity Period in **Security Policies**

- a. Log in to DeviceManager.

- b. Choose  **Settings** >  **Permission Settings** > **Security Policies**.

- i. On the right navigation bar, click  **Settings**.

- ii. In the **Basic Service Settings** area on the function pane, click  **Permission Settings**.

The **Security Policies** page is displayed.

- iii. In the left navigation tree, select **Security Policies**.

The **Security Policies** page is displayed.

The screenshot shows the 'Security Policies' configuration page. It includes sections for 'Username Policy' and 'Password Policy'. In the 'Password Policy' section, the 'Password Validity Period (days)' field is set to 180, which is highlighted in red. The 'Password Expiration Warning Period (days)' field is set to 7. Other policy parameters like character complexity and history length are also displayed.

- c. Deselect **Password Validity Period (days)**.

- d. Click **Save**.

The **Execution Results** dialog box is displayed, indicating that the security policy configuration succeeds.

- e. Click **Close**.

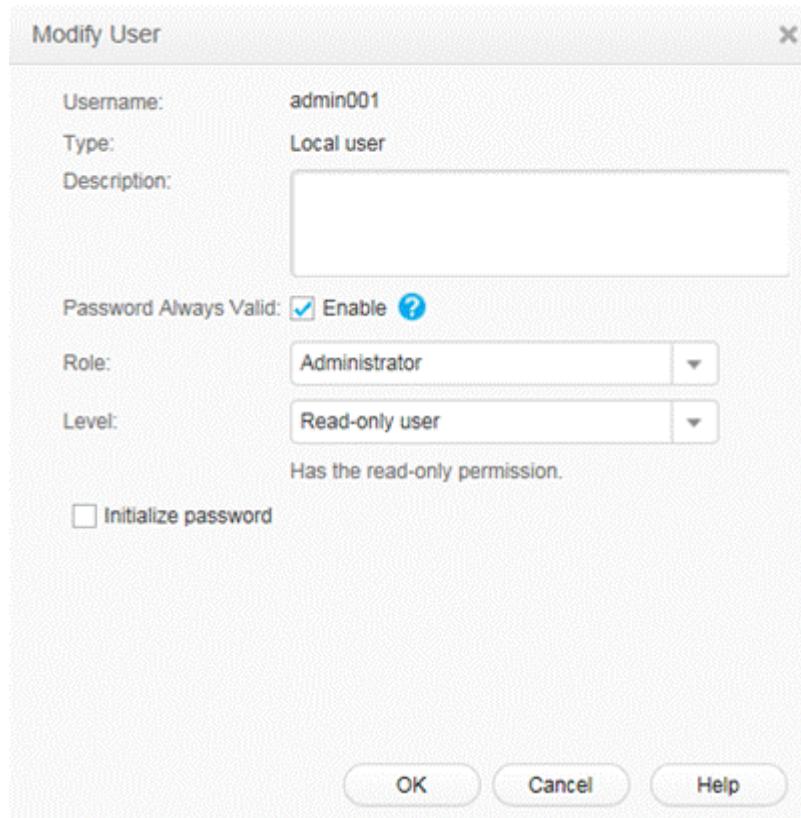
Passwords of all users in the storage system will never expire.

● Configuring **Password Policies** in **User Management**

- a. Log in to DeviceManager.

- b. Choose **Settings** > **Permission Settings** > **User Management**.  
c. In the middle function pane, select a user that you want to modify and click **Modify**.

The **Modify User** dialog box is displayed.



- d. Select **Password Always Valid**.
- e. Click **OK**.  
The **Execution Result** dialog box is displayed indicating that the operation succeeded.
- f. Click **Close**.  
The password of the specified user will never expire.

### 5.3.3.11 Removing a User

This operation enables you to remove an unwanted user.

#### Context

- Only a super administrator has the permission to remove the administrators, read-only users and other super administrators.
- An online user cannot be removed.

#### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Settings** >  **Permission Settings** > **User Management**.

**Step 3** In the middle function pane, select the user that you want to remove and click **Remove**.

The security alert dialog box is displayed.

**Step 4** Confirm the user removal.

1. Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation.**
2. Click **OK**.  
The **Success** dialog box is displayed, indicating that the operation succeeded.
3. Click **OK**.

----End

### 5.3.4 Migrating a Storage System AD Domain (Applicable to V300R006C30)

This section describes how to migrate the AD domain for a storage system.

#### Context

- After the AD domain on the user network is migrated, the storage system must exit from the original AD domain and be added to the new AD domain.
- If the storage system is configured with cross-protocol user mappings before AD domain migration, the mappings will become invalid after the storage system is added to the new AD domain. You need to configure the mappings again.
- If the storage system creates AD domain user quota before AD domain migration, the quota will become invalid after the storage system is added to the new AD domain. You need to create the quota again.
- After the storage system is added to the new AD domain, users of the new AD domain can perform operations in the CIFS shared directory and have the same operation permissions as those of the original AD domain.

#### Procedure

**Step 1** Log in to the CLI of the storage system and run the **change domain ad\_config sid\_history\_enable=yes** command to enable the AD domain migration function.

If the message **Command executed successfully** is displayed, the function is enabled successfully. If it is not, perform operations as prompted and enable the AD domain migration function again.

```
admin:/>change domain ad_config sid_history_enable=yes
Command executed successfully.
```

**Step 2** Exit the original AD domain.

1. Log in to DeviceManager.
2. Choose **Settings > Storage Settings > File Storage Service > Domain Authentication**.

The screenshot shows a configuration interface for joining an Active Directory domain. It includes fields for the Domain Administrator Username, Password, Full Domain Name (with a 'Test' button), Organization Unit, System Name, and Overwrite System Name (with an 'Enable' checkbox). There are also fields for Domain Status, Join Domain, and Exit Domain buttons.

3. In the **AD Domain Settings** area, enter **Domain Administrator Username** and **Password**.
4. Click **Exit Domain**.  
The **Success** dialog box is displayed.
5. Click **OK** to exit the AD domain.

**Step 3** Add the storage system to the new AD domain.

For details, see section "Configuring a Storage System to Add It to an AD Domain" in the *Basic Storage Service Configuration Guide for File* corresponding to your product.

**Step 4** (Optional) Configure user mappings.

For details, see section "Managing User Mappings Across Protocols (CIFS-NFS)" in the *Basic Storage Service Configuration Guide for File* corresponding to your product.

**Step 5** (Optional) Create a quota.

For details, see section "(Optional) Creating a Quota" in the *Basic Storage Service Configuration Guide for File* corresponding to your product.

----End

## 5.4 Managing Alarm Notifications

The storage system provides alarm notification functions. This section describes how to modify alarm notification settings to meet changing service requirements.

### 5.4.1 Managing Email Notification

This section describes how to modify the SMTP server and email address for receiving alarm notifications.

### 5.4.1.1 Adding a Backup SMTP Server

This section describes how to add a backup Simple Mail Transfer Protocol (SMTP) server. After a backup SMTP server is configured, the two SMTP servers back up each other. If one fails, the other one takes over to send email notifications.

#### Prerequisites

- A maximum of two SMTP servers can be added.
- The connections between each SMTP server and primary and secondary controllers are normal.
- You have logged in to DeviceManager as the super administrator or an administrator who has operation permission.
- The DNS server communicates properly with the storage array or third-party server.

#### Procedure

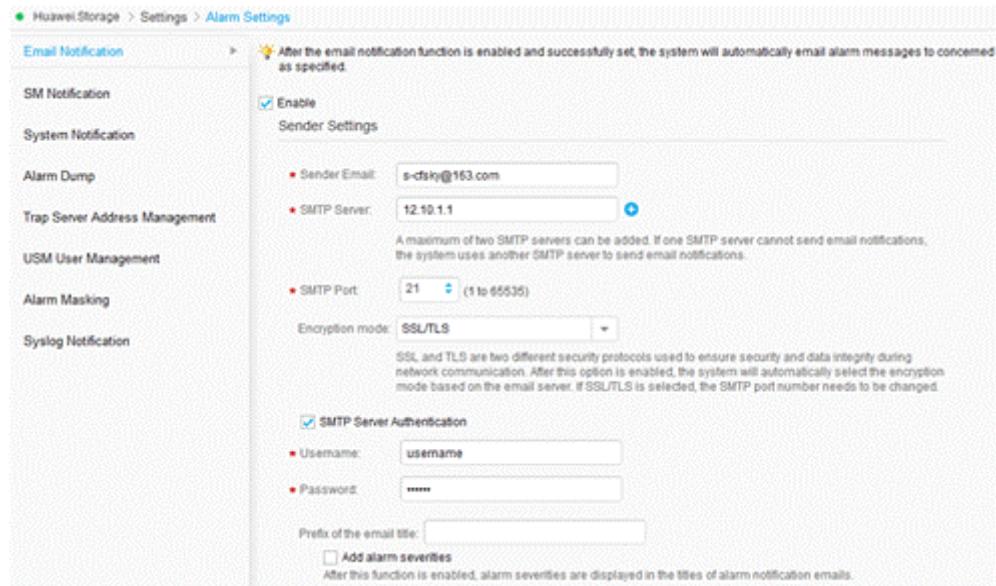
**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Settings** >  **Alarm Settings** > **Email Notification**.

**Step 3** Add a backup SMTP server.

1. Click  on the right of **SMTP Server** in the **Sender Settings** area to display the text box for the SMTP server address.
2. Enter the IP address or domain name of the backup SMTP server to be added.

**Figure 5-16** Email notification page



**Step 4** Confirm that parameters listed in **Table 5-9** are properly set and click **Save**.

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

**Table 5-9** Email notification parameters

Parameter	Description	Setting
Sender Email	Email address of the sender.	[Example] user@163.com
SMTP Port	<p>Indicates the port setting of SMTP. The default value is 25.</p> <p><b>NOTE</b> The SMTP port number configured on a storage system must be consistent with that configured on the SMTP server.</p>	[Remarks] The range of the SMTP port is 1 to 65535. [Example] 3
Encryption mode	<p>The encryption mode during network communication between system and email server.</p> <ul style="list-style-type: none"><li>● Not encrypted: the data transfer is not encrypted.</li></ul> <p><b>NOTE</b> There are security risks if you select this. You are advised to select another encryption mode to improve the security of data transfer.</p> <ul style="list-style-type: none"><li>● 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.</li><li>● STARTTLS: After the <b>STARTTLS</b> command is executed, TLS is encrypted. Communication data is not encrypted before the <b>STARTTLS</b> command is executed.</li></ul> <p><b>NOTE</b> The encryption mode configured on a storage system must be consistent with that configured on the SMTP server.</p>	[Example] STARTTLS

Parameter	Description	Setting
SMTP Server Authentication	Indicates whether the SMTP server needs to authenticate senders. If it is not selected, <b>Username</b> and <b>Password</b> are unavailable.	[Example] Select the option button if the SMTP server requires authentication. Otherwise, leave it unselected.
Username	SMTP account name of the sender. When emails are sent through the SMTP server, the sender is prompted to type their SMTP account name and password for authentication.	[Remarks] 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 their SMTP account name and password for authentication.	[Remarks] <ul style="list-style-type: none"><li>● The value cannot be blank, and contains 1 to 63 characters.</li><li>● The password cannot contain extended ASCII characters or Unicode characters. Otherwise, the password is invalid. It is recommended that the password contain characters from the following categories:<ul style="list-style-type: none"><li>- Base 10 digits (0-9)</li><li>- English uppercase characters (A-Z)</li><li>- English lowercase characters (a-z)</li><li>- Space</li><li>- Special characters such as [ ] ^ _ { } ~ ` @ ! " # \$ % &amp; ' ( ) * + - . / ; &lt; = &gt; ?</li></ul></li></ul> [Example] aJ1p23dySQ
Prefix of the email title	Email title field defined by senders. If there are too many emails, users can search for desired emails using this field.	The value contains 0 to 511 bytes and cannot contain a single quotation mark ('). [Example] -

Parameter	Description	Setting
Add alarm severities	After this function is enabled, alarm severities are displayed in the titles of alarm notification emails. Alarm severities contain <b>critical</b> , <b>major</b> and <b>warning</b> .	[Example] Add alarm severities

**Step 5** Click **Close**.

----End

#### 5.4.1.2 Managing Recipient Email Addresses

This operation enables you to update the recipient email addresses.

##### Prerequisites

- You have logged in to DeviceManager as the super administrator or an administrator who has operation permission.
- The email notification function has been enabled.
- An SMTP server is available and has been configured.

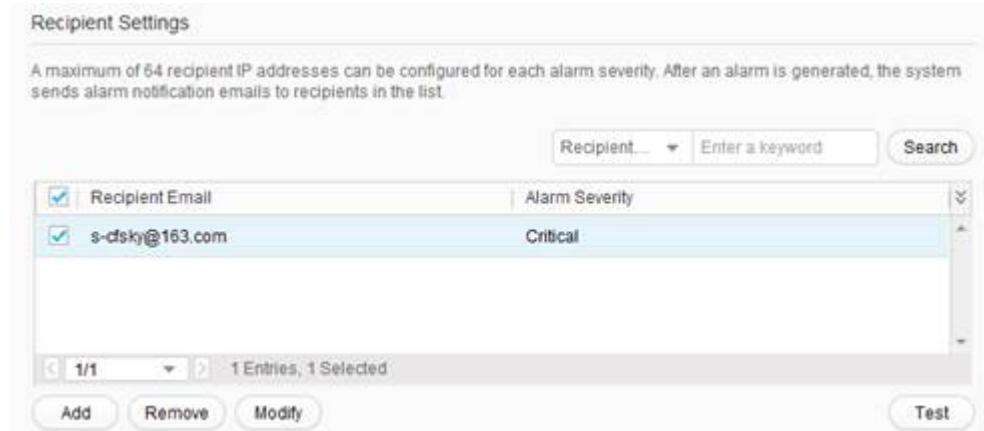
##### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose   **Settings** > **Alarm Settings** > **Email Notification**.

**Step 3** Manage recipient email addresses. **Table 5-10** details the operations.

**Figure 5-17** Recipient Settings



**Table 5-10** Relevant operations

Operation	Procedure
Adding a recipient email address	<ol style="list-style-type: none"><li>Under the <b>Recipient Settings</b> list, click <b>Add</b>.</li><li>The <b>Add Recipient Information</b> dialog box is displayed.</li><li>Set <b>Recipient Email</b> and <b>Alarm Severity</b>. <b>NOTE</b> The alarm severities include <b>Critical</b>, <b>Major</b>, and <b>Warning</b>.</li><li>Click <b>OK</b>.</li><li>The <b>Recipient Settings</b> list displays the newly added recipient email address.</li></ol>
Editing a recipient email address	<ol style="list-style-type: none"><li>In the <b>Recipient Settings</b> list, select an email box that you want to edit and click <b>Modify</b>.</li><li>The <b>Modify Recipient Information</b> dialog box is displayed.</li><li>Set <b>Recipient Email</b> and <b>Alarm Severity</b>.</li><li>Click <b>OK</b>.</li><li>The <b>Recipient Settings</b> list displays the edited recipient email address.</li></ol>
Removing a recipient email address	In the list, select a recipient email address that you want to remove and click <b>Remove</b> .

**Step 4** Click **Save**.

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

**Step 5** Click **Close**.

----End

## 5.4.2 Managing SMS Notification

The DeviceManager can send alarm information to specific mobile phones using SMS, allowing easy device monitoring.

### 5.4.2.1 Managing Recipient Mobile Phone Numbers

This operation enables you to update the recipient mobile phone numbers.

#### Prerequisites

- You have logged in to DeviceManager as the super administrator or an administrator who has operation permission.
- The email notification function has been enabled.

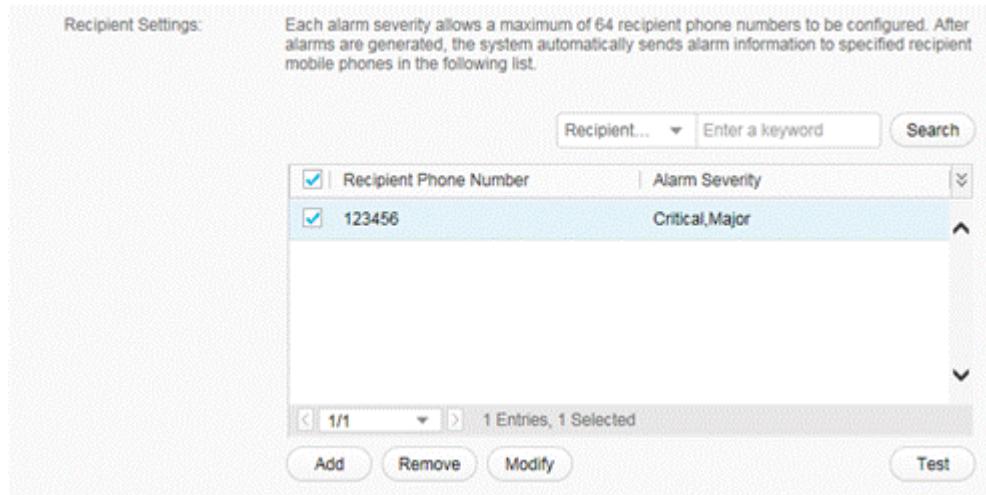
## Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Settings** >  **Alarm Settings** > **SM Notification**.

**Step 3** Manage recipient mobile phone numbers. **Table 5-11** details the operations.

**Figure 5-18** Recipient Settings



**Table 5-11** Relevant operations

Operation	Procedure
Adding a recipient mobile phone number	<ol style="list-style-type: none"><li>Under the <b>Recipient Settings</b> list, click <b>Add</b>.</li><li>The <b>Add Recipient Information</b> dialog box is displayed.</li><li>Set <b>Recipient Phone Number</b> and <b>Alarm Severity</b>. <b>NOTE</b><ul style="list-style-type: none"><li>The recipient mobile phone number contains 3 to 31 digits. If the mobile phone number is a foreign phone number, it must be in the format of Plus sign (+) + Country code + Recipient mobile phone number.</li><li>The alarm severities include <b>Critical</b>, <b>Major</b>, and <b>Warning</b>.</li></ul></li><li>Click <b>OK</b>.</li><li>The <b>Recipient Settings</b> list displays the newly added recipient mobile phone number.</li></ol>

Operation	Procedure
Modifying a recipient mobile phone number	<ol style="list-style-type: none"><li>1. In the <b>Recipient Settings</b> list, select a mobile phone number that you want to edit. Click <b>Modify</b>.</li><li>2. The <b>Modify Recipient Information</b> dialog box is displayed.</li><li>3. Set <b>Recipient Phone Number</b> and <b>Alarm Severity</b>.</li><li>4. Click <b>OK</b>.</li><li>5. The <b>Recipient Settings</b> list displays the modified recipient mobile phone number.</li></ol>
Removing a recipient mobile phone number	In the list, select a mobile phone number that you want to remove and click <b>Remove</b> .

**Step 4** Click **Save**.

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

**Step 5** Click **Close**.

----End

#### 5.4.2.2 Configuring the GSM Modem (OceanStor 2000, 5000, and 6000 Series)

After setting the GSM modem, you can configure short message notification in management software. The storage system will send alarm information to a specified mobile phone. You can learn about storage system exceptions and solve them in a timely manner.

#### Prerequisites

You need to connect the storage device with a GSM modem, make sure you have installed GSM modem.

#### Context



#### NOTICE

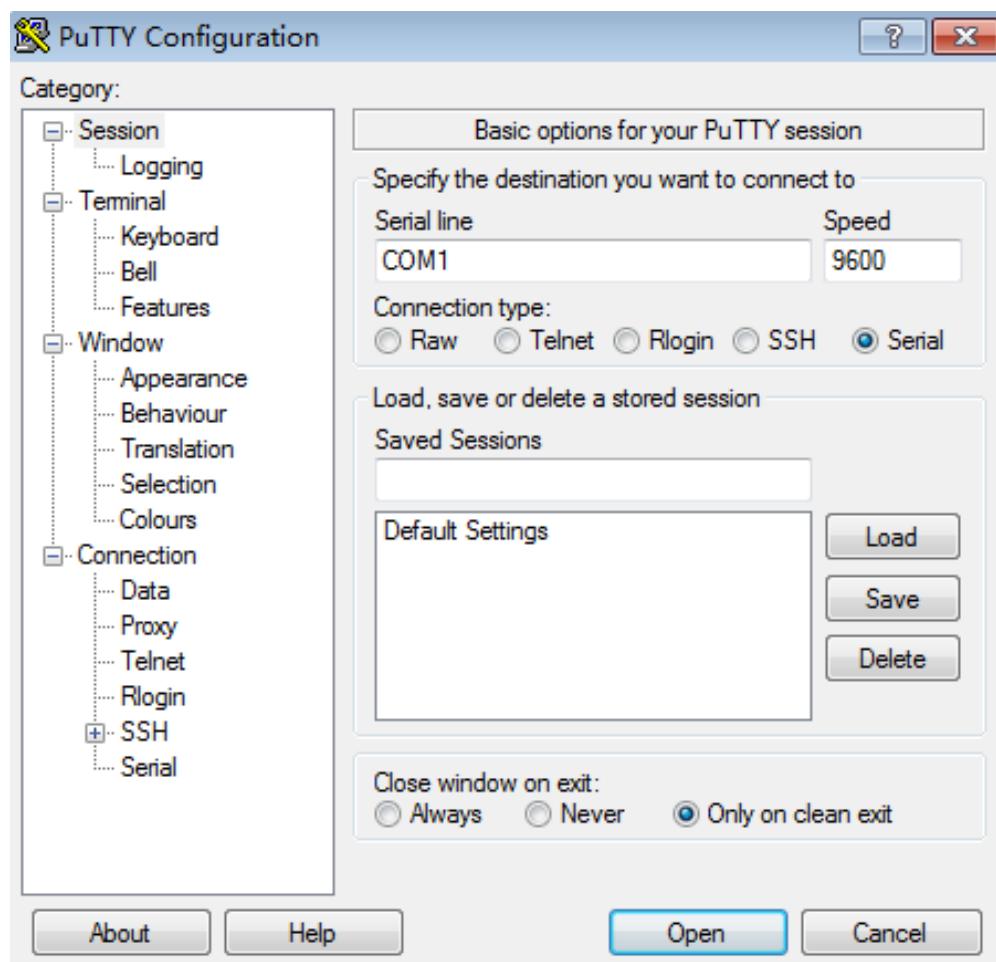
- If the GSM modem is not hot-swappable, do not insert or remove it when it is running.
- If the storage system is enabled with short message notification, the serial port on the controller enclosure serves only the GSM.
- For a storage system with eight or more controllers, GSM modems can only be configured for the first eight controllers.
- For a 2 U controller enclosure, you are advised to connect the GSM modem to the serial port of controller A. If the serial port of controller A fails, connect the GSM modem to the serial port of controller B.
- For a 3 U or 6 U controller enclosure, 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) is 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** Put 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 **Session > Logging**. The **Basic options for your PuTTY session** page for configuring the GSM modem is displayed, as shown in [Figure 5-19](#).

**Figure 5-19** Page for **Basic options for your PuTTY session**

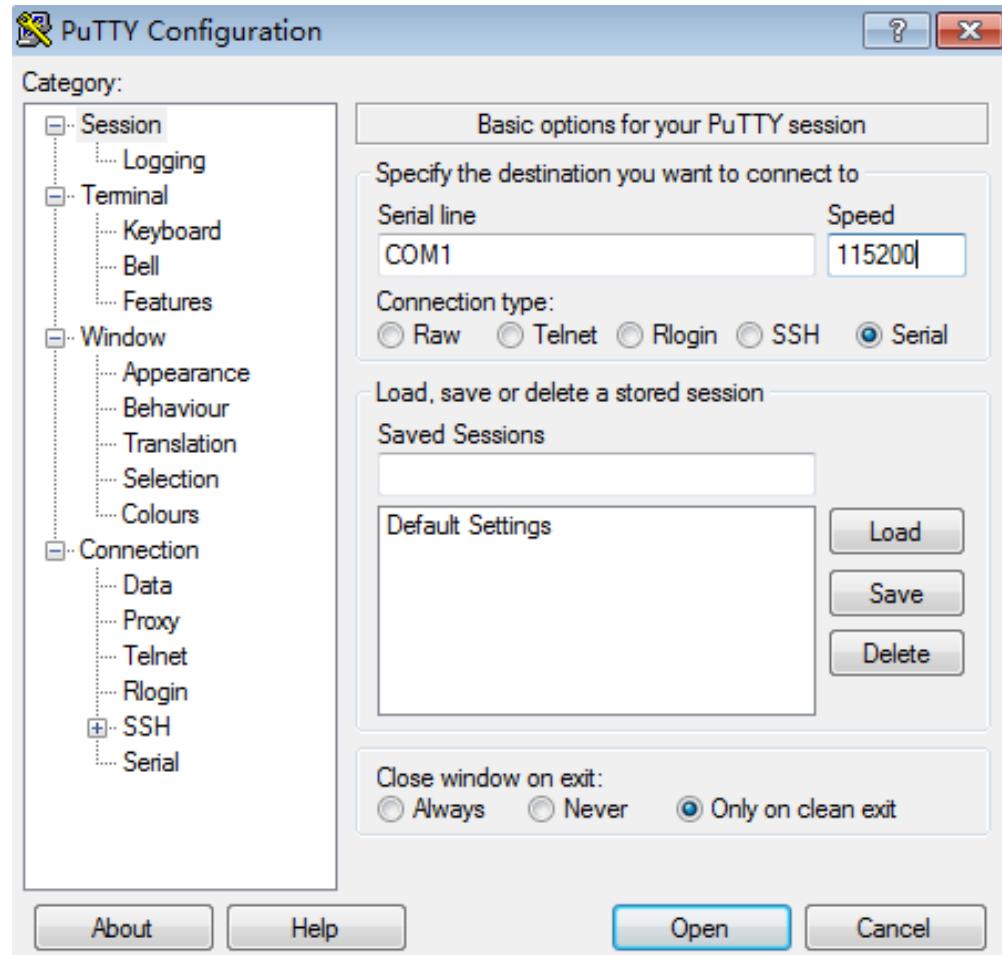


- Step 5** Click **Open**.
- Step 6** Run the **at** command on the **COM1-PuTTY**, and **OK** appears in the output if the GSM modem has connected to the host through the serial port. If this is true, go to [Step 9](#). If

running that command responds with nothing, the GSM modem has been disconnected from the serial port. If this is true, 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. Then run the **at** command on the **COM1-PuTTY** page, and check that the command output is **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, 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. To verify the configuration, the following shows the configuration success page.

```
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

### 5.4.2.3 Configuring the GSM Modem (OceanStor 18000 Series)

After setting the GSM modem, you can configure short message notification in management software. The storage system will send alarm information to a specified mobile phone so that you can learn about storage system exceptions and solve them in a timely manner.

#### Prerequisites

The SVP is connected to a GSM modem that is properly installed.

#### Context

- OceanStor mission critical storage systems support wireless and wired modems. Only wireless modems have power converters for connecting to the storage system's PDUs.
- If your modem cannot connect to a PDU, use an external power supply for the modem.
- Storage systems do not have a planned position for installing modems. You are advised to bind your modem to a location near the bay and on top of a disk enclosure or file engine.



#### NOTICE

- If the GSM modem is not hot-swappable, do not insert or remove it when it is running.
- If the storage system has enabled short message notification, the serial port on the SVP can be connected only to the GSM.

This section describes how to configure a GSM modem, with the COM1 serial port (baud rate = 115200 bits/s) on the SVP and the DB9 serial port on the GSM modem (default baud rate = 9600 bits/s) used as an example.

#### Procedure

- Step 1** Insert a SIM card into the GSM modem.

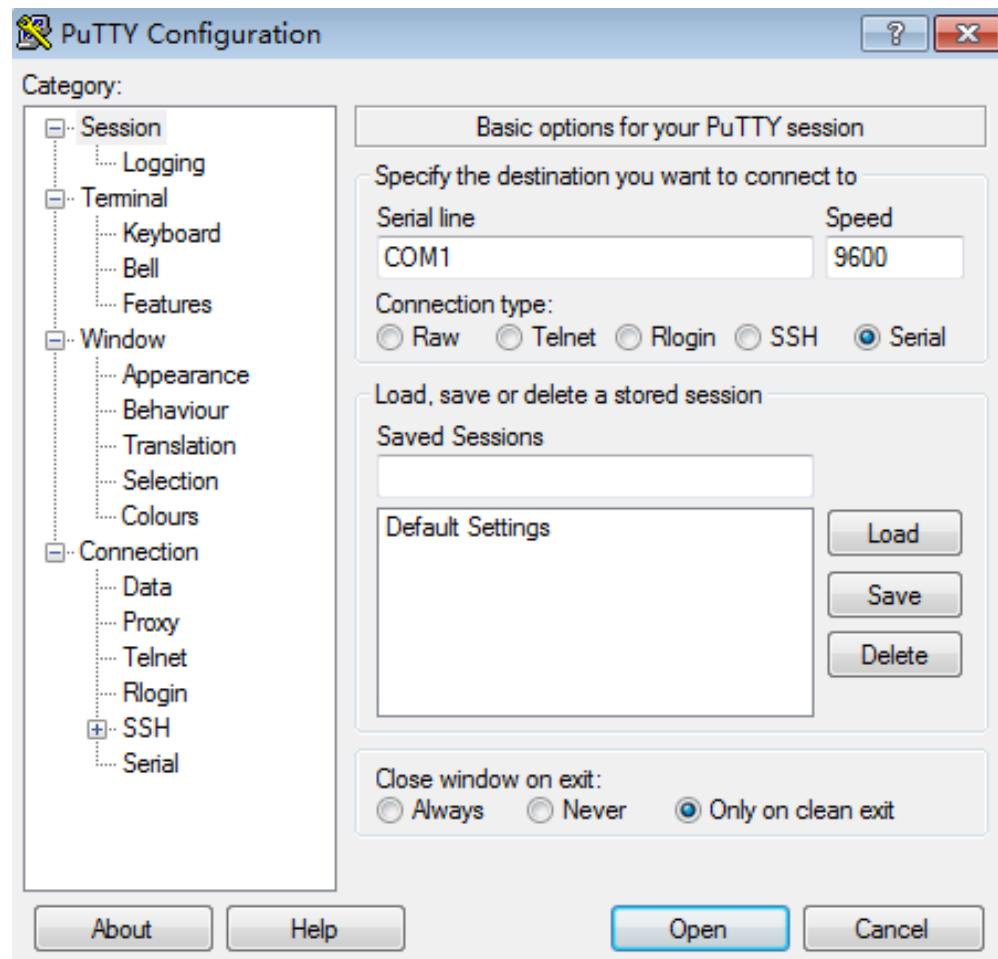
- Step 2** Connect the GSM modem to the serial port on the maintenance terminal through a DB9 serial cable.

- 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 **Session > Logging**. The **Basic options for your PuTTY session** page for configuring the GSM modem is displayed, as shown in [Figure 5-21](#).

**Figure 5-21** Page for **Basic options for your PuTTY session**

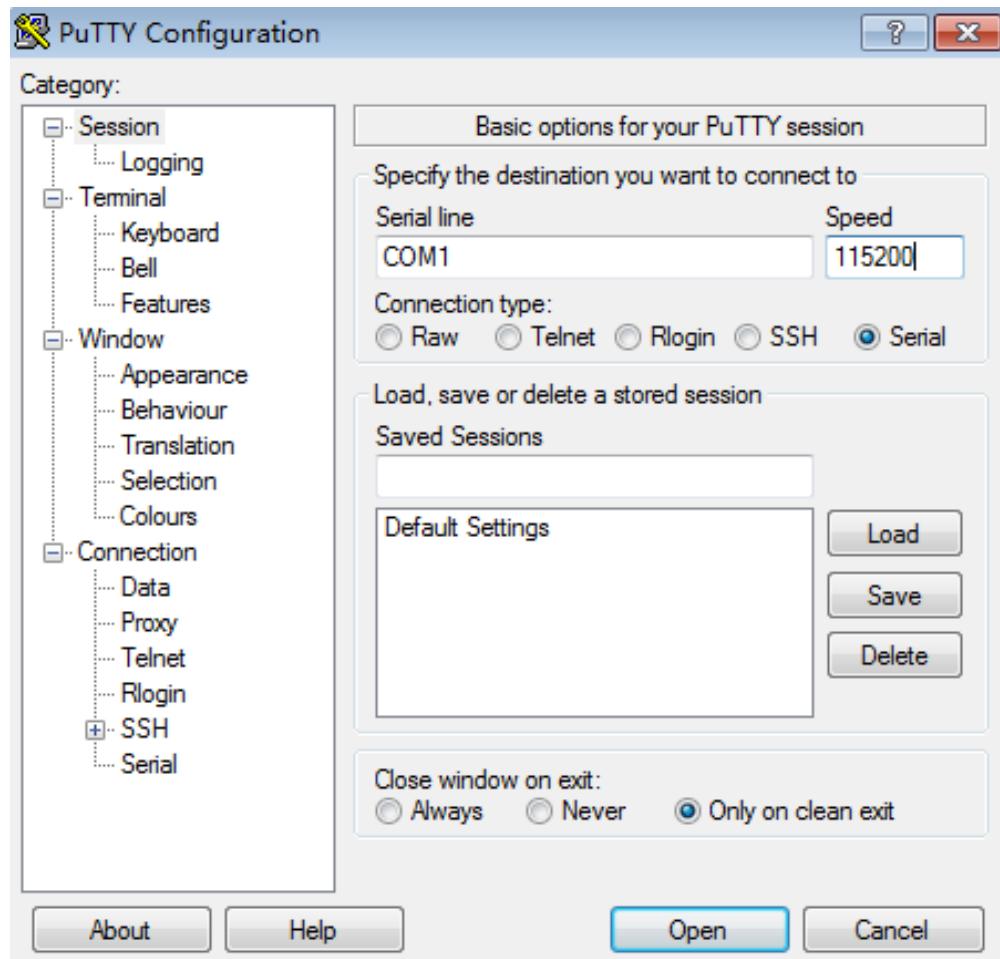


- Step 5** Click **Open**.

- Step 6** Run the **at** command on the **COM1-PuTTY** page.

- If **OK** appears, the GSM modem is connected to the host through the serial port. Go to [Step 9](#).
- If there is no response to the command, the GSM modem has been disconnected from the serial port. Go to [Step 7](#).

- Step 7** Re-log in to the page for configuring the GSM modem, as shown in [Figure 5-22](#).

**Figure 5-22** 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 known, try to set it multiple times until the baud rate of the GSM modem and that of the serial port are consistent. In this condition, PuTTY can be used to configure the GSM modem.
- The baud rate can be configured using the command **at+ipr=115200**.

**Step 9** Set other parameters, for example whether to reply automatically.

**Step 10** Click **OK** to save and exit.

You can run the following commands to view the configuration. The following command output indicates that the configuration is successful.

```
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 SVP for use.

 **NOTE**

For details about configuring the GSM modem, see the associated manual delivered with the GSM modem.

----End

## 5.4.3 Managing Syslog Notification

You can modify the receiver server address, notification type, and alarm severity of Syslog notifications based on service requirements.

### 5.4.3.1 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 the super administrator or an administrator who has operation permission.
- 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.

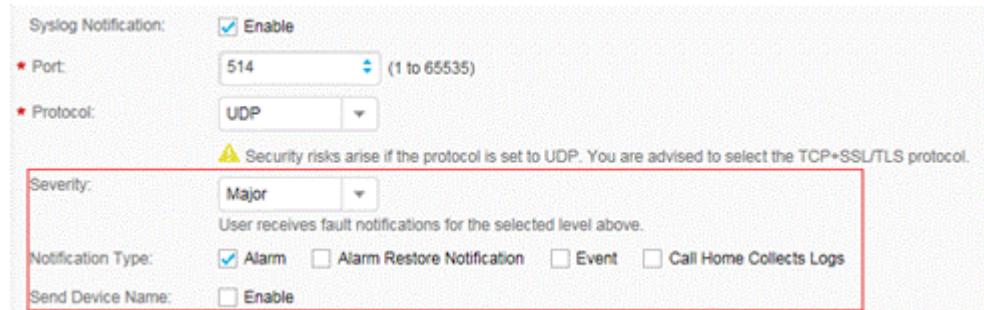
#### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose   **Settings** > **Alarm Settings** > **Syslog Notification**.

**Step 3** Configure the Syslog notification type and severity. **Table 5-12** describes the parameters.

**Figure 5-23** Syslog notification settings



**Table 5-12** Syslog notification parameters

Parameter	Description	Value
Severity	Indicates the lowest severity of a Syslog alarm that can be sent. Possible values are <b>Informational</b> , <b>Warning</b> , <b>Major</b> , and <b>Critical</b> .	[Example] Warning
Notification Type	Possible values are <b>Alarm</b> , <b>Alarm Restore Notification</b> , <b>Event</b> , and <b>Call Home</b> .	[Example] Event
Send Device Name	Indicates whether the device name should be sent to the Syslog server.  <b>NOTE</b> After <b>Send Device Name</b> is enabled, the system sends device names to the Syslog notification server. You can choose  <b>Settings &gt; Basic Information &gt; Device Information</b> to view device names.	[Example] Enable

**Step 4** (Optional) Click **Test** to test the connectivity between the storage system and Syslog server.

**Step 5** Click **Save**.

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

**Step 6** Click **Close**.

----End

#### 5.4.3.2 Managing the Receiver 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 the super administrator or an administrator who has operation permission.
- 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.

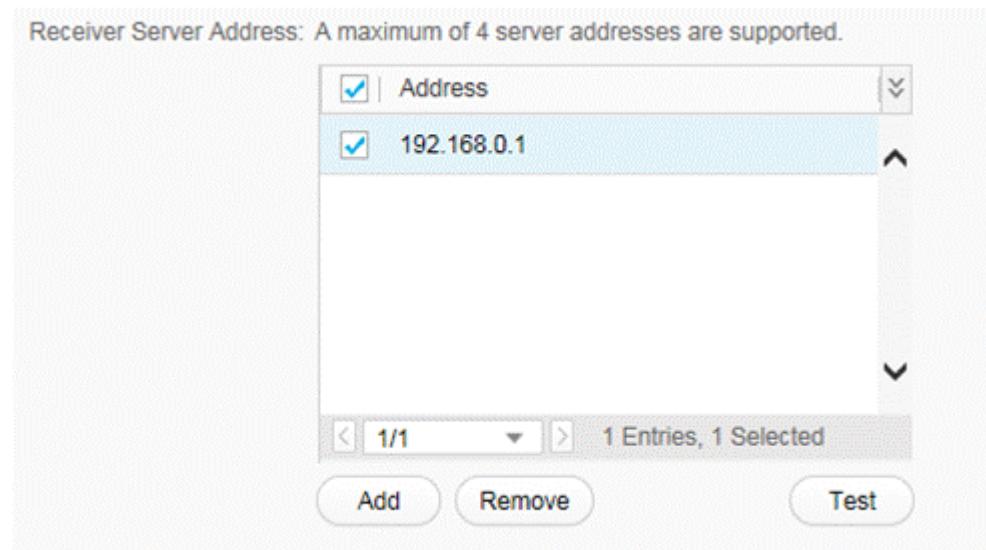
#### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Settings > Alarm Settings > Syslog Notification**.

**Step 3** Manage the receiver server addresses of Syslog notifications. **Table 5-13** details the operations.

**Figure 5-24** Receiver server address settings



**Table 5-13** Relevant operations

Operation	Procedure
Adding an address	<ol style="list-style-type: none"><li>Under the <b>Receiver Server Address</b> list, click <b>Add</b>.</li><li>The <b>Add Receiver Server Address</b> dialog box is displayed.</li><li>Specify the server address that you want to add. <b>NOTE</b><ul style="list-style-type: none"><li>An IPv4 address has the following requirements:</li><li>The 32-bit address is evenly divided into four fields. Each 8-bit field is expressed in dotted-decimal.</li><li>Each field of the IP address cannot be blank and must be an integer.</li><li>The value of the first field ranges from 1 to 223 (excluding 127).</li><li>The values of other fields range from 0 to 255.</li><li>The IP address cannot be a special address such as the broadcast address.</li><li>An IPv6 address has the following requirements:</li><li>The 128-bit address is evenly divided into eight fields. Each 16-bit field is expressed in four hexadecimal numbers and separated with colons.</li><li>In each 16-bit field, zeros before integers can be removed. However, at least one digit must be reserved in each field.</li><li>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-colon (:) can also be used to represent neighboring zeros of the IP address.</li><li>The IP address cannot be a special address such as network address, loop address, or multicast address.</li><li>The domain name has the following requirements:</li><li>A domain name is not case-sensitive and must be an English domain name.</li><li>An English domain name contains 1 to 255 characters.</li><li>An English domain name can only contain letters (a to z, A to Z), digits (0 to 9), dots (.), and hyphens (-). It cannot start or end with hyphens (-).</li></ul></li><li>Click <b>OK</b>.</li><li>The <b>Receiver Server Address</b> displays the newly added server address.</li></ol>
Removing a receiver server address	In the <b>Receiver Server Address</b> list, select receiver server addresses that you want to remove and click <b>Remove</b> .

**Step 4** (Optional) Click **Test** to test the connectivity between the storage system and Syslog server.

**Step 5** Click **Save**.

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

**Step 6** Click Close.

----End

## 5.4.4 Managing Trap Notification

You can modify the addresses that receive trap alarm notifications based on service requirements. The storage system's alarm information will be sent to the network management systems or other storage systems specified by the trap servers.

### 5.4.4.1 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.

#### 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 community string is **storage\_public** and the default write community string is **storage\_private**.

#### Procedure

**Step 1** Run **change snmp community read\_community=\*\*\*\*\*  
write\_community=\*\*\*\*\*** to modify community strings.



When you enter a community string, asterisk signs (\*) are displayed. Remember or record the community string.

Parameter	Value
Read community string	<p>[Default rules]</p> <p>Complexity requirements are as follows:</p> <ul style="list-style-type: none"><li>● Must contain 6 to 32 characters.</li><li>● Must contain a special character, such as a space or one of the following: ! " # \$ % &amp; ' ( ) * + , - . / : ; &lt; = &gt; ? @ [ \ ] ^ ` { _   } ~.</li><li>● Must contain any two of the following character types: uppercase letter, lowercase letter, and digit.</li><li>● Community strings cannot be the user name or reversed user name.</li></ul> <p><b>NOTE</b></p> <p>You can run <b>change snmp safe_strategy</b> on the CLI to change the default rules.</p> <p>[Example]</p> <p>usmuser@123</p>
Write community string	<p>[Default rules]</p> <p>Complexity requirements are as follows:</p> <ul style="list-style-type: none"><li>● Must contain 6 to 32 characters.</li><li>● Must contain a special character, such as a space or one of the following: ! " # \$ % &amp; ' ( ) * + , - . / : ; &lt; = &gt; ? @ [ \ ] ^ ` { _   } ~.</li><li>● Must contain any two of the following character types: uppercase letter, lowercase letter, and digit.</li><li>● Community strings cannot be the user name or reversed user name.</li></ul> <p><b>NOTE</b></p> <p>You can run <b>change snmp safe_strategy</b> on the CLI to change the default rules.</p> <p>[Example]</p> <p>usmuser@456</p>

**Step 2** Use the third-party network management tool to verify that the community strings can be used to interwork with the storage system.

----End

#### 5.4.4.2 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.

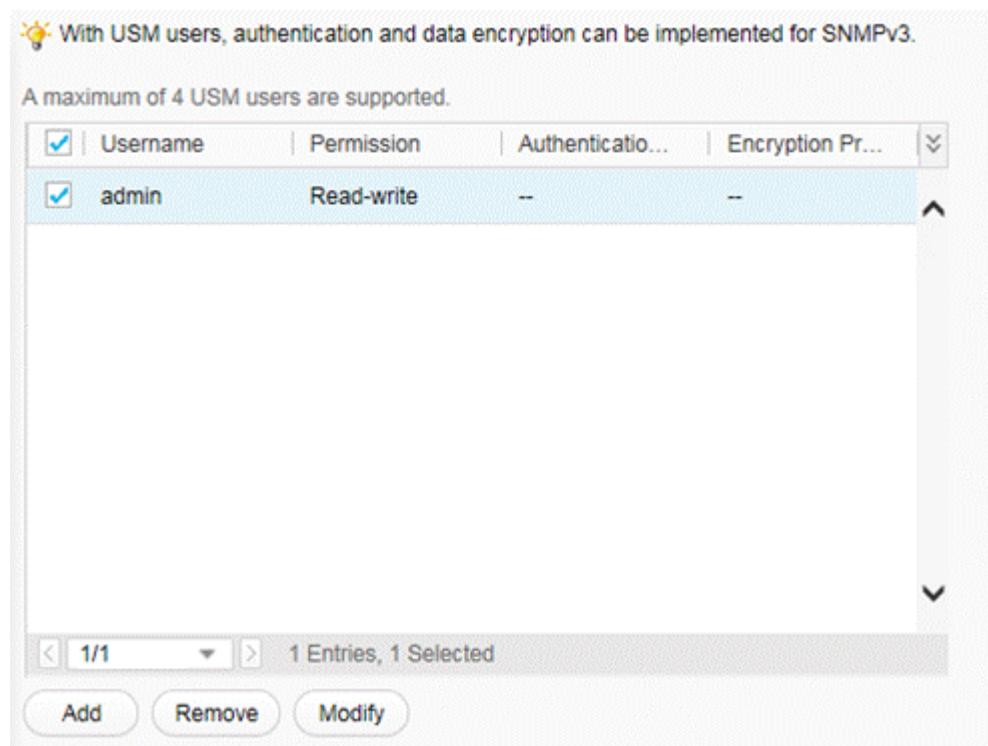
#### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Settings** >  **Alarm Settings** > **USM User Management**.

**Step 3** Manage USM users. **Table 5-14** details the operations.

**Figure 5-25** USM user management



**Table 5-14** Relevant operations

Operation	Procedure
Adding a USM user	<ol style="list-style-type: none"><li>Click <b>Add</b>. The <b>Add USM User</b> dialog box is displayed.</li><li>Set USM parameters. For related parameters, see <b>Table 5-15</b>.</li><li>Click <b>OK</b>.</li><li>The USM user list displays the newly added USM user.</li></ol>
Modifying a USM user	<ol style="list-style-type: none"><li>Select the USM user that you want to modify and click <b>Modify</b>.</li><li>The <b>Modify USM User</b> dialog box is displayed.</li><li>Modify USM parameters. <b>Table 5-15</b> describes the related parameters.</li><li>Click <b>OK</b>.</li><li>The USM user list displays the modified USM user.</li></ol>
Removing a USM user	Select the USM user that you want to remove and click <b>Remove</b> .

**Table 5-15** USM user parameters

Parameter	Description	Value
Username	Name of a USM user	[Rules]  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 Authentication	Whether to enable user authentication	[Default Value] Enable
Authentication Protocol	Authentication protocols of a USM user including <b>MD5</b> and <b>SHA</b>  <b>NOTE</b> SHA is more secure than MD5. For security purposes, you are advised to select SHA for authentication.	[Default Value] SHA
Authentication Password	Authentication password of a USM user	[Default Rules]  The password must meet the following complexity requirements: <ul style="list-style-type: none"><li>● Contains 6 to 32 characters.</li><li>● Must contain special characters. Special characters include !"#\$%&amp;'()*+,-./;:&lt;=&gt;?@[{}]^`_{_}~ and spaces.</li><li>● Must contain two uppercase letters, lowercase letters, and digits.</li><li>● Cannot be the same as the username or the username written backwards.</li></ul> <b>NOTE</b> You can modify the default rule through CLI command <b>change snmp safe_strategy</b> .  [Example] usmuser@123

Parameter	Description	Value
Confirm Authentication Password	Confirming authentication password of a USM user	[Example] usmuser@123
Data Encryption	Whether to enable data encryption	[Default Value] Enable
Encryption Protocol	Encryption protocols of a USM user including <b>3DES</b> , <b>DES</b> , and <b>AES</b> .  <b>NOTE</b> Security performance order of three encryption protocols is as follows: AES > 3DES > DES. For security purposes, you are advised to select AES.	[Default Value] AES
Data Encryption Password	Password used by a USM user to encrypt data	[Default Rules] The password must meet the following complexity requirements: <ul style="list-style-type: none"><li>● Contains 6 to 32 characters.</li><li>● Must contain special characters. Special characters include !"#\$%&amp;'()*+,-./;:&lt;=&gt;?@[{}]^~_{ }~ and spaces.</li><li>● Must contain two uppercase letters, lowercase letters, and digits.</li><li>● Cannot be the same as the username or the username written backwards.</li></ul> <b>NOTE</b> You can modify the default rule through CLI command <b>change snmp safe_strategy</b> . [Example] dataencrypt@123
Confirm Data Encryption Password	Confirming that USM users used data encryption password	[Example] dataencrypt@123
User Level	User level of a USM user, including <b>Read-write</b> and <b>Read-only</b> .	[Default Value] Read-write

**Step 4** Click Save.

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

**Step 5** Click Close.

----End

#### 5.4.4.3 Managing Trap Server Addresses

To ensure that the storage system's alarm information 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 *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 generated after the trap server is configured and does not send alarms 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 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. These types of messages are sent to a recipient using User Datagram Protocol (UDP) and are not reliable. Specify trap service addresses if SNMP is used to report alarm messages.
- The DeviceManager provides the trap function to send the alarm messages of managed storage devices to another network management system or to a device at a specific server address. If alarm messages are reported in SNMP mode, you must configure Trap server addresses.

**NOTE**

To enable the trap function, install the associated software on application servers. For example, you must install **MIB** interface software on the application servers that run Windows 2003. To download the software, click this ([Link](#)), and see *MIB\_Interface\_File\_Usage\_Guide* to download software.

- To report alarm messages to other network management systems or storage devices, add or change the existing server addresses to the server addresses of those systems or devices.

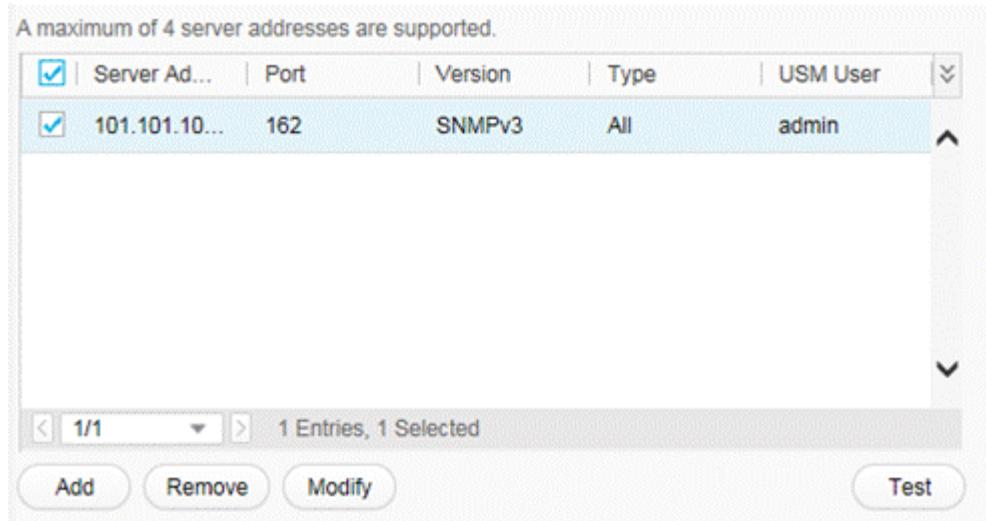
## Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Settings** >  **Alarm Settings** > **Trap Server Address Management**.

**Step 3** Manage trap server addresses. **Table 5-16** details the operations.

**Figure 5-26** Trap server address management area



**Table 5-16** Relevant operations

Operation	Procedure
Adding a server IP address	<ol style="list-style-type: none"><li>Click <b>Add</b>.</li><li>The <b>Add Server Address</b> dialog box is displayed.</li><li>Set the parameters for creating trap server addresses. <b>Table 5-17</b> lists related parameters.</li><li>Click <b>OK</b>.</li><li>The server list displays the newly added server IP address.</li></ol>
Modifying a server IP address	<ol style="list-style-type: none"><li>In the trap server address list, select the trap server address that you want to change and click <b>Modify</b>.</li><li>The <b>Modify Server Address</b> dialog box is displayed.</li><li>Change the trap server addresses.</li><li>Click <b>OK</b>.</li><li>The server list displays the modified server IP address.</li></ol>

Operation	Procedure
Removing a server IP address	In the list, select a server address that you want to remove and click <b>Remove</b> .

**Table 5-17** Trap server parameters

Parameter	Description	Example Value
Server Address	The address of a network management system or storage device for receiving alarm messages.	<p>[Value range]</p> <ul style="list-style-type: none"><li>● An IPv4 address has the following requirements:<ul style="list-style-type: none"><li>● The 32-bit address is evenly divided into four fields. Each 8-bit field is expressed in dotted-decimal.</li><li>● Each field of the IP address cannot be blank and must be an integer.</li><li>● The value of the first field ranges from 1 to 223 (excluding 127).</li><li>● The values of other fields range from 0 to 255.</li><li>● The IP address cannot be a special address such as the broadcast address.</li></ul></li><li>● An IPv6 address has the following requirements:<ul style="list-style-type: none"><li>● The 128-bit address is evenly divided into eight fields. Each 16-bit field is expressed in four hexadecimal numbers and separated with colons.</li><li>● In each 16-bit field, zeros before integers can be removed. However, at least one digit must be reserved in each field.</li><li>● 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-colon (:) can also be used to represent neighboring zeros of the IP address.</li><li>● The IP address cannot be a special address such as network address, loop address, or multicast address.</li><li>● The domain name has the following requirements:<ul style="list-style-type: none"><li>● A domain name is not case-sensitive and must be an English domain name.</li><li>● An English domain name contains 1 to 255 characters.</li><li>● An English domain name can only contain letters (a to z, A to Z), digits (0 to 9), dots (.), and hyphens (-). It cannot start or end with hyphens (-).</li></ul></li></ul></li></ul>

Parameter	Description	Example Value
		[Example] 192.168.100.11 fc00::1234 www.test.com
Port	Port for receiving alarm messages on the network management system or storage device.	[Value range] The value ranges from 1 to 65535. [Example] 2234
Version	SNMP version of a network management system or storage device. The possible value can be <b>SNMPv1</b> , <b>SNMPv2c</b> , or <b>SNMPv3</b> . <b>NOTE</b> To ensure data security, you are advised to use SNMPv3.	[Example] SNMPv3
USM User	The user report alarms from SNMP.	[Example] usm001

Parameter	Description	Example Value
Type	<p>Type of an alarm sent by a storage device to the trap server.</p> <ul style="list-style-type: none"><li>● Parsed: parsed alarms whose alarm IDs correspond to the same object identifier (OID).</li><li>● Original: alarms that have not been parsed.</li><li>● Parsed alarm oid: parsed alarms whose alarm IDs correspond to different OIDs.</li><li>● Parsed time string: parsed alarms whose alarm IDs correspond to the same OID. The data type of the event fields generated by alarms is OCTET STRING.</li><li>● Original time string: original alarms that have not been parsed. The data type of alarm occurring time (character string) and alarm clearing time (character string) is OCTET STRING.</li><li>● All: all alarms including the <b>Parsed</b>, <b>Original</b>, and <b>Parsed alarm oid</b> alarms.</li></ul> <p><b>NOTE</b></p> <ul style="list-style-type: none"><li>● Parsed and Original are two forms of one alarm. An alarm in the Original form carries only original alarm parameters, whereas an alarm in the Parsed form is readable and processed based on the Original form.</li><li>● When the value of <b>Version</b> is <b>SNMPv1</b>, the value of <b>Type</b> cannot be <b>Parsed alarm oid</b>.</li></ul>	[Example] Parsed

**Step 4** Click Save.

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

**Step 5** Click Close.

----End

## Follow-up Procedure

The following describes the format in which an alarm trap is sent.

- **Table 5-18** describes the format in which a Parsed alarm trap is sent.

**Table 5-18** Format in which an alarm trap of a Parsed alarm trap is sent

Bind Variable	Data Type	Meaning	Permission	Status
hwIsmReportingAlarmNode-Code OID: 1.3.6.1.4.1.2011.2.91.10.3.1.1 .1	OCTET STRING	Indicates the number of the node reporting an alarm.	accessible-for-notify	current
hwIsmReportingAlarmLocationInfo OID: 1.3.6.1.4.1.2011.2.91.10.3.1.1 .2	OCTET STRING	Indicates the location of an alarm. The format is Name1=Value1, ..., NameN=ValueN.	accessible-for-notify	current
hwIsmReportingAlarmRestoreAdvice OID: 1.3.6.1.4.1.2011.2.91.10.3.1.1 .3	OCTET STRING	Indicates the alarm clearance suggestion.	accessible-for-notify	current
hwIsmReportingAlarmFault-Title OID: 1.3.6.1.4.1.2011.2.91.10.3.1.1 .4	OCTET STRING	Indicates the title of alarm information.	accessible-for-notify	current
hwIsmReportingAlarmFault-Type OID: 1.3.6.1.4.1.2011.2.91.10.3.1.1 .5	INTEGER	Indicates the alarm type. For example, 2 represents a device alarm.	accessible-for-notify	current

Bind Variable	Data Type	Meaning	Permission	Status
hwIsmReportingAlarmFault-Level  OID: 1.3.6.1.4.1.2011.2.91.10.3.1.1 .6	INTEGER	Indicates the alarm severity of the I2000 network management system (NMS) software.  ● 1-Critical alarm ● 2-Major alarm ● 3-Minor alarm ● 4-Warning alarm	accessible-for-notify	current
hwIsmReportingAlarmAlarmID  OID: 1.3.6.1.4.1.2011.2.91.10.3.1.1 .7	Gauge32	Indicates the alarm ID of the I2000 NMS software.	accessible-for-notify	current
hwIsmReportingAlarmFault-Time  OID: 1.3.6.1.4.1.2011.2.91.10.3.1.1 .8	DateAnd Time	Indicates the time an alarm is generated.	accessible-for-notify	current
hwIsmReportingAlarmSerial-No  OID: 1.3.6.1.4.1.2011.2.91.10.3.1.1 .9	Gauge32	Indicates the alarm SN.	accessible-for-notify	current
hwIsmReportingAlarmAdditionInfo  OID: 1.3.6.1.4.1.2011.2.91.10.3.1.1 .10	OCTET STRING	Describes the cause of an alarm.	accessible-for-notify	current
hwIsmReportingAlarmFault-Category  OID: 1.3.6.1.4.1.2011.2.91.10.3.1.1 .11	INTEGER	Indicates the alarm type.  ● 1-Fault alarm ● 2-Recovery alarm ● 3-Event alarm	accessible-for-notify	current

Bind Variable	Data Type	Meaning	Permission	Status
hwIsmReportingAlarmLocationAlarmID  OID: 1.3.6.1.4.1.2011.2.91.10.3.1.1 .12	Counter64	Indicates the ID of the original alarm.	accessible-for-notify	current
hwIsmReportingAlarmProductModel  OID: 1.3.6.1.4.1.2011.2.91.10.3.1.1 .13	Integer32	Indicates the device model.	accessible-for-notify	current
hwIsmReportingAlarmProductSN  OID: 1.3.6.1.4.1.2011.2.91.10.3.1.1 .14	OCTET STRING	Indicates the device SN.	accessible-for-notify	current
hwIsmReportingAlarmProductName  OID: 1.3.6.1.4.1.2011.2.91.10.3.1.1 .15	OCTET STRING	Indicates the device name.	accessible-for-notify	current

- **Table 5-19** describes the format in which an Original alarm trap is sent.

**Table 5-19** Format in which an Original alarm trap is sent

Bind Variable	Data Type	Meaning	Permission	Status
hwIsmTrapEventType  OID: 1.3.6.1.4.1.34774.4.1.3.3 .1	Gauge32	Indicates the alarm type. The value can be: ● 0: Event ● 1: Fault ● 2: Recovery	accessible-for-notify	current
hwIsmTrapEventID  OID: 1.3.6.1.4.1.34774.4.1.3.3 .2	Counter64	Indicates the ID of the original alarm.	accessible-for-notify	current

Bind Variable	Data Type	Meaning	Permission	Status
hwIsmTrapEventLevel OID: 1.3.6.1.4.1.34774.4.1.3.3 .3	Gauge 32	Indicates the alarm severity. The value can be: <ul style="list-style-type: none"><li>● 2: Information</li><li>● 3: Warning</li><li>● 5: Major</li><li>● 6: Critical</li></ul>	accessible-for-notify	current
hwIsmTrapEventSequence OID: 1.3.6.1.4.1.34774.4.1.3.3 .4	Gauge 32	Indicates the alarm SN.	accessible-for-notify	current
hwIsmTrapEventTime OID: 1.3.6.1.4.1.34774.4.1.3.3 .5	Gauge 32	Indicates the UTC time (in seconds) when an alarm is generated.	accessible-for-notify	current
hwIsmTrapEventRecoveryTime OID: 1.3.6.1.4.1.34774.4.1.3.3 .6	Gauge 32	Indicates the UTC time (in seconds) when an alarm is cleared.	accessible-for-notify	current
hwIsmTrapEventParameter OID: 1.3.6.1.4.1.34774.4.1.3.3 .7	OCTET STRING	Indicates an alarm parameter (format: Para1, Para2, and so on). <b>NOTE</b> This parameter can be used to provide the alarm description. It is used together with the alarm configuration file of the upper-layer network management system.	accessible-for-notify	current
hwIsmTrapEventID32Bit OID: 1.3.6.1.4.1.34774.4.1.3.3 .8	Gauge 32	Indicates the alarm ID of the I2000 NMS software.	accessible-for-notify	current
hwIsmTrapEventTimeStr OID: 1.3.6.1.4.1.34774.4.1.3.3 .9	OCTET STRING	Indicates the time an alarm is generated (format: character string).	accessible-for-notify	current

Bind Variable	Data Type	Meaning	Permission	Status
hwIsmTrapEventRecoveryTimeStr OID: 1.3.6.1.4.1.34774.4.1.3.3 .10	OCTET STRING	Indicates the time an alarm is cleared (format: character string).	accessible-for-notify	current

- **Table 5-20** describes the format in which a Parsed time string alarm trap is sent.

**Table 5-20** Format in which a Parsed time string alarm trap

Bind Variable	Data Type	Meaning	Permission	Status
hwStorageReportingAlarm-NodeCode OID: 1.3.6.1.4.1.2011.2.251.20.1.3 .1	OCTET STRING	Indicates the number of the node reporting an alarm.	accessible-for-notify	current
hwStorageReportingAlarm-LocationInfo OID: 1.3.6.1.4.1.2011.2.251.20.1.3 .2	OCTET STRING	Indicates the location of an alarm. The format is Name1=Value1, Name2=Value2, and so on.	accessible-for-notify	current
hwStorageReportingAlarm-RestoreAdvice OID: 1.3.6.1.4.1.2011.2.251.20.1.3 .3	OCTET STRING	Indicates the alarm clearing suggestion.	accessible-for-notify	current
hwStorageReportingAlarm-FaultTitle OID: 1.3.6.1.4.1.2011.2.251.20.1.3 .4	OCTET STRING	Indicates the title of alarm information.	accessible-for-notify	current
hwStorageReportingAlarm-FaultType OID: 1.3.6.1.4.1.2011.2.251.20.1.3 .5	INTEGER	Indicates the alarm type. For example, 2 represents a device alarm.	accessible-for-notify	current

Bind Variable	Data Type	Meaning	Permission	Status
hwStorageReportingAlarm-FaultLevel  OID: 1.3.6.1.4.1.2011.2.251.20.1.3 .6	INTEGER	Indicates the alarm severity of the I2000 NMS software. <ul style="list-style-type: none"><li>● 1-Critical alarm</li><li>● 2-Major alarm</li><li>● 3-Minor alarm</li><li>● 4-Warning alarm</li></ul>	accessible-for-notify	current
hwStorageReportingAlarm-AlarmID  OID: 1.3.6.1.4.1.2011.2.251.20.1.3 .7	Gauge 32	Indicates the alarm ID of the I2000 NMS software.	accessible-for-notify	current
hwStorageReportingAlarm-FaultTime  OID: 1.3.6.1.4.1.2011.2.251.20.1.3 .8	OCTET STRING	Indicates the time an alarm is generated.	accessible-for-notify	current
hwStorageReportingAlarm-SerialNo  OID: 1.3.6.1.4.1.2011.2.251.20.1.3 .9	Gauge 32	Indicates the alarm SN.	accessible-for-notify	current
hwStorageReportingAlarm-AdditionInfo  OID: 1.3.6.1.4.1.2011.2.251.20.1.3 .10	OCTET STRING	Describes the cause of an alarm.	accessible-for-notify	current
hwStorageReportingAlarm-FaultCategory  OID: 1.3.6.1.4.1.2011.2.251.20.1.3 .11	INTEGER	Indicates the alarm type. <ul style="list-style-type: none"><li>● 1-Fault alarm</li><li>● 2-Recovery alarm</li><li>● 3-Event alarm</li></ul>	accessible-for-notify	current
hwStorageReportingAlarm-LocationAlarmID  OID: 1.3.6.1.4.1.2011.2.251.20.1.3 .12	Counter64	Indicates the ID of the original alarm.	accessible-for-notify	current

Bind Variable	Data Type	Meaning	Permission	Status
hwStorageReportingAlarm-ProductModel  OID: 1.3.6.1.4.1.2011.2.251.20.1.3 .13	Integer32	Indicates the device model.	accessible-for-notify	current
hwStorageReportingAlarm-ProductSN  OID: 1.3.6.1.4.1.2011.2.251.20.1.3 .14	OCTET STRING	Indicates the device SN.	accessible-for-notify	current
hwStorageReportingAlarm-ProductName  OID: 1.3.6.1.4.1.2011.2.251.20.1.3 .15	OCTET STRING	Indicates the device name.	accessible-for-notify	current

- **Table 5-21** describes the format in which an alarm trap of the Original time string type is sent.

**Table 5-21** Format in which an Original time string alarm trap is sent

Bind Variable	Data Type	Meaning	Permission	Status
hwStorageTrapEvent-Type  OID: 1.3.6.1.4.1.2011.2.251.2 0.2.2.1	Gauge 32	Indicates the alarm type. The value can be: <ul style="list-style-type: none"><li>● 0: Event</li><li>● 1: Fault</li><li>● 2: Recovery</li></ul>	accessible-for-notify	current
hwStorageTrapEventID  OID: 1.3.6.1.4.1.2011.2.251.2 0.2.2.2	Counter64	Indicates the ID of the original alarm.	accessible-for-notify	current
hwStorageTrapEventLevel  OID: 1.3.6.1.4.1.2011.2.251.2 0.2.2.3	Gauge 32	Indicates the alarm severity. The value can be: <ul style="list-style-type: none"><li>● 2: Information</li><li>● 3: Warning</li><li>● 5: Major</li><li>● 6: Critical</li></ul>	accessible-for-notify	current

Bind Variable	Data Type	Meaning	Permission	Status
hwStorageTrapEvent-Sequence  OID: 1.3.6.1.4.1.2011.2.251.2 0.2.2.4	Gauge 32	Indicates the alarm SN.	accessible-for-notify	current
hwStorageTrapEvent-Time  OID: 1.3.6.1.4.1.2011.2.251.2 0.2.2.5	Gauge 32	Indicates the UTC time (in seconds) when an alarm is generated.	accessible-for-notify	current
hwStorageTrapEventRecoveryTime  OID: 1.3.6.1.4.1.2011.2.251.2 0.2.2.6	Gauge 32	Indicates the UTC time (in seconds) when an alarm is cleared.	accessible-for-notify	current
hwStorageTrapEventParameter  OID: 1.3.6.1.4.1.2011.2.251.2 0.2.2.7	OCTET STRING	Indicates an alarm parameter (format: Para1, Para2, and so on).  <b>NOTE</b> This parameter can be used to resolve alarm description. It is used together with the alarm configuration file of the upper-layer network management system.	accessible-for-notify	current
hwStorageTrapEventID32Bit  OID: 1.3.6.1.4.1.2011.2.251.2 0.2.2.8	Gauge 32	Indicates the alarm ID of the I2000 NMS software.	accessible-for-notify	current
hwStorageTrapEventTimeStr  OID: 1.3.6.1.4.1.2011.2.251.2 0.2.2.9	OCTET STRING	Indicates the time an alarm is generated (format: character string).	accessible-for-notify	current
hwStorageTrapEventRecoveryTimeStr  OID: 1.3.6.1.4.1.2011.2.251.2 0.2.2.10	OCTET STRING	Indicates the time an alarm is cleared (format: character string).	accessible-for-notify	current

- **Table 5-22** describes the format in which a Parsed alarm oid alarm trap is sent.

**Table 5-22** Format in which a Parsed alarm oid alarm trap

Bind Variable	Data Type	Meaning	Permission	Status
hwStorageReportingAlarm-NodeCode OID: 1.3.6.1.4.1.2011.2.251.20.1.3 .1	OCTET STRING	Indicates the number of the node reporting an alarm.	accessible-for-notify	current
hwStorageReportingAlarm-LocationInfo OID: 1.3.6.1.4.1.2011.2.251.20.1.3 .2	OCTET STRING	Indicates the location of an alarm. The format is Name1=Value1, Name2=Value2, and so on.	accessible-for-notify	current
hwStorageReportingAlarm-RestoreAdvice OID: 1.3.6.1.4.1.2011.2.251.20.1.3 .3	OCTET STRING	Indicates the alarm clearing suggestion.	accessible-for-notify	current
hwStorageReportingAlarm-FaultTitle OID: 1.3.6.1.4.1.2011.2.251.20.1.3 .4	OCTET STRING	Indicates the title of alarm information.	accessible-for-notify	current
hwStorageReportingAlarm-FaultType OID: 1.3.6.1.4.1.2011.2.251.20.1.3 .5	INTEGER	Indicates the alarm type. For example, 2 represents a device alarm.	accessible-for-notify	current
hwStorageReportingAlarm-FaultLevel OID: 1.3.6.1.4.1.2011.2.251.20.1.3 .6	INTEGER	Indicates the alarm severity of the I2000 NMS software. ● 1-Critical alarm ● 2-Major alarm ● 3-Minor alarm ● 4-Warning alarm	accessible-for-notify	current
hwStorageReportingAlarm-AlarmID OID: 1.3.6.1.4.1.2011.2.251.20.1.3 .7	Gauge 32	Indicates the alarm ID of the I2000 NMS software.	accessible-for-notify	current

Bind Variable	Data Type	Meaning	Permission	Status
hwStorageReportingAlarm-FaultTime  OID: 1.3.6.1.4.1.2011.2.251.20.1.3 .8	OCTET STRING	Indicates the time an alarm is generated.	accessible-for-notify	current
hwStorageReportingAlarm-SerialNo  OID: 1.3.6.1.4.1.2011.2.251.20.1.3 .9	Gauge 32	Indicates the alarm SN.	accessible-for-notify	current
hwStorageReportingAlarmAdditionInfo  OID: 1.3.6.1.4.1.2011.2.251.20.1.3 .10	OCTET STRING	Describes the cause of an alarm.	accessible-for-notify	current
hwStorageReportingAlarm-FaultCategory  OID: 1.3.6.1.4.1.2011.2.251.20.1.3 .11	INTEGER	Indicates the alarm type. ● 1-Fault alarm ● 2-Recovery alarm ● 3-Event alarm	accessible-for-notify	current
hwStorageReportingAlarm-LocationAlarmID  OID: 1.3.6.1.4.1.2011.2.251.20.1.3 .12	Counter64	Indicates the ID of the original alarm.	accessible-for-notify	current
hwStorageReportingAlarm-ProductModel  OID: 1.3.6.1.4.1.2011.2.251.20.1.3 .13	Integer32	Indicates the device model.	accessible-for-notify	current
hwStorageReportingAlarm-ProductSN  OID: 1.3.6.1.4.1.2011.2.251.20.1.3 .14	OCTET STRING	Indicates the device SN.	accessible-for-notify	current
hwStorageReportingAlarm-ProductName  OID: 1.3.6.1.4.1.2011.2.251.20.1.3 .15	OCTET STRING	Indicates the device name.	accessible-for-notify	current

## 5.4.5 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.

### 5.4.5.1 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 to 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

#### 5.4.5.2 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 alarm dump is not configured for the storage system, when the number of generated events reaches 45,000, the alarm named **The Space That Stores Event Logs Is To Be Used Up** is triggered. When the number of generated events reaches 50,000 (the upper limit), the first 10,000 events are deleted automatically.

- If alarm dump is configured for the storage system, when the number of generated events reaches 45,000, the alarm named **The Space That Stores Event Logs Is To Be Used Up** is not triggered. When the number of generated events reaches 50,000 (the upper limit), the first 10,000 events are dumped automatically to the specified FTP server or SFTP server.

## Procedure

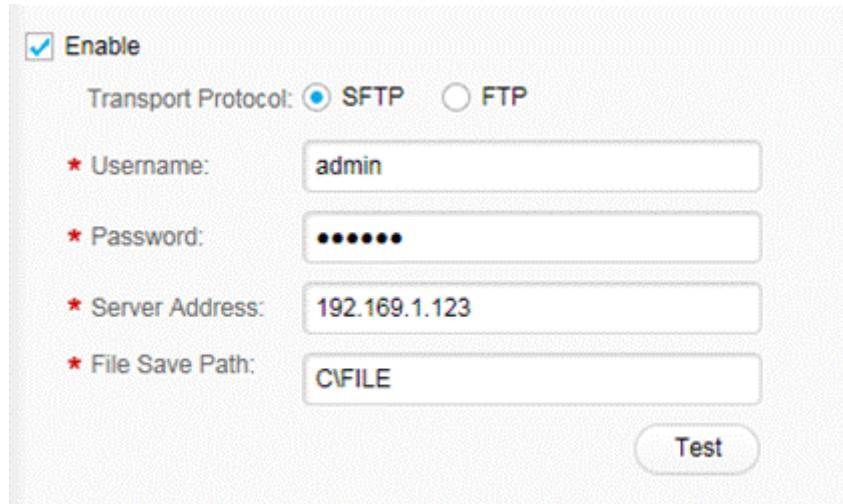
**Step 1** Log in to DeviceManager.

**Step 2** Choose  Settings >  Alarm Settings.

**Step 3** Modify parameters for the alarm dump.

1. In the navigation tree, choose **Alarm Dump**.
2. Modify parameters for the alarm dump. **Table 5-23** lists related parameters.

**Figure 5-27** Page for alarm dump settings



**Table 5-23** Parameters for the alarm dump

Parameter	Description	Example Value
Transport Protocol	<p>The transport protocol of the alarm dump. The values are <b>SFTP</b> or <b>FTP</b>.</p> <p><b>NOTE</b></p> <p>To ensure the security of data transfers, you are advised to use Secure File Transfer Protocol (SFTP).</p>	[Example] FTP

Parameter	Description	Example Value
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
Password	Password for logging in to a server.	[Value range] - The value must contain 1 to 63 characters. - The password cannot contain extended ASCII characters or Unicode characters. Otherwise, the password is invalid. It is recommended that the password contain characters from the following categories: <ul style="list-style-type: none"><li>■ Base 10 digits (0-9)</li><li>■ English uppercase characters (A-Z)</li><li>■ English lowercase characters (a-z)</li><li>■ Space</li><li>■ Special characters such as [!^_{}~`@!"#\$%&amp;'()^+-.:/;,&lt;=&gt;?]</li></ul> [Example] 123456

Parameter	Description	Example Value
Server	IP address or domain name of a server.	<p>[Value range]</p> <ul style="list-style-type: none"><li>- An IPv4 address has the following requirements:<ul style="list-style-type: none"><li>- The 32-bit address is evenly divided into four fields. Each 8-bit field is expressed in dotted-decimal.</li><li>- Each field of the IP address cannot be blank and must be an integer.</li><li>- The value of the first field ranges from 1 to 223 (excluding 127).</li><li>- The values of other fields range from 0 to 255.</li><li>- The IP address cannot be a special address such as the broadcast address.</li></ul></li><li>- An IPv6 address has the following requirements:<ul style="list-style-type: none"><li>- The 128-bit address is evenly divided into eight fields. Each 16-bit field is expressed in four hexadecimal numbers and separated with colons.</li><li>- In each 16-bit field, zeros before integers can be removed. However, at least one digit must be reserved in each field.</li><li>- If the IP address contains a long string of zeros, you can represent the neighboring zeros with double-colon (::) in the colon-separated hexadecimal field. Each IP address contains only one double-colon (::). The double-colon (::) can also be used to represent neighboring zeros of the IP address.</li><li>- The IP address cannot be a special address such as network address, loop address, or multicast address.</li><li>- The domain name has the following requirements:</li></ul></li></ul>

Parameter	Description	Example Value
		<ul style="list-style-type: none"> <li>- A domain name is not case-sensitive and must be an English domain name.</li> <li>- An English domain name contains 1 to 255 characters.</li> <li>- An English domain name can only contain letters (a to z, A to Z), digits (0 to 9), dots (.), and hyphens (-). It cannot start or end with hyphens (-).</li> </ul> <p>[Example]</p> <p>192.168.0.1 fc00::1234 www.test.com</p>
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 <b>File Save Path</b> on DeviceManager.	<p>[Value range]</p> <p>A file saving path must contain 1 to 255 characters.</p> <p>[Example]</p> <p>If you set the path to <b>G:\</b> and create a folder named <b>alarm</b> on the FTP server, type <b>alarm</b> in <b>File Save Path</b>.</p>

3. (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 4** Confirm the parameter modification for the alarm dump.

1. Click **Save**.  
The **Execution Result** dialog box is displayed indicating that the operation succeeded.
  2. Click **Close**.
- End

## 5.4.6 Configuring Alarm Masking

After the alarm masking function is enabled, DeviceManager does not monitor alarms of a specified object or does not monitor certain unimportant alarms to improve fault locating efficiency.

### Context

After the alarm masking function is enabled, alarms of the specified devices will not be reported to the NMS (including DeviceManager management interface or third-party NMS

connected to the storage system), and will not trigger email notification, SMS notification, Syslog notification, or Trap alarm notification.

## Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  Settings >  Alarm Settings.

**Step 3** In the left navigation tree, select the **Alarm Masking** node.

**Step 4** View all of the alarms in the system. Table 5-24 describes the related parameters.

**Figure 5-28** Alarm masking management dialog box

Name	Alarm ID	Alarm Type	Level	Alarm Masking	Unhandled Alarms
<input checked="" type="checkbox"/> Management Network Port Is Fa...	0xF0060001	--	Major	Disable	Not Exist
<input type="checkbox"/> Host Port Link Down	0xF0060002	--	Major	Disable	Not Exist
<input type="checkbox"/> Expansion Port Partially Damaged	0xF01080014	--	Informational	Enable	Exist
<input type="checkbox"/> Port Negotiated Rate Is Smaller...	0xF00C90016	--	Warning	Enable	Exist
<input type="checkbox"/> Disk Is About To Fail	0xF00A0001	--	Critical	Disable	Exist
<input type="checkbox"/> Slow Disk Response	0xF00A0002	--	Warning	Enable	Exist
<input type="checkbox"/> Coffer Disks Not Found	0xF00A0003	--	Major	Disable	Not Exist
<input type="checkbox"/> Failed To Authenticate Self-Encr...	0xF00A0004	--	Warning	Enable	Not Exist
<input type="checkbox"/> LUN Has A Medium Error	0xF00B0001	--	Major	Enable	Not Exist
<input type="checkbox"/> FC Link Of Heterogeneous Array...	0xF00B0002	--	Warning	Disable	Not Exist
<input type="checkbox"/> iSCSI Link Of Heterogeneous Ar...	0xF00B003D	--	Critical	Disable	Exist
<input type="checkbox"/> An Unrepairable Sector Was Dis...	0xF00B0050	--	Informational	Enable	Exist
<input type="checkbox"/> Succeeded In Modifying The Na...	0x200F000E0014	--	Informational	Disable	Not Exist
<input type="checkbox"/> Failed To Delete A Host Group	0x200F000E0015	--	Major	Disable	Not Exist
<input type="checkbox"/> Succeeded In Deleting A Host G...	0x200F000E0016	--	Warning	Enable	Exist
<input type="checkbox"/> Failed To Add A Host	0x200F000E0017	--	Critical	Enable	Exist
<input type="checkbox"/> Link Between A Host And Storag...	0xF00150019	--	Major	Disable	Not Exist
<input type="checkbox"/> Succeeded In Creating A Host	0xF0015001A	--	Informational	Disable	Not Exist
<input type="checkbox"/> Host Is Not Redundantly Connec...	0xF0015001B	--	Critical	Enable	Exist

**Table 5-24** Alarm masking parameters

Parameter	Description
Name	Indicates the name of an alarm.
Alarm ID	Indicates the alarm ID.
Alarm Type	Indicates the system type of an alarm.
Level	Indicates the severity of an alarm. The possible values are <b>Critical</b> , <b>Major</b> , <b>Warning</b> , and <b>Info</b> .
Alarm Masking	Enables or disables alarm masking.
Unhandled Alarms	Indicates whether alarms are not cleared in the system or not.

 **NOTE**

- You can select one or more alarms that you want to mask and click **Enable Alarm Masking**. The system will not report the selected alarms.
- You can select one or more alarms and click **Disable Alarm Masking**. The system will not mask the selected alarms.

----End

## 5.5 Enabling and Managing the Call Home Service (Applicable to V300R006C10 and later)

The storage system provides the Call Home service to automatically upload alarms and logs to Huawei technical support center, thereby improving the troubleshooting efficiency.

### 5.5.1 About the Call Home Service

The Call Home service enables a storage system to periodically upload performance data, running data, alarm data, system logs, and diagnostic files to eService cloud, reducing the maintenance cost and improving the maintenance efficiency.

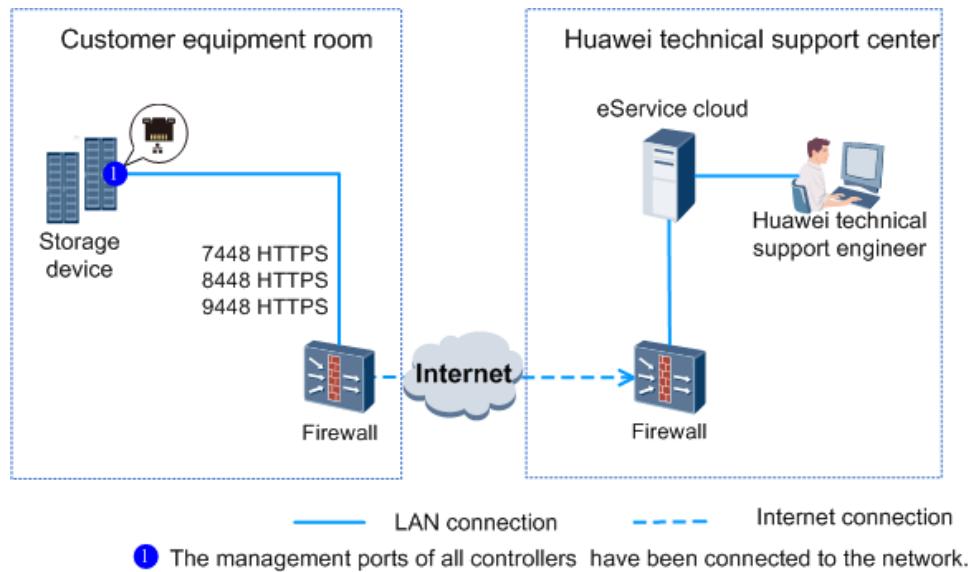
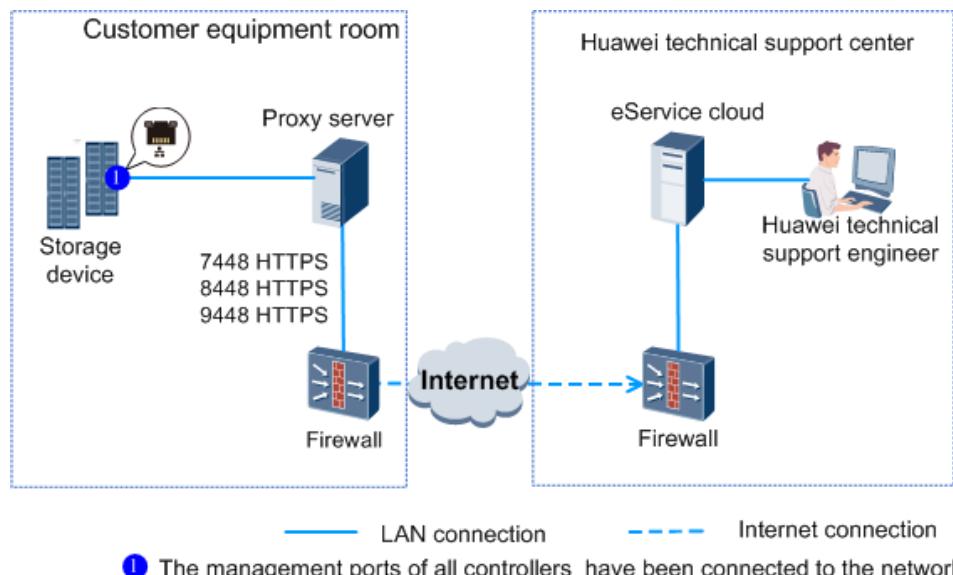
#### Positioning

Traditionally, performance data, running data, alarm data, system logs, and diagnostic files 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 Call Home service enables storage systems to periodically upload system data and logs to eService cloud. In this way, if a fault occurs on a storage system, Huawei technical support center can be promptly informed of fault information. This facilitates fault discovery and shortens troubleshooting time.

The Call Home service securely connects a storage system and the eService cloud remotely deployed in Huawei technical support center. The storage system encrypts alarm data, running data, performance data, and system logs and sends them to the eService cloud through Internet.

- The eService cloud receives alarm data, running data, performance data, and diagnostic files from storage systems 24/7 hours and automatically notifies Huawei technical support engineers.
- Technical support engineers need to manually trigger the uploading of system logs from the eService cloud to Huawei technical support center.

The Call Home service uses the secure Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS). The Call Home service allows a storage system to communicate with eService directly or through an internal HTTP proxy server. [Figure 5-29](#) and [Figure 5-30](#) illustrate the two types of networking.

**Figure 5-29** Direct-connection networking**Figure 5-30** 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 direct-connection networking nor internal HTTP proxy server is supported, the eService Client can be deployed to upload storage alarms and logs to the eService cloud. For details, see the *eService V2R2C00 User Guide*.

## Supported Data Types

After the Call Home service is enabled, running, performance, alarm data, system logs, and diagnostic files of storage systems can be uploaded to Huawei technical support center. **Table 5-25** describes the data.

**Table 5-25** Supported data types

Data Type	Description	Uploading Interval
Performance data	A .txt file in the JSON format	New performance data is uploaded to the eService cloud every 5 minutes.
Running data	A .txt file	Running data is uploaded to the eService cloud every 24 hours.
Alarm data	<ul style="list-style-type: none"><li>● A .txt file in the JSON format</li><li>● HTTP POST request, with the media type being <b>application/json</b></li></ul>	<ul style="list-style-type: none"><li>● File New alarm data is uploaded to the eService cloud every 5 minutes.</li><li>● HTTP POST request New alarm data is uploaded to the eService cloud every minute.</li></ul>
System log	A .tgz file	Huawei technical support engineers manually trigger the uploading of system logs from the eService cloud 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.
Diagnostic file	A .tgz file	<ul style="list-style-type: none"><li>● If fault alarms of a storage system are generated, a diagnostic file will be sent at the maximum frequency of one time per hour.</li><li>● If no fault alarm of a storage system is generated within 24 hours, a diagnostic file will be sent every 24 hours.</li></ul>

 **NOTE**

The performance data file uploaded a time must not exceed 5 MB. There is no limit on the size of alarm data, running data, system log and diagnostic files to be uploaded.

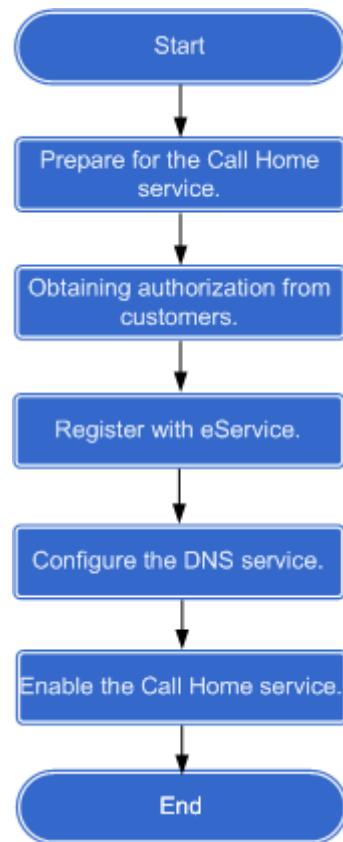
## 5.5.2 Configuring the Call Home Service

This section describes how to prepare and configure the Call Home service.

### 5.5.2.1 Configuration Process

This section describes the overall process for configuring the Call Home service.

[Figure 5-31](#) illustrates the overall process for configuring the Call Home service.

**Figure 5-31** Overall process for configuring the Call Home service

### 5.5.2.2 Preparations

This section describes preparations that you are advised to make before configuring the Call Home service.

Item	Description
Obtaining contact details about Huawei technical support center.	<p>Before deploying the Call Home service, you need to obtain the Letter of Authorization on the Deployment of Huawei OceanStor eService and Processing of [Customer]'s Data from Huawei technical support center. During Call Home service configuration, you need to contact Huawei technical support center to authenticate storage devices on which the Call Home service will be deployed.</p> <p>To obtain contact details about Huawei technical support center:</p> <ul style="list-style-type: none"><li>For carrier users, visit <a href="http://support.huawei.com/carrier/docview!docview?nid=IN0000034614&amp;path=NN-000005#click=myApply">http://support.huawei.com/carrier/docview!docview?nid=IN0000034614&amp;path=NN-000005#click=myApply</a>.</li><li>For enterprise users, visit <a href="http://e.huawei.com/en/service-hotline">http://e.huawei.com/en/service-hotline</a>.</li></ul>

Item	Description
Obtaining the Equipment Serial Number (ESN) and site name of a storage device	The ESN and site name of a storage device are required when Huawei technical support center authenticates the storage device.  You can obtain the ESN based on the following procedure: <ul style="list-style-type: none"><li>On the navigation bar of DeviceManager, click <b>Home</b>. In the function pane, locate <b>SN</b> in the <b>Basic information</b> area.</li><li>Log in to the command-line interface (CLI). Run the <b>show system general</b> command and locate <b>SN</b>.</li></ul>
Preparing the network	The network bandwidth must be greater than or equal to 10 Mbit/s.
Enabling ports 7448/TCP, 8448/TCP, and 9448/TCP on the firewall	The eService cloud server uses ports 7448, 8448, and 9448. Enable the three ports on the firewall to allow storage systems to send HTTP requests to the eService cloud server.
(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 customer's support account	Customer's support account must be sent to Huawei technical support center for registration so that the customer can use the support account to log in to eService.
Obtaining a Huawei employee support account for device authentication	During Call Home service configuration, a Huawei employee support account is required for device authentication. If you do not have such an account, contact Huawei technical support center to apply for one.

### 5.5.2.3 Obtaining Authorization from Customers

Before enabling the Call Home service, you must obtain authorization from the customer.

To ensure customer network and information security and avoid cyber security risks caused by human factors, Huawei will clarify information (including data collection intervals and modes) about all operations to be performed as well as their scopes and impact to customers before deploying a service and apply for authorization on these operations. Huawei can perform only authorized operations after obtaining written consent from customers.

Obtain the Letter of Authorization on the Deployment of Huawei OceanStor eService and Processing of [Customer]'s Data from Huawei technical support center. Invite the customer to sign the Letter.

### 5.5.2.4 Registering with eService

Huawei technical support center can handle alarms and logs reported by a storage device only after the device is registered with eService.

## Context

- Maintenance personnel at Huawei technical center are responsible for registering a storage device with eService.
- Call Home service support personnel must provide the ESN and site name of the storage device to be registered as well as the customer's support account to maintenance personnel at Huawei technical center. For details about how to obtain contact details about Huawei technical center and the ESN of a storage device, see [5.5.2.2 Preparations](#).

## Procedure

- Step 1** Call Home service support personnel email the scanned copy of *Deployment of Huawei OceanStor eService and Processing of [Customer]’s Data* signed by the customer to maintenance personnel at Huawei technical support center and contact them to register the site with eService.
- Step 2** Maintenance personnel of Huawei technical support center enter the ESN, site name of the storage device, and customer's support account to eService and complete the registration.
- Step 3** After the storage device is registered, maintenance personnel at Huawei technical support center notify the Call Home service support personnel.

----End

## 5.5.2.5 Configuring the DNS Service

After a storage system is connected to a DNS server, you can resolve and access the external domain addresses through the storage system. This operation enables you to configure a system management IP address for the active or standby DNS.

## Prerequisites

Network management personnel of a customer's equipment room have confirmed that DNS servers are running properly.

## Context

- A DNS server is used to resolve external domain name addresses.
- If you want to configure a standby DNS server, keep the domain names of the active and standby servers consistent.
- Management network port 0 of management module A or management module B of the controller enclosure 0 has been connected to the network. And run **change system management\_ip** command to change the management IP address to an IP address in the customer's network segment. For details about the command, see *CommandReference*

## 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.

4. (Optional) Test the connection between the DNS server and storage system.
  - You can click **Test** of each DNS IP address to test its availability.
  - You can click **Test All** to test the connection between the DNS server and storage system.

**Step 4** Click **Save**.

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

**Step 5** Click **OK**.

----End

### 5.5.2.6 Enabling the Call Home Service

This section describes how to enable the Call Home service for a storage system.

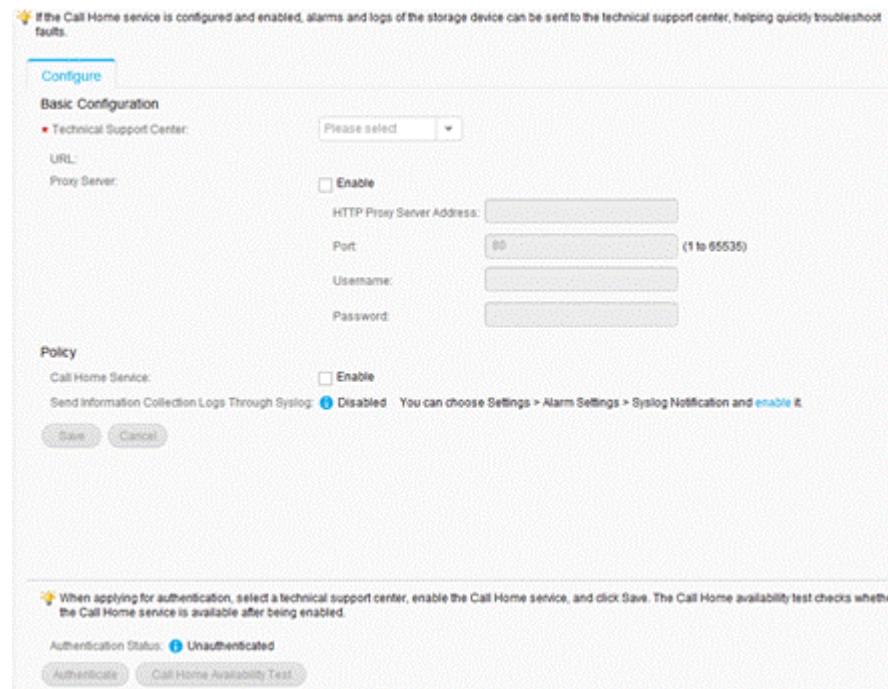
#### Prerequisites

- The storage system is working properly.
- The management ports of the storage system have been connected to the public transmission network. For details about how to connect management ports to the public transmission network, see the *Installation Guide* of the corresponding product model.
- The DNS service has been configured.
- The storage system has been registered with eService.
- The network bandwidth is greater than or equal to 10 Mbit/s.

#### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose **Settings** > **Storage Settings** > **Value-added Service Settings** > **Call Home Service**.

**Step 3** Set basic configuration for the Call Home service.

1. Select the technical support center to which the storage system data will be uploaded.  
**Table 5-26** describes basic parameters.

**Table 5-26** Basic parameters for the Call Home service

Parameter	Description	Value
Technical Support Center	Specifies the technical support center to which data will be uploaded.	[Value range] <b>Carrier in China region</b> , <b>Carrier in Romania region</b> , <b>Enterprise in China region</b> , and <b>Enterprise in Romania region</b> [Example] <b>Enterprise in Romania region</b>

Parameter	Description	Value
URL	<p>Displays the URL of the technical support center to which data will be uploaded.</p> <p><b>NOTE</b></p> <p>After you select <b>Technical Support Center</b>, the URL address of the technical support center is displayed. You do not need to manually select a URL.</p>	<p>[Value range]</p> <ul style="list-style-type: none"><li>- <b>Carrier in China region:</b> icloudservice-cn.huawei.com</li><li>- <b>Carrier in Romania region:</b> itr-eservicero-carrier.huawei.com</li><li>- <b>Enterprise in China region:</b> ecloudService-cn.huawei.com</li><li>- <b>Enterprise in Romania region:</b> itr-eservicero-ent.huawei.com</li></ul> <p>[Example]</p> <p><b>itr-eservicero-ent.huawei.com</b></p>

1. (Optional) Configure a proxy server.

If storage systems access Internet through internal HTTP proxy, a proxy server must be configured. [Table 5-27](#) describes the proxy server parameters.

**Table 5-27** Proxy server parameters

Parameter	Description	Value	
HTTP Proxy Server Address	Specifies the HTTP proxy server address.	[Value range] Only IPv4 addresses and domain names are supported. <ul style="list-style-type: none"><li>- An IPv4 address has the following requirements:<ul style="list-style-type: none"><li>- The 32-bit address is evenly divided into four fields. Each 8-bit field is expressed in dotted-decimal.</li><li>- Each field of the IP address cannot be blank and must be an integer.</li><li>- The values of other fields range from 0 to 255.</li><li>- The value of the first field ranges from 1 to 223.</li><li>- The IP address cannot be a special address such as the broadcast address.</li><li>- The domain name has the following requirements:<ul style="list-style-type: none"><li>- A domain name is not case-sensitive and must be an English domain name.</li><li>- An English domain name contains 1 to 255 characters.</li><li>- An English domain name can only contain letters (a to z, A to Z), digits (0 to 9), dots (.), and hyphens (-). It cannot start or end with hyphens (-).</li></ul></li></ul></li></ul>	[Example] 192.168.0.1

Parameter	Description	Value
		test.com
Port	Specifies the HTTP proxy server port.	[Value range] 1 to 65535 [Example] 80
Username	Specifies the username.	[Value range] - The username must contain 1 to 63 characters. - The username cannot contain single quotation marks ('). [Example] files
Password	Specifies the user password.	[Value range] The password must contain 1 to 63 characters. [Example] 123456

**Step 4** Configure policies for the Call Home service. **Table 5-28** describes policy parameters.

**Table 5-28** Policy parameters

Parameter	Description	Value
Call Home Service	Specifies whether to enable the Call Home service to collect device logs.	[Example] Enabled
(Optional) Send Information Collection Logs Through Syslog	Enables and configures Syslog notification to send device logs collected by the Call Home service to the specified Syslog server. For details, see 5.3.3.1 Modifying the Syslog Notification Policy.	[Example] Enabled

**Step 5** Confirm and save basic and policy configurations for the Call Home service.

- Click **Save**.

The security alert dialog box is displayed.

2. Confirm information in the dialog box. Select **I have read and understand the consequences associated with performing this operation**, and click **OK**.  
The **Execution Result** dialog box is displayed.
3. Click **OK**.  
The Call Home service is configured successfully.

**Step 6** Apply for authentication.

The technical support center can process the data uploaded by a storage system only after the storage system passes authentication.

 **NOTE**

If the **Call Home Service** is not selected and saved when configure policies, you cannot apply for authentication.

1. Click **Authenticate**.  
The **Authenticate Device** dialog box is displayed.
2. Enter your Support account and password.

 **NOTE**

If you do not have a Huawei support account, contact Huawei technical support center to apply for such an account.

3. Click **OK**.  
The **Execution Result** dialog box is displayed.
4. Click **OK**.  
After device authentication is successful, the authentication status becomes **Authenticated**.
5. (Optional) Click **Call Home Availability Test** to check whether the Call Home service is working properly.

 **NOTE**

After the Call Home service is enabled, device authentication is available. After the device authentication is complete, the Call Home availability test is available.

----End

### 5.5.3 Exporting a Data Package to Be Uploaded

If the Call Home service becomes unavailable, you can manually export data packages to be uploaded to Huawei technical support center.

#### Context

- If the Call Home service becomes unavailable, the eService client saves data uploaded within 24 hours. After the Call Home service recovers, the eService client continues receiving data. Before the Call Home service 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 5-29** Parameters

Parameter	Description	Value
<b>ip=?</b>	IP address of a File Transfer Protocol (FTP) server or a Secure File Transfer Protocol (SFTP) server. <b>NOTE</b> To export log files, an FTP server or an SFTP server must be available and is accessible to the storage system.	-
<b>user=?</b>	Name of a user for logging in to an FTP server or an SFTP server.	The value contains 1 to 64 characters without colons (:).
<b>password=?</b>	Password for logging in to an FTP server or an SFTP server.	The value contains 1 to 64 characters.
<b>path=?</b>	File name and path to an exported log file.	The path must start with <code>/.Path</code> for saving events or logs on the FTP/SFTP server. <ul style="list-style-type: none"><li>● <code>/test/</code> indicates that events or logs are saved in the <b>test</b> folder on the FTP/SFTP server. The file name is automatically generated.</li><li>● <code>/test</code> indicates that events or logs are saved in the <b>test</b> file.</li><li>● If you specify the file name, we recommend you add the file suffix <b>.tgz</b>. If you do not specify the suffix, CLI will add it automatically.</li></ul>
<b>port=?</b>	ID of the employed port on an FTP server or an SFTP server.	The value is an integer between 1 and 65535. <ul style="list-style-type: none"><li>● If protocol is set to <b>FTP</b>, the default value is <b>21</b>.</li><li>● If protocol is set to <b>SFTP</b>, the default value is <b>22</b>.</li></ul>

----End

## Example

Export certain Call Home 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 Call Home data will be stored in the root directory of the FTP server, and the exported Call Home 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 employ optimization configurations to improve system performance.

You can use the OceanStor DeviceManager management software or SystemReporter performance analysis tool to monitor a storage system. You can use DeviceManager by simply logging in to it through a web browser. Compared with DeviceManager, SystemReporter needs to be installed by yourself but provides more comprehensive and detailed performance analysis data. For details, see the *OceanStor V3 Series V300R006 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.

## Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Settings** >  **Basic Information** > **Device Time**.

**Step 3** Configure the storage device time.



### NOTICE

After this operation is executed, if the device time changes, the following impacts may be triggered:

- If the changed device time exceeds the license validity period, the license may be invalid.
- If the changed device time exceeds the certificate validity period, the certificate may expire.
- If the changed device time exceeds the password validity period set by a user, the system may force the user to change the login password.

---

The storage device time can be configured in the following ways:

- Synchronize client time

Select **Synchronize client time**.



If DeviceManager cannot obtain the time zone ID, **Time Zone** is displayed. Set **Time Zone** to the time zone of the place where the client resides.

- Set NTP automatic synchronization



For detailed operations of configuring automatic synchronization of the NTP server time, see section **Configuring the NTP Service** of the *InstallationGuide* of the corresponding product model.

- Manually modify time

- a. Select **Manual**.
- b. Click **Modify**.

The **Modify Time** dialog box is displayed.

- c. Change the storage device time.

- In the **Date** group box, change the device date.
  - In the **Time** group box, change the device time.
  - From the **Current Time Zone** drop-down list, select the time zone of the storage device.
- d. Click **OK**.

 **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.

**Step 4** Confirm the device time setting.

1. Click **Save**.  
The **Warning** dialog box is displayed.
2. Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation**.
3. Click **OK**.  
The **Execution Result** dialog box is displayed indicating that the operation succeeded.
4. Click **Close**.

----End

## 5.7.2 Setting the Device Name and Location

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** Set **Device Name** and **Device Location**.

- Device name must contain 1 to 127 characters and only letters, digits, periods (.), underscores (\_), and hyphens (-). It cannot be blank.
- Device location must contain 1 to 511 characters and cannot be blank.

**Step 4** Confirm the configuration of basic information about storage devices.

1. Click **Save**.  
The **Execution Result** dialog box is displayed indicating that the operation succeeded.
2. Click **Close**.

----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.

## 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** (Applicable to V300R006C00/C10/C20) Choose **Active License** in the navigation tree on the left.

**Step 4** 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.



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.



If licenses are controlled by capacity, their **Expiry Date** is **Permanent**.



As the OceanStor SystemReporter and OceanStor UltraPath are 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** (Applicable to V300R006C00/C10/C20) Choose **Active License** in the navigation tree on the left.

**Step 4** Back up active license files.

1. Click **Back Up**.

The **File Download** dialog box is displayed.



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 5-32](#) and [Figure 5-33](#) illustrate the major processes of space reclamation.

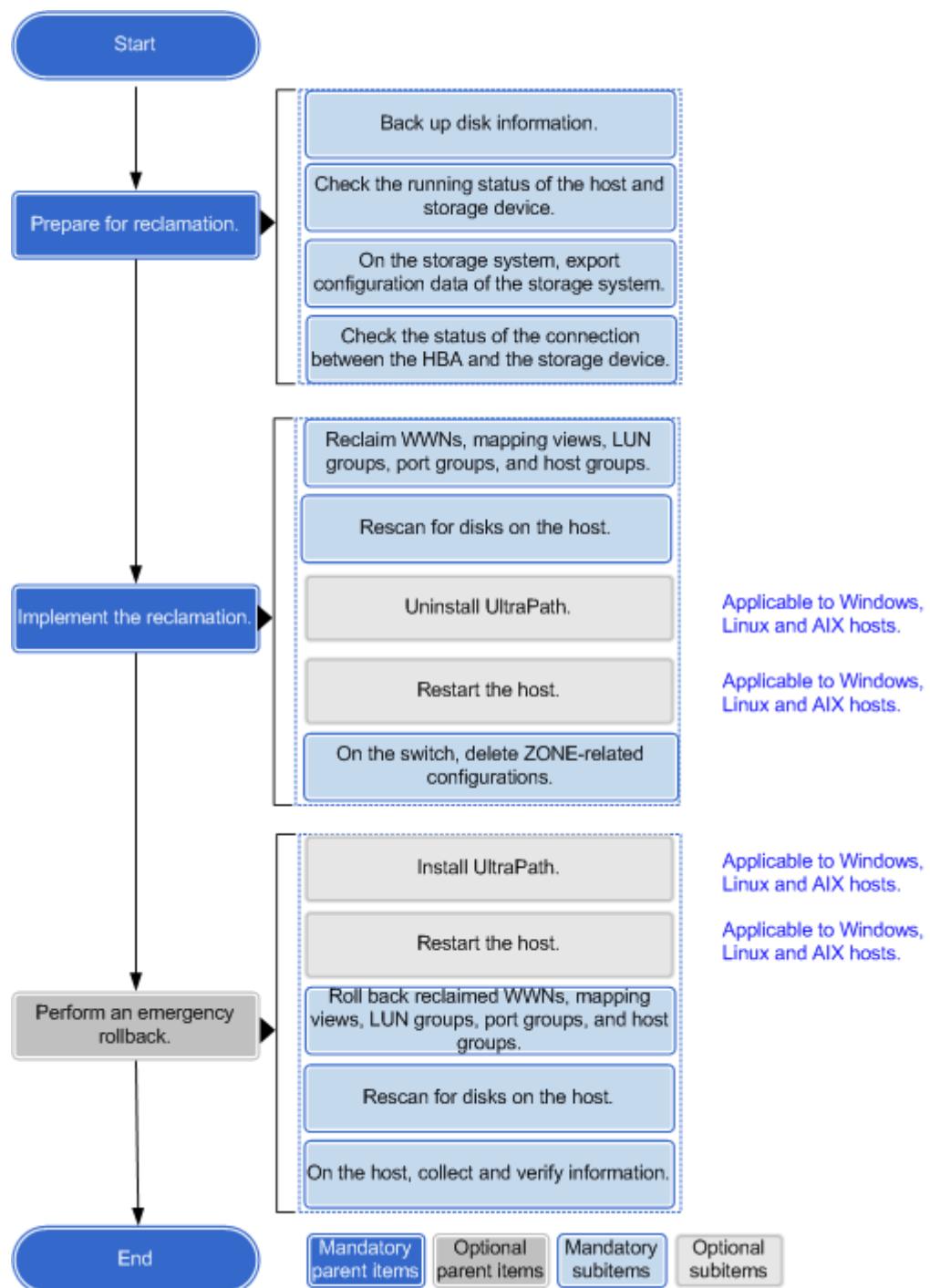


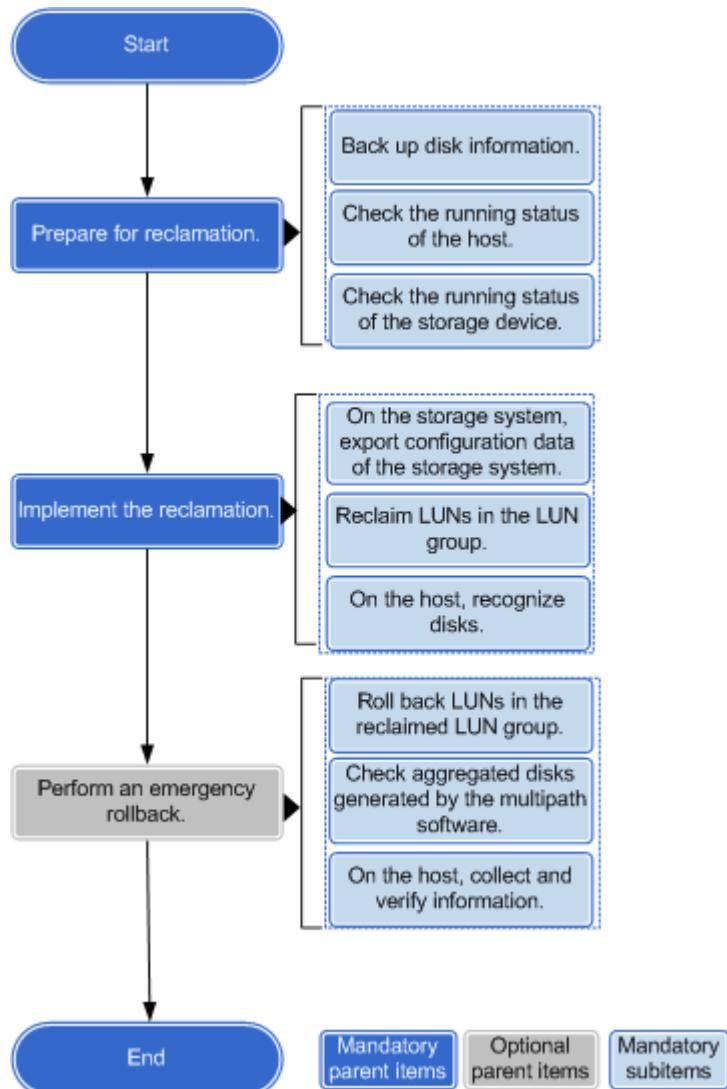
#### NOTICE

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 5-32** Process for full space reclamation



**Figure 5-33** 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 **Degraded** exists, run **upadm set phypathnormal**. Specify the path whose status is **Degraded** 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.



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

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.

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 no, 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
Health Status     Running Status    Type
-----  -----
Normal           Online          Thick
WWN
-----
60022a1100*****
```

**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 no, 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 **Degraded** exists, run **upadmin set phypathnormal**. Specify the path whose status is **Degraded** 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.



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

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
-----
10000000000000*   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
-----
10000000000000*   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-claimed mapping view and the to-be-claimed 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-claimed mapping view and the to-be-claimed 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-claimed mapping view and the to-be-claimed 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-claimed 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-claimed 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
```

Health Status	Running Status	Type
Normal	Online	Thick
WWN		
60022a1100*****		

**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 **Degraded**, run **upadmin set phypathnormal** to set the path to **Normal**. In the command, set **path\_id** to the ID of the **Degraded** 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 **Degraded**, 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.



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

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
-----
10000000000000*   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-claimed mapping view and the to-be-claimed 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-claimed mapping view and the to-be-claimed 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-claimed mapping view and the to-be-claimed 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-claimed 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 **Islpp -L | grep -i UltraPath** to view the version of the installed UltraPath.
2. Run **installpp -u program\_name** to uninstall UltraPath, where **program\_name** is the name of UltraPath shown in [Step 8.1](#).
3. Run **Islpp -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 v lun** 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
Health Status     Running Status   Type
-----  -----
Normal           Online          Thick
WWN
-----
60022a1100*****
```

---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 no longer required, 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 Multipathing Plug-In (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 user name and password are **admin** and **Admin@storage** respectively.

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
-----  -----
10000000000000*   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 7.2** 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-claimed 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
Health Status     Running Status    Type
-----  -----
Normal           Online          Thick
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. [5.9.6 Emergency Rollback of Space Reclamation](#) and [Figure 5-35](#) show the major procedures.

Figure 5-34 Emergency rollback procedure (full reclamation)

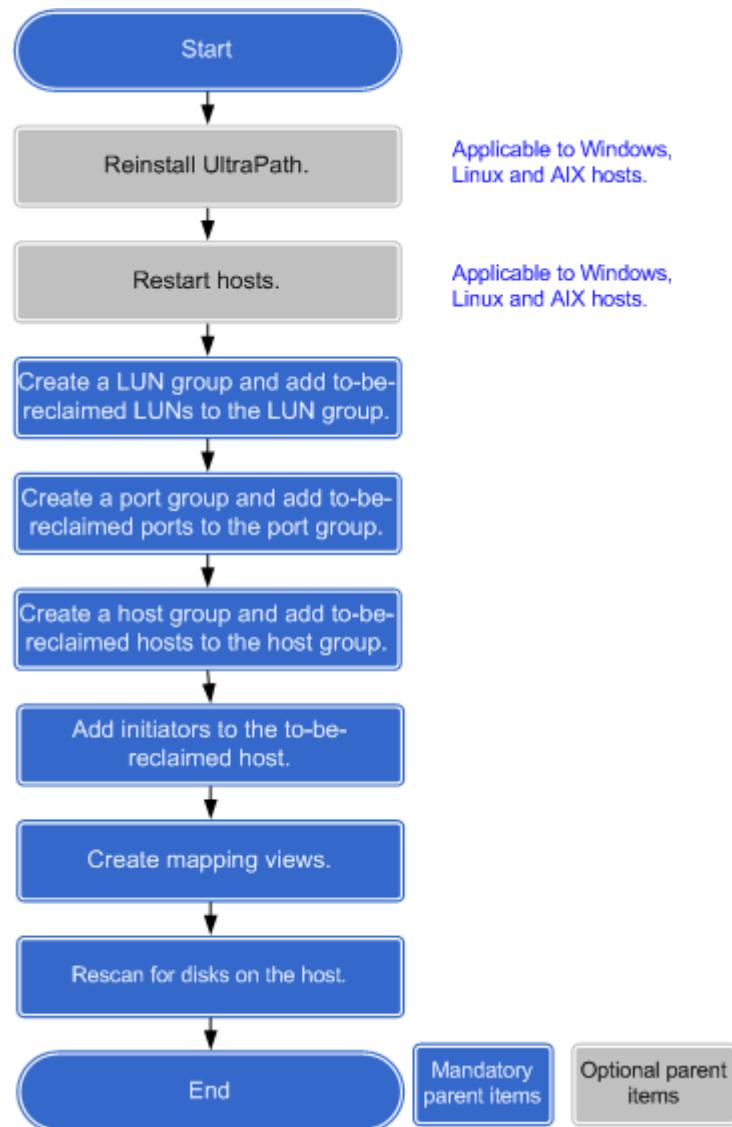
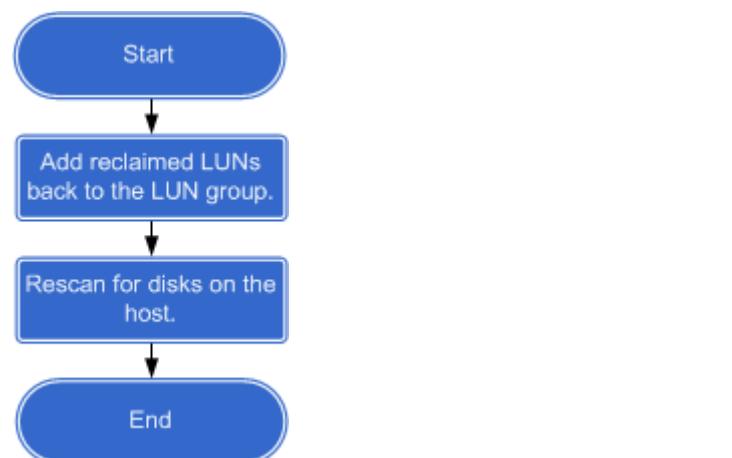


Figure 5-35 Emergency rollback procedure (partial reclamation)



## 5.9.7 Disk Data Destruction

This operation enables you to destroy the data on a disk before discarding the disk data. The destroyed data cannot be recovered, which ensures data security.

### Prerequisites

Data destruction can only be performed for self-encrypting disks that are not added to a disk domain.

### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  System.

**Step 3** Select the disk whose data you want to destroy.

**Step 4** Destroy data of the disk.

1. Click **Disk Data Destruction** in the lower area of the function pane.

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

2. Click **Close**.

----End

## 5.10 Obtaining System Version Information

You can use DeviceManager and the command-line interface (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. In addition, you can also use the CLI to query historical versions of the storage system.

### 5.10.1 Obtaining Current System Version Information

#### Obtaining Current System Version Information Using DeviceManager

You can use DeviceManager to view the current storage system version.

**Step 1** Log in to DeviceManager.

Go to the DeviceManager management page.

**Step 2** In the navigation tree on the right, click  Home.

**Step 3** In **Basic Information**, view **Version**. That is, you can view the current storage system version, as shown in [Figure 5-36](#).

**Figure 5-36** Basic storage system information

The screenshot shows the OceanStor DeviceManager interface. At the top, there is a navigation bar with the Huawei logo and the text "OceanStor DeviceManager". Below it, a breadcrumb navigation shows "STORAGE-DEVICE45 > Home". The main content area is titled "Basic Information". It features a green circular icon with a checkmark and the word "Normal", followed by the text "The device is working well.". Below this, there are several fields: "Device Model" (with a blurred value), "Device Location" (with a blurred value), "Version" (with a blurred value), "Patch Version" (with a blurred value), "SN" (with a blurred value), and "WWN" (with a blurred value). At the bottom, there is a table showing storage details:

Type	Used/Total
SSD(1.799 TB)	25/25

On either side of the table are icons for SSD (25) and NL-SAS (75). A "Show All" link is located at the bottom right of the table.

You can understand the supported software version based on the obtained storage system version and the *Version Mapping* when installing or upgrading UltraPath and SmartKit.

----End

## Obtaining Current System Version Information Using the CLI

You can use the command-line interface (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.

**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 understand the supported software version based on the obtained storage system version and the *Version Mapping* when installing or upgrading UltraPath and SmartKit.

----End

## 5.10.2 Obtaining System Historical Version Information

You can use the command-line interface (CLI) to query and familiarize yourself with 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
-----
XXXXXXXXXXXXXXXXXXXXXX 0A 10.94.80.72  VX00R00XCXX    --           Controller
XXXXXXXXXXXXXXXXXXXXXX 0B 10.94.80.73  VX00R00XCXX    --           Controller
HotPatch Version

SN          Name IP          Current Version History Version Type
-----
XXXXXXXXXXXXXXXXXXXXXX 0A 10.94.80.72  --           --           Controller
XXXXXXXXXXXXXXXXXXXXXX 0B 10.94.80.73  --           --           Controller
```

**History Version** indicates historical version information about the storage system, including historical version information about the software and hot patches.

----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 5-30** lists the protocol interfaces or plug-ins that can be used for a third-party NMS to interconnect with Huawei storage devices.

**Table 5-30** 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.	<i>eSDK Storage SMI-S Provider Quick Start Guide</i>
SNMP	The SNMP protocol is used for a third-party NMS to view information about storage devices, including LUNs, ports, and storage pools.	-
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.	<i>eSDK Storage Quick Guide (vCenter, Plug-in)</i>
System Center	OceanStor System Center Operations Manager Plug-in (SCOM plug-in for short) is a Huawei-developed plug-in for Microsoft SCOM and is used to monitor Huawei storage devices.	<i>eSDK Storage Quick Guide (SCOM, Plug-in)</i>
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.	the <i>REST Interface Reference</i> of the corresponding product model.

 **NOTE**

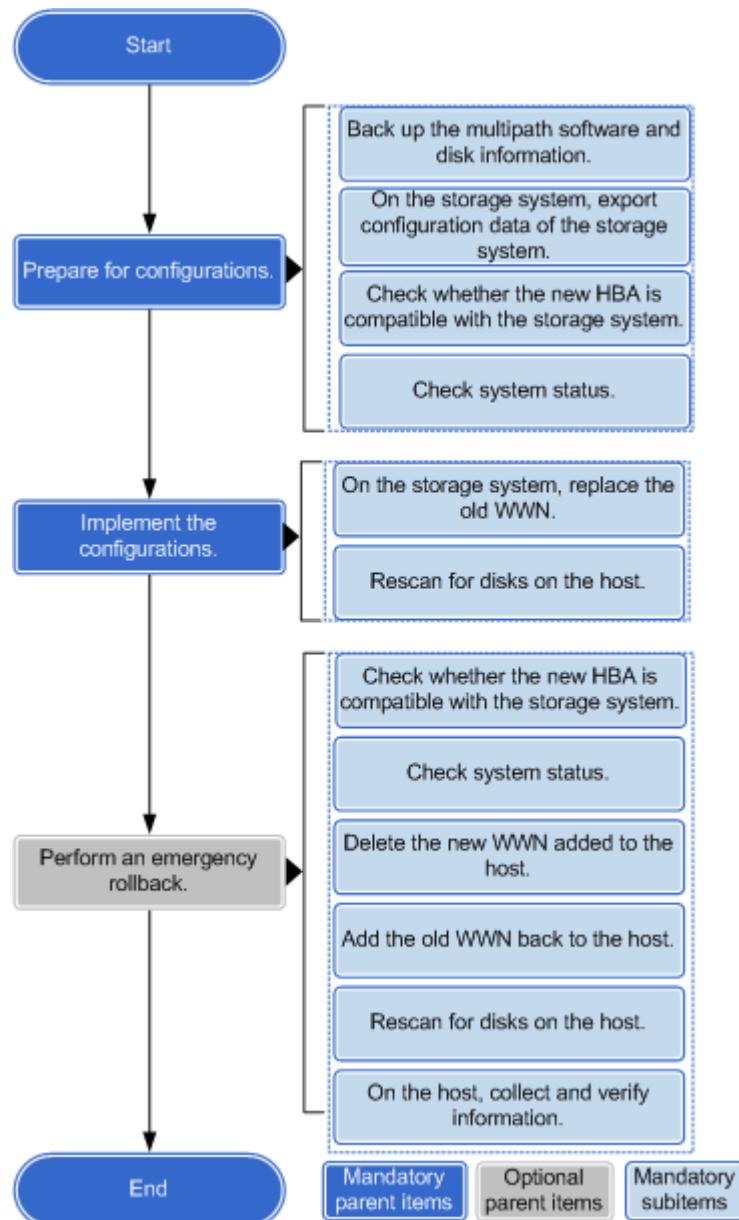
Log in to <http://enterprise.huawei.com>. Search for and download the required document of the latest version.

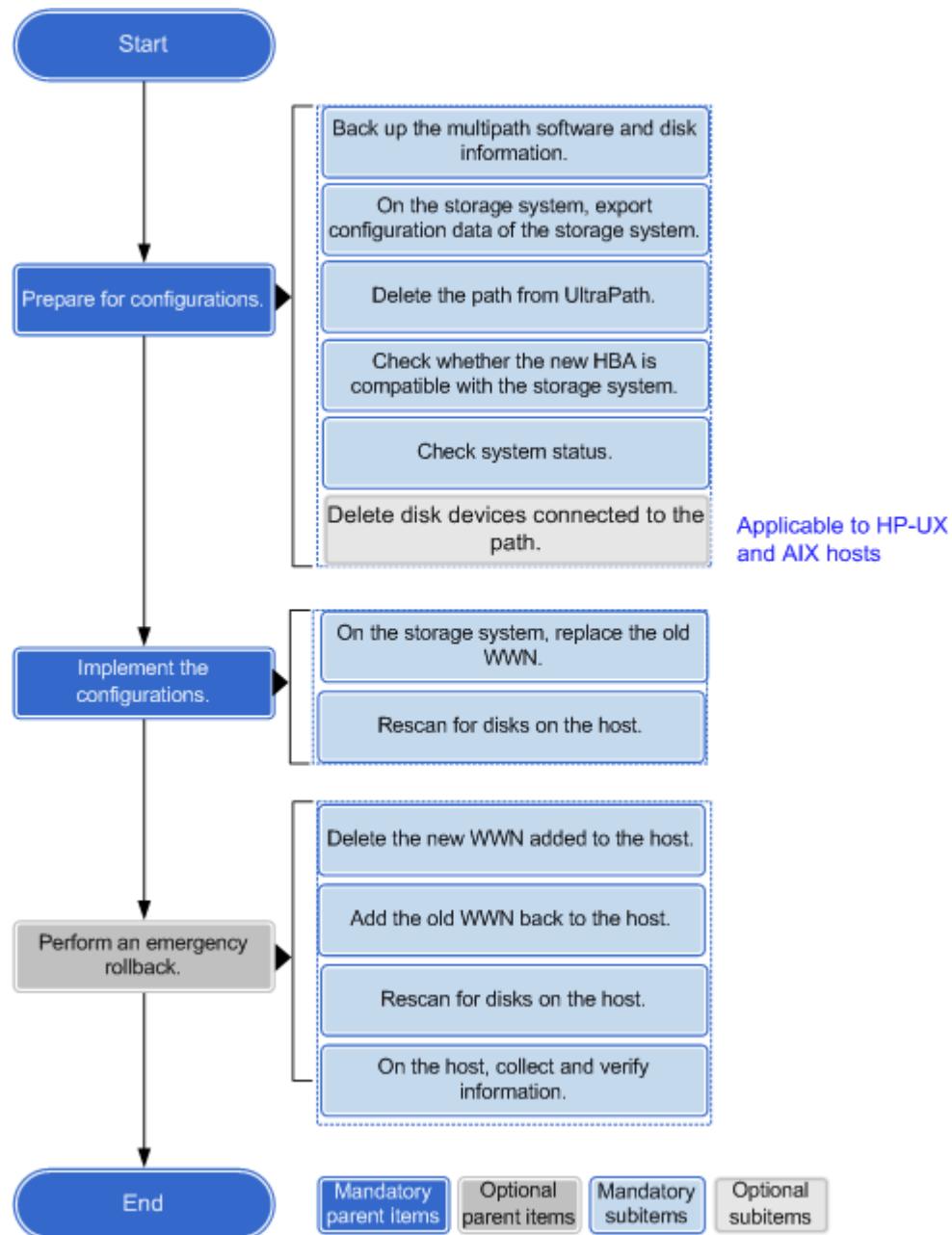
## 5.12 Connection Change Between the Storage System and an Application Server

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 replacement either online or offline. The main configuration procedures after an HBA replacement are shown in [Figure 5-37](#) and [Figure 5-38](#).

**Figure 5-37** Configuration procedure after an HBA offline replacement



**Figure 5-38** Configuration procedure after an HBA online replacement

## 5.12.1 Configurations and Operations After an HBA Replacement (in Windows)

This section describes how to configure the HBA on the storage system and the host to make it work correctly after replacing the HBA of a Windows host.

### 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:
    1. Press **Windows+R** to open the **Run** dialog box.
    2. Type **cmd** and press **Enter**.
    3. 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:
    4. Press **Windows+R** to open the **Run** dialog box.
    5. Type **devmgmt.msc** and press **Enter** to open the **Device Manager** page.
    6. Select **Storage controllers** and double-click **Fibre Chanel 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.



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

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:
  1. 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**.
  2. 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.

3. 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 **Windows+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 Chanel 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 **Degraded**, 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.

ID	WWN	Multipath Type	Running Status	Free	Alias	Host
--	100000000000*	Default	Online	Yes	--	

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 no, 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 v lun** 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.



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

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 v lun** 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 see 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 see 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 see 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.

ID	WWN	Multipath Type	Running Status	Free	Alias	Host
--	100000000000*	Default	Online	Yes	--	

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 **Degraded**, 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.



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

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 *fcdY* represents the new HBA.
2. Run **fctstat 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 **fctstat** command.

**Step 7** Check the system status and see whether there are disks or tapes connected to the HBA.

1. Run **erprt** 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** to 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 see 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 ID	Multipath Type	Running Status	Free	Alias	Host
--	100000000000*	Online	Yes	--	

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.



If the system reports a failure in querying the WWN of a new HBA, run the **cfgmgr** 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 -vI 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 **Degraded**, 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 user name and password are **admin** and **Admin@storage** respectively.

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 **femsutil /dev/fcdY** to check whether the WWN of the new HBA is as planned, where *fcdY* represents the new HBA.
2. Run **femsutil /dev/fcdY vpd** to check whether the HBA is compatible with the storage system.

**Step 7** Check the system status and see 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 see 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.

ID	WWN	Multipath Type	Running Status	Free	Alias	Host
--	100000000000*	Default	Online	Yes	--	

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 the **create initiator fc wwn=?** command to create an FC initiator. **wwn** is the WWN of the new HBA.
4. Run **add host initiator host\_id=? initiator\_type=FC wwn=?** command 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** command. 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** commands to show the disks and volume groups (VGs) on the host.
2. Run **ioscan -fNC disk** command to scan for disks.
3. Rerun **ioscan -fnkC disk** command 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** command and confirm that the LUN device files are generated.
5. Rerun **ioscan -fnkC disk** command 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** command and confirm that the NMP is enabled.

- b. Run **ioscan -funC disk** command to view the number of disk paths when NMP is not enabled.
- c. Rerun **ioscan -funNC disk** command and confirm that the number of newly generated aggregated disks is the same as planned.
- d. Run **ioscan -m dsf** command to view the mappings between persistent disks and legacy disks.
- e. Run **scsimgr lun\_map -D /dev/rdisk/diskX** command to view disk path information with NMP enabled, where **diskX** represents a disk on the host.

**Step 3** Run **sar -L 1 30** command 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.

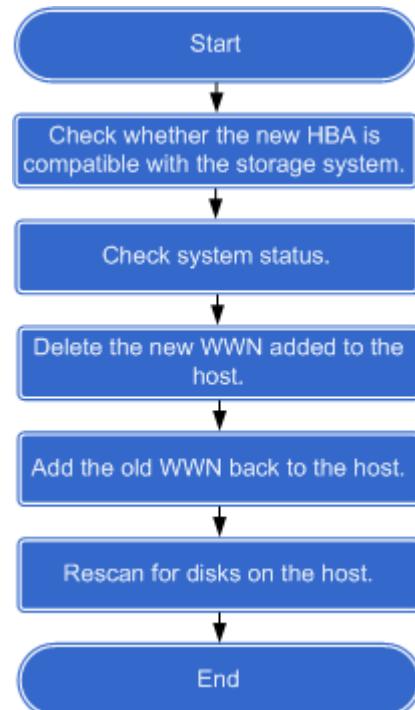
----End

## 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 [5.12.5 Emergency Rollback of Configurations and Operations After Replacing an HBA](#) and [Figure 5-40](#).

**Figure 5-39** Emergency rollback procedure after an offline HBA replacement



**Figure 5-40** Emergency rollback procedure after an online HBA replacement

## 5.13 Managing VMs (OceanStor 18000 Series)

This chapter describes basic operations related to VMs deployed on SVP, including closing and restarting a VM as well as querying VM status.

### 5.13.1 Querying VM Status

This section explains how to query the status of running virtual machines (VMs).

#### Prerequisites

**Xshell 5** has been installed on the maintenance terminal.

#### Procedure

**Step 1** Log in to the host running the service processor (SVP).

1. Start the **Xshell 5** software on the maintenance terminal.  
The **Xshell 5 (Free for Home/School)** window is displayed.
2. Choose **File > New**.  
The **New Session Properties** window is displayed.
3. Set **Protocol** and **Port Number** to **SSH** and **20** respectively. Set **Host** to the IP address of the SVP management port. Click **OK**.
4. In the **Sessions** dialog box that is displayed, click the newly created session and click **Connect**.
5. On the **SSH User Name** page that is displayed, enter the user name (**svp\_user** by default) for logging in to the host and click **OK**.
6. In the **SSH User Authentication** dialog box, select **Keyboard Interactive** and click **OK**.
7. In the **SSH User Authentication - Keyboard Interactive** dialog box that is displayed, enter the password. The default password is **Aguser@12#\$**. Click **OK**.

 **NOTE**

Upon first login, the system will prompt you to change the default password. Enter the new password in subsequent logins.

You have successfully logged in to the host running the SVP.

**Step 2** Run **su root** to switch to the **root** account.

**Step 3** Enter the password as prompted (**Admin@12#\$** by default) and press **Enter**.

**Step 4** Run **virsh list --all** to view VM status.

```
# virsh list --all
Id   Name           State
-----
27   Linux          running
28   Windows        shut off
```

----End

## 5.13.2 Restarting a VM

This section describes how to restart a virtual machine (VM) deployed on a service processor (SVP).

### Prerequisites

- **Xshell 5** has been installed on the maintenance terminal.
- The status of the VM to be restarted is **running**.

### Procedure

**Step 1** Log in to the host running the service processor (SVP).

1. Start the **Xshell 5** software on the maintenance terminal.  
The **Xshell 5 (Free for Home/School)** window is displayed.
2. Choose **File > New**.  
The **New Session Properties** window is displayed.
3. Set **Protocol** and **Port Number** to **SSH** and **20** respectively. Set **Host** to the IP address of the SVP management port. Click **OK**.
4. In the **Sessions** dialog box that is displayed, click the newly created session and click **Connect**.
5. On the **SSH User Name** page that is displayed, enter the user name (**svp\_user** by default) for logging in to the host and click **OK**.
6. In the **SSH User Authentication** dialog box, select **Keyboard Interactive** and click **OK**.
7. In the **SSH User Authentication - Keyboard Interactive** dialog box that is displayed, enter the password. The default password is **Aguser@12#\$**. Click **OK**.

 **NOTE**

Upon first login, the system will prompt you to change the default password. Enter the new password in subsequent logins.

You have successfully logged in to the host running the SVP.

**Step 2** Run **su root** to switch to the **root** account.

**Step 3** Enter the password as prompted (**Admin@12#\$** by default) and press **Enter**.

**Step 4** Run **virsh reboot Linux** or **virsh shutdown Windows** to restart the Linux or Windows VM.

----End

### 5.13.3 Closing a VM

This section describes how to close a virtual machine (VM) deployed on a service processor (SVP).

#### Prerequisites

- **Xshell 5** has been installed on the maintenance terminal.
- The status of the VM to be closed is **running**.

#### Procedure

**Step 1** Log in to the host running the service processor (SVP).

1. Start the **Xshell 5** software on the maintenance terminal.

The **Xshell 5 (Free for Home/School)** window is displayed.

2. Choose **File > New**.

The **New Session Properties** window is displayed.

3. Set **Protocol** and **Port Number** to **SSH** and **20** respectively. Set **Host** to the IP address of the SVP management port. Click **OK**.

4. In the **Sessions** dialog box that is displayed, click the newly created session and click **Connect**.

5. On the **SSH User Name** page that is displayed, enter the user name (**svp\_user** by default) for logging in to the host and click **OK**.

6. In the **SSH User Authentication** dialog box, select **Keyboard Interactive** and click **OK**.

7. In the **SSH User Authentication - Keyboard Interactive** dialog box that is displayed, enter the password. The default password is **Aguser@12#\$**. Click **OK**.

#### NOTE

Upon first login, the system will prompt you to change the default password. Enter the new password in subsequent logins.

You have successfully logged in to the host running the SVP.

**Step 2** Run **su root** to switch to the **root** account.

**Step 3** Enter the password as prompted (**Admin@12#\$** by default) and press **Enter**.

**Step 4** Run **virsh shutdown Linux** or **virsh shutdown Windows** to close the Linux or Windows VM.

----End

## 5.13.4 Forcibly Closing a VM

This section describes how to forcibly close a virtual machine (VM) deployed on a service processor (SVP) when the VM becomes abnormal and cannot be closed.

### Prerequisites

- **Xshell 5** has been installed on the maintenance terminal.
- A VM is abnormal and cannot be closed in a normal way.

### Procedure

**Step 1** Log in to the host running the service processor (SVP).

1. Start the **Xshell 5** software on the maintenance terminal.  
The **Xshell 5 (Free for Home/School)** window is displayed.
2. Choose **File > New**.  
The **New Session Properties** window is displayed.
3. Set **Protocol** and **Port Number** to **SSH** and **20** respectively. Set **Host** to the IP address of the SVP management port. Click **OK**.
4. In the **Sessions** dialog box that is displayed, click the newly created session and click **Connect**.
5. On the **SSH User Name** page that is displayed, enter the user name (**svp\_user** by default) for logging in to the host and click **OK**.
6. In the **SSH User Authentication** dialog box, select **Keyboard Interactive** and click **OK**.
7. In the **SSH User Authentication - Keyboard Interactive** dialog box that is displayed, enter the password. The default password is **Aguser@12#\$. Click OK.**

#### NOTE

Upon first login, the system will prompt you to change the default password. Enter the new password in subsequent logins.

You have successfully logged in to the host running the SVP.

**Step 2** Run **su root** to switch to the **root** account.

**Step 3** Enter the password as prompted (**Admin@12#\$** by default) and press **Enter**.

**Step 4** Run **virsh destroy Linux** or **virsh destroy Windows** to forcibly close the VM.

----End

## 5.13.5 Redefining a VM

After you modify the configuration file of a VM, you need to restart and then redefine the VM.

### Prerequisites

- **Xshell 5** has been installed on the maintenance terminal.
- You have manually modified the configuration file of the VM.

- You have shut down the VM and the VM status is **shut off**.

## Procedure

- Step 1** Log in to the host running the service processor (SVP).
1. Start the **Xshell 5** software on the maintenance terminal.  
The **Xshell 5 (Free for Home/School)** window is displayed.
  2. Choose **File > New**.  
The **New Session Properties** window is displayed.
  3. Set **Protocol** and **Port Number** to **SSH** and **20** respectively. Set **Host** to the IP address of the SVP management port. Click **OK**.
  4. In the **Sessions** dialog box that is displayed, click the newly created session and click **Connect**.
  5. On the **SSH User Name** page that is displayed, enter the user name (**svp\_user** by default) for logging in to the host and click **OK**.
  6. In the **SSH User Authentication** dialog box, select **Keyboard Interactive** and click **OK**.
  7. In the **SSH User Authentication - Keyboard Interactive** dialog box that is displayed, enter the password. The default password is **Aguser@12#\$. Click OK.**

 **NOTE**

Upon first login, the system will prompt you to change the default password. Enter the new password in subsequent logins.

You have successfully logged in to the host running the SVP.

- Step 2** Run **su root** to switch to the **root** account.

- Step 3** Enter the password as prompted (**Admin@12#\$** by default) and press **Enter**.

- Step 4** Run **virsh undefine Linux** or **virsh undefine Windows** to remove the original definition of the VM.

- Step 5** Run **virsh create /img/linux.xml** or **virsh create /img/windows.xml** to enable the modified configuration file.

----End

## 5.13.6 Starting a VM

This section describes how to start a virtual machine (VM) deployed on a service processor (SVP).

### Prerequisites

- **Xshell 5** has been installed on the maintenance terminal.
- The status of the VM is **shut off**.

## Procedure

- Step 1** Log in to the host running the service processor (SVP).

1. Start the **Xshell 5** software on the maintenance terminal.  
The **Xshell 5 (Free for Home/School)** window is displayed.
2. Choose **File > New**.  
The **New Session Properties** window is displayed.
3. Set **Protocol** and **Port Number** to **SSH** and **20** respectively. Set **Host** to the IP address of the SVP management port. Click **OK**.
4. In the **Sessions** dialog box that is displayed, click the newly created session and click **Connect**.
5. On the **SSH User Name** page that is displayed, enter the user name (**svp\_user** by default) for logging in to the host and click **OK**.
6. In the **SSH User Authentication** dialog box, select **Keyboard Interactive** and click **OK**.
7. In the **SSH User Authentication - Keyboard Interactive** dialog box that is displayed, enter the password. The default password is **Aguser@12#\$. Click OK.**

 **NOTE**

Upon first login, the system will prompt you to change the default password. Enter the new password in subsequent logins.

You have successfully logged in to the host running the SVP.

**Step 2** Run **su root** to switch to the **root** account.

**Step 3** Enter the password as prompted (**Admin@12#\$** by default) and press **Enter**.

**Step 4** Run **virsh start Linux** or **virsh start Windows** to start the VM.

----End

### 5.13.7 Logging In to the Linux VM of the SVP Using VNC

If management software in the SVP works incorrectly, you can log in to the Linux VM of the SVP using VNC for maintenance. This section describes how to log in to the Linux VM.

#### Prerequisites

The KVM has been configured for the storage system.

#### Procedure

**Step 1** Start the KVM.

**Step 2** Log in to the SVP host as user **svp\_user**. The default password is **Aguser@12#\$**.

**Step 3** On the host desktop, choose **Applications > System > Terminal > Xterm**.

**Step 4** In the command window that is displayed, run **vncviewer 127.0.0.1:0**.

The login page of the Linux operating system built in the SVP is displayed.

**Step 5** Log in to the Linux VM as user **root**. The default password is **VM12@storage**.

----End

## Follow-up Procedure

After logging in to the Linux VM using VNC, you need only to operate the VM as a Linux operating system. You can manually collect system or software logs and restart malfunctioning processes or replace faulty applications to rectify faults in a timely manner.

## 5.14 Expanding Storage Space

After adding storage components, you need to perform necessary configurations on the storage system and application server to allocate the added storage space to system services.

If you want to expand the capacity of storage components, contact the technical support center.

To obtain contact details about Huawei technical support center:

- For carrier users, visit <http://support.huawei.com/carrier/docview!docview?nid=IN000034614&path=NN-000005#click=myApply>.
- For enterprise users, visit <http://e.huawei.com/en/service-hotline>.

You can expand the storage capacity for block services. For block services, you can expand the capacity using the following methods:

- Increasing the LUN capacity  
Increase the capacity of a LUN for the server, which includes complex operations.
- Adding LUNs  
Add LUNs to the server, which is applicable to scenarios using LVM/volume management in AIX, SUSE, or Windows operating systems. This method involves simple operations and minor impacts on host applications.

### 5.14.1 Performing the Pre-expansion Evaluation

Before expanding a disk domain, use SmartKit for evaluation.

#### Procedure

**Step 1** Open SmartKit.

**Step 2** Add a storage device to SmartKit.

1. In the SmartKit main window, click the **Devices** tab and select **Add**.
2. In **Basic Information**, select **Specify IP Address (add a device by the IP address)** and enter the management IP address of the storage system. 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 SmartKit main window, choose **Home > Expansion > Expansion Evaluation**.

The **Expansion Evaluation** page is displayed.

**Step 4** Select devices.

1. Click **Select Devices**. The **Select Devices** dialog box is displayed.
2. Select the storage system to be expanded and the save path for 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 backup can be used to restore the storage system in the event of an expansion failure.

**Step 5** Evaluate the capacity expansion solution.

1. Click **Expansion Evaluation**.

The **Expansion evaluation Wizard** dialog box is displayed.

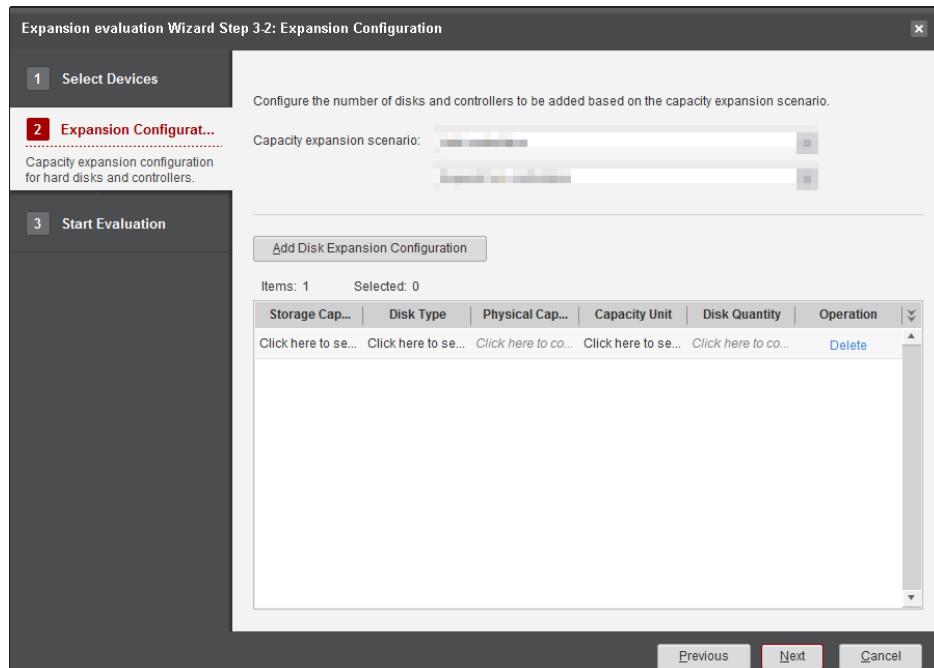
2. Select the storage system to be expanded and click **Next**.

The **Expansion Configuration** page is displayed.

3. Select **Add disks, disk enclosures, and disk cabinets** in **Capacity expansion scenario**.
4. Click **Add Disk Expansion Configuration**.

 **NOTE**

You can add multiple configuration policies.



5. Specify the configuration parameters according to the capacity expansion plan. **Table 5-31** lists the parameters.

**Table 5-31** Capacity evaluation parameters

Parameter	Description
Storage Capacity Expansion Mode	Method to add storage space.

Parameter	Description
Disk Type	Type of the new disks. <b>NOTE</b> <ul style="list-style-type: none"><li>– Self-encryption drives (SEDs) are supported.</li><li>– To add multiple disk types, click <b>Add Disk Expansion Configuration</b> to add new configuration policies.</li></ul>
Physical Capacity of a Single Disk	Capacity of the new disks. <b>NOTE</b> To add disks of different capacity specifications, click <b>Add Disk Expansion Configuration</b> to add new configuration policies.
Capacity Unit	Capacity unit of the new disks.
Disk Quantity	Number of new disks.
Operation	You can click <b>Delete</b> to delete the current configuration policy.

6. Click **Next**.

The **Start Evaluation** page is displayed and the system starts evaluating the capacity expansion solution.



**NOTE**

- After the evaluation is complete, click **Open the report** to go to the save path of the evaluation report. The report is a .zip file named by the evaluation time.
- You can also click **View the report** to open the report directly.

7. Click **Finish**.



**NOTICE**

Rectify the failed items (if any) according to the suggestions and evaluate the solution again. If the items fail again, contact Huawei technical support engineers for assistance. Otherwise, risks may arise during capacity expansion.

----End

## 5.14.2 Expanding LUN Capacity

If LUN space where service data resides is insufficient, you can increase LUN capacity to meet your service requirements.

The following operations must be performed in sequence to expand the LUN:

1. Expand the existing LUN in the storage system. Huawei provides technical support for this operation.
2. Adjust the partition table, volume management, database, and application on the host. The customer takes responsibility for this operation. This document provides related expansion operations, which are used for reference.



## WARNING

Some third-party software, which is not deployed by Huawei, is used on the host during the capacity expansion. Huawei does not receive any information about the software and thereby cannot help the customer to assess potential risks. Based on 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.

The known potential risks in expanding LUN capacity include but are not limited to:

- It is risky to expand LUN capacity on the host (that is, expand the volume and file system capacity of the host), and the risks are existed for all storage vendors, not just for Huawei.
- Each operating system, file system, or volume management software has a specific limit for 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

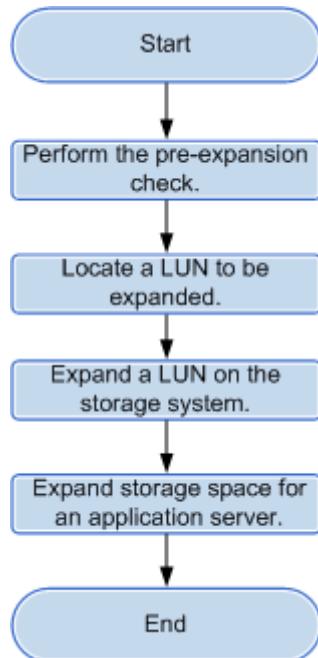
For details about the maximum LUN capacity supported by each operating system, refer to the official documents of the operating system.

- For the partition table, it is highly risky to expand LUN capacity, which may damage the partition table or result in data loss.
- For the volume management software, LUN capacity expansion may cause the disk space to exceed the capacity limit of the volume management software, resulting in an expansion failure.
- For the database, LUN capacity expansion may disorder metadata, leading to data inconsistency or loss.
- For application software, the impact of LUN capacity expansion cannot be determined due to its various types and complex scenarios.

### 5.14.2.1 Understanding the Expansion Process

Before the expansion, read the following expansion procedure. Before the expansion, be familiar with the expansion procedure.

[Figure 5-41](#) shows the storage space expansion procedure.

**Figure 5-41** Capacity expansion process

**Table 5-32** describes each step of expanding storage space.

**Table 5-32** Steps for expanding storage space

Procedure	Description
Perform the pre-expansion check.	Before expanding the storage space, 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 a LUN to be expanded.	Before expanding a LUN for storage services, confirm information about the LUN where current service data resides to ensure successful LUN expansion.
Expand a LUN on the storage system.	Expand the LUN online to provide the required storage capacity.
Expand storage space for an application.	After the expansion, scan for disks on the application server to detect and use the expanded LUN.

### 5.14.2.2 Performing the Pre-expansion Check

Storage space can be expanded without service interruptions. Before the expansion, check the storage system environment and service environment to ensure a smooth expansion.

## Prerequisites

- You can log in to DeviceManager management interface as the super administrator. Only a super administrator has expansion permission.
- The storage system is running correctly.
- You have obtained and recorded the WWPN or IQN of the application server that uses the LUN and the WWN or LUN ID of the LUN. The LUN is correctly mapped to the application server and the host on the storage system.

## Procedure

**Step 1** Log in to DeviceManager as the super administrator. Make sure that the storage environment meets the expansion requirement.

1. In the **Basic Information** area of the **Home** page, check **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 engineers to locate and troubleshoot the problem. 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 disk domain, storage pool, or LUN to be expanded, follow instructions in the **Suggestion** to handle the alarms. These alarms include **Storage Pool Is Degraded**, **Disk Domain Is Faulty**, 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, click  **Provisioning**.  
The **Provisioning** page is displayed.
2. Click **Host**.  
The **Host** page is displayed.
3. Based on the WWPN or IQN of the application server you have recorded, find the host corresponding to the application server.
4. Select the host and check whether its state is normal.  
If an alarm is found, handle it in time based on the alarm information and handling suggestion.
5. In the **Mapped LUN** area of **Details**, find the LUN to be expanded based on the LUN WWN or host LUN ID you have recorded. Record the LUN's capacity and owning storage pool.

 **NOTE**

If the LUN WWN or host LUN ID is not displayed in the **Mapped LUN** area, click  and choose **WWN** or **Host LUN ID** from the drop-down list. The LUN WWN or host LUN ID is displayed.

----End

### 5.14.2.3 Locating a LUN to Be Expanded

Before expanding a LUN for storage services, confirm information about the LUN where current service data resides to ensure successful LUN expansion.

#### Prerequisites

- If a Fibre Channel network is used, ensure that the world wide name (WWN) of a Fibre Channel initiator has been obtained.
- If an Internet Small Computer Systems Interface (iSCSI) network is used, ensure that the iSCSI qualified name (IQN) of an iSCSI initiator has been obtained.
- The UltraPath software has been installed on the host.

#### Context

For an HP-UX operating system, run **scsimgr -p get\_attr all\_lun -a device\_file -a wwid** to view the WWN of a disk 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 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.

Parameter	Description	Value
<b>initiator_type=?</b>	Type of an initiator.	Possible values are: - <b>iSCSI</b> : iSCSI initiator. - <b>FC</b> : Fibre Channel initiator.
<b>wwn=?</b>	WWN of a Fibre Channel initiator. This parameter is available only when <b>initiator_type=?</b> is <b>FC</b> .	To obtain the value, run the <b>show initiator</b> command without parameters.
<b>iscsi_iqn_name=?</b>	IQN of an iSCSI initiator. This parameter is available only when <b>initiator_type=?</b> is <b>iSCSI</b> .	To obtain the value, run the <b>show initiator</b> command without parameters.

```
admin:/>show initiator initiator_type=FC wwn=100000109b1c80ba

      WWN          : 100000109b1c80ba
      Running Status : Online
      Free           : No
      Alias          : --
      Host ID        : 0
      Multipath Type : Default
      Failover Mode  : --
```

```
Path Type      : --
Special Mode Type : --
```

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	Host LUN ID
74	LUN0750000	1
75	LUN0750001	2
76	LUN0750002	3

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, view the WWN of the LUN.

1. Log in to the CLI of UltraPath on the host.
2. On the host where UltraPath is installed, run **show vLUN** to view the WWN of a disk on the host.

 **NOTE**

For details about how to use the **show vLUN** command, see the UltraPath *User Guide* prepared for specific operating systems.

**Step 3** Check whether the two WWNs are the same. If they are the same, you can determine that the LUN is the one to be expanded.

 **NOTE**

For details about the preceding commands, see the *Command Reference*.

----End

#### 5.14.2.4 Expanding a LUN on the Storage System

A user granted the super administrator permission can use the OceanStor DeviceManager to expand LUN capacity and make expanded LUNs available to application servers.

#### Prerequisites

- The storage system is working properly.
- The capacity that you want to add to LUNs has been determined.
- For V300R006C00/C10 storage systems, a LUN for which Snapshot, Clone, LUN Copy, HyperMirror, or SmartMigration is configured cannot be expanded.
- For V300R006C20 and later version storage systems, a LUN for which Snapshot, Clone, LUN Copy, HyperMirror, or SmartMigration is configured cannot be expanded.
- For V300R006C00/C10 storage systems, a LUN for which Snapshot or SmartMigration is configured cannot be expanded. To perform LUN capacity expansion in the Remote Replication feature or HyperMetro feature, see [6.5 How Can I Expand the Capacity of a LUN Used in a Remote Replication Pair? \(Applicable to V300R006C00/C10\)](#) and [6.3 How Can I Expand the Capacity of a LUN Used in the HyperMetro Feature? \(Applicable to V300R006C00/C10\)](#).

- For V300R006C20 and later version storage systems, a LUN for which SmartMigration is configured cannot be expanded. To perform LUN capacity expansion in the Remote Replication feature or HyperMetro feature, see [6.6 How Can I Expand the Capacity of a LUN Used in a Remote Replication Pair? \(Applicable to V300R006C20 and Later\)](#) and [6.4 How Can I Expand the Capacity of a LUN Used in the HyperMetro Feature? \(Applicable to V300R006C20 and Later\)](#).

## Procedure

**Step 1** Check that the storage pool housing the LUN to be expanded has sufficient free space.

1. In the navigation tree on the right, click  **Provisioning**.  
The **Provisioning** page is displayed.
2. Click **Storage Pool**. Check the total capacity, allocated capacity, and free capacity of the storage pool that houses the LUN to be expanded.
  - If the free capacity is sufficient, go to [Step 5](#).
  - If the free capacity is insufficient, record the disk domain of the storage pool and go to [Step 2](#).

**Step 2** Return to the **Provisioning** page and click **Disk Domain**. Check the total capacity, allocated capacity, and free capacity of the disk domain.

- If the free capacity meets expansion requirements, go to [Step 4](#).
- If the free capacity does not meet expansion requirements, go to [Step 3](#).

**Step 3** Expand a disk domain.



### NOTICE

For the capacity tier (NL-SAS), performance tier (SAS), and high-performance tier (SSD), if you want to expand disks in any two tiers or three tiers, you can only expand them tier by tier.

---

1. In the **Disk Domain** area, select a disk domain that you want to expand and click **Expand**.
2. Select the type and number of disks that you want to expand, and enable the free space of the disk domain to meet LUN expansion requirements.
  - All available disks  
All available disks of the storage system are included.
  - Specifying a disk type  
Type and number of disks must be specified.
  - Manually selecting disks  
Optional disks must be manually selected and added.

 **NOTE**

You are advised to set the capacity of the new disks to the same as that of disks in the storage tier to be expanded. If the capacity of the new disks is greater than that of disks in the storage tier to be expanded, you are advised to create a new disk domain for the new disks. Otherwise, the capacity of the new disks is wasted and cannot be used efficiently or may become a performance bottleneck.

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

- If  $D \leq 100$ , configure all disks of this tier in one disk domain.
- If  $100 < D \leq 200$ , configure all disks of this tier in two disk domains.
- If  $D > 200$ , configure 100 disks of this tier for each of the first  $N-1$  disk domains, and then configure the rest  $100 + M$  disks in two disk domains.

3. Click **OK**.

The **Success** dialog box is displayed.

4. Click **OK**.

**Step 4** Expand a storage pool.

1. In the **Storage Pool** area, select the storage pool that you want to expand and click **Modify Capacity**.
2. In the page of modifying capacity, choose **Expand capacity** and in the **Added Capacity** area, enter the value of the capacity that you want to expand and select the unit.
3. Click **OK**. The **Warning** dialog box is displayed. Select **I have read and understand the consequences associated with performing this operation** and click **OK**.

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

4. Click **Close**.

**Step 5** Expand a LUN.

1. In the **LUN** area, select the LUN that you want to expand and click **Expand**.
2. In the **Added Capacity** area, enter the value of the capacity that you want to expand and select the unit.
3. Click **OK**. The **Info** dialog box is displayed. Click **OK**.

**Step 6** Verify and use the capacity added to the LUN.

1. Under **Block Storage Service** on the **Provisioning** page, click **LUN**.

The **LUN** page is displayed.

2. Select the expanded LUN and check **Capacity**.

If the displayed capacity is consistent with the actual capacity, the LUN is correctly expanded. If the LUN is incorrectly expanded, troubleshoot faults based on alarm information.

3. After expanding the LUN, log in to the application server as a system administrator and scan for disks. The expanded LUN is available to the application server after being detected.

**----End**

## 5.14.2.5 Expanding Storage Space for an Application Server

A LUN must be expanded when its capacity is insufficient to meet service requirements. An application server can use an expanded LUN only after required configurations are performed on the application server.

### 5.14.2.5.1 Expanding a LUN on an Application Server in Windows

After expanding a LUN on its storage system, perform the expansion configuration on the corresponding application server for it to identify and use the expanded storage space. This task uses an application server running Windows Server 2008 as an example to describe how to expand a LUN on an application server. For application servers running other versions of Windows operating systems, adjust the operations based on actual conditions.

#### Prerequisites

A LUN has been expanded on the storage system.

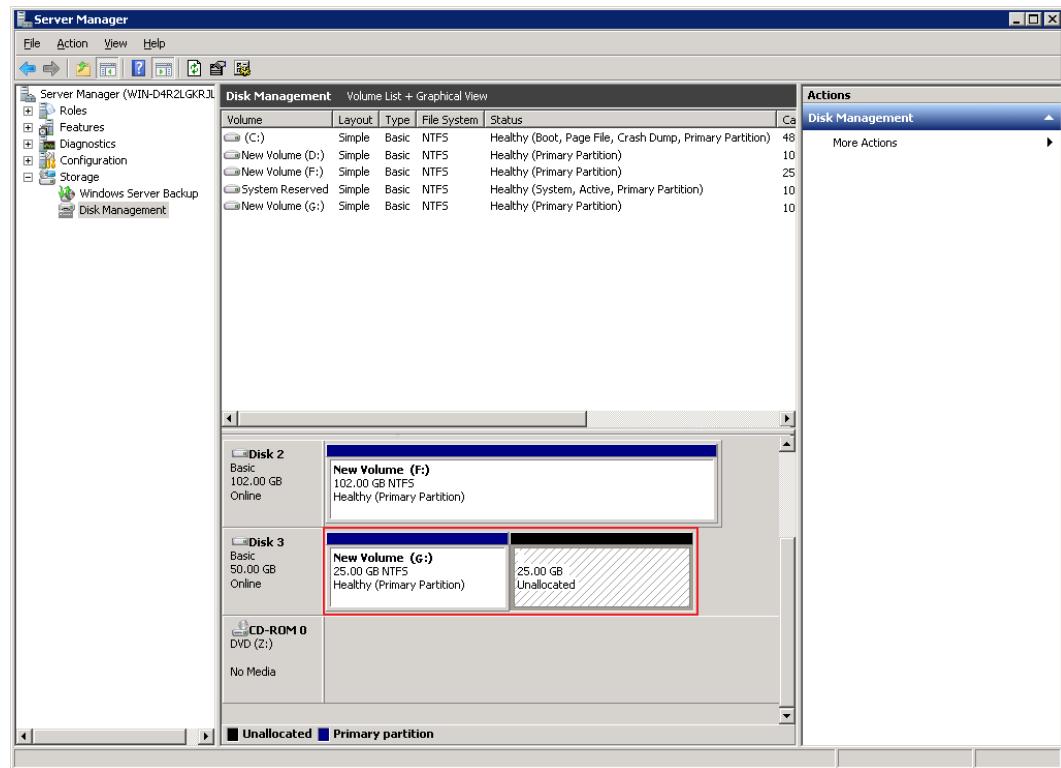
#### Context

In the example of this section, the LUN is mapped as disk 3 on the application server. Its drive letter is G:\, original capacity is 25 GB, and expanded capacity is 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** from the shortcut menu.  
The **Server Manager** dialog box is displayed.
- Step 3** On the left navigation bar of the **Server Manager** dialog box, right-click **Disk Management** and choose **Rescan Disks** from the shortcut menu.  
After the scanning is complete, the system displays the result as shown in [Figure 5-42](#). On the right of disk G, the capacity of the partition to be expanded is displayed.

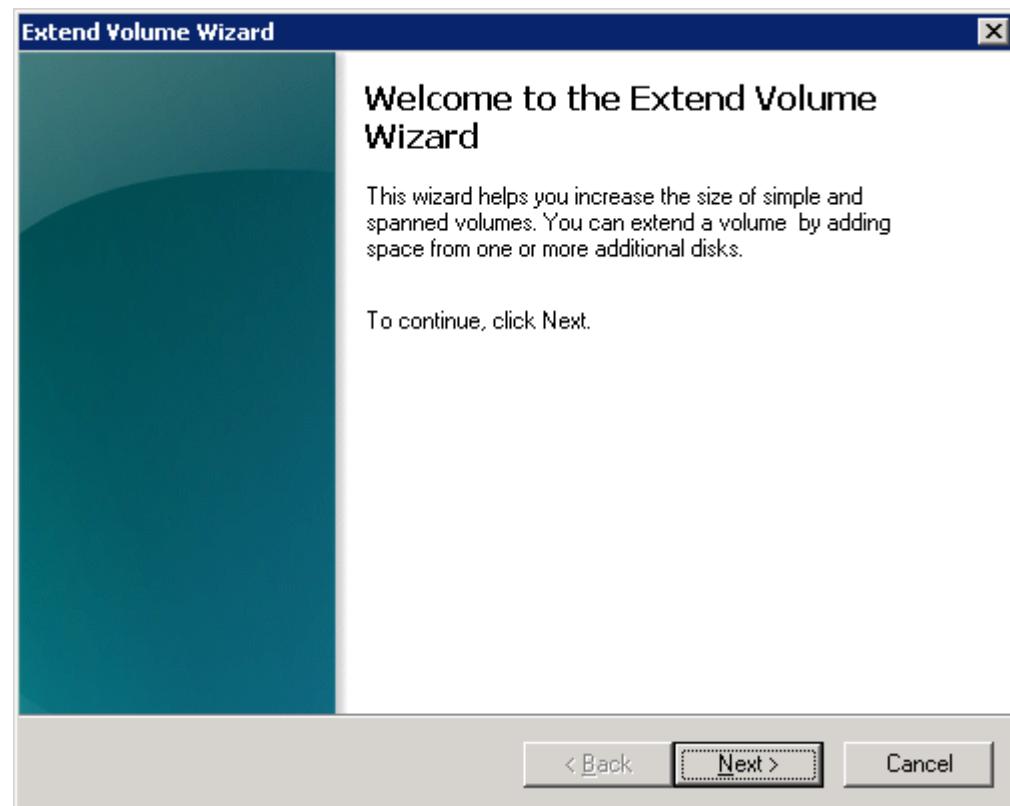
Figure 5-42 Disk scanning result



**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 5-43](#).

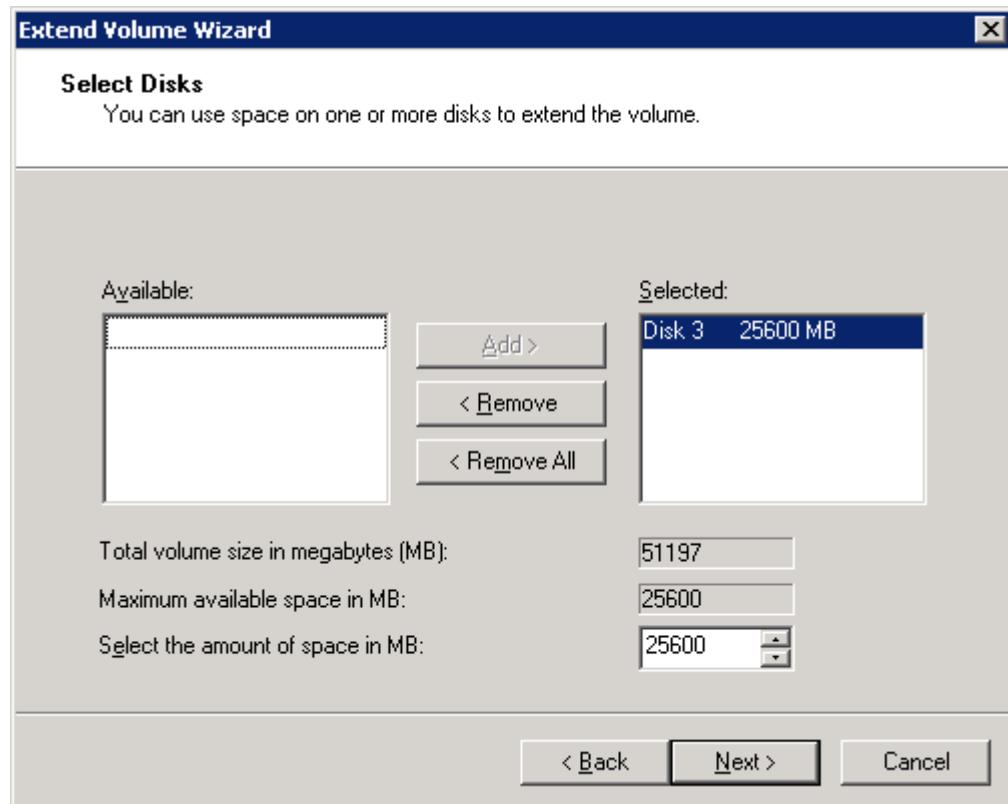
**Figure 5-43** Extend Volume Wizard



**Step 5** Click **Next**.

The **Select Disks** page is displayed, as shown in [Figure 5-44](#).

**Figure 5-44** Select Disks



**NOTE**

- Disk 3 is the disk mapped from the LUN to be expanded on the application server.
- You can change the expansion storage space in **Select the amount of space in MB** to suit your need. By default, the maximum storage space is used.

**Step 6** Click **Next**.

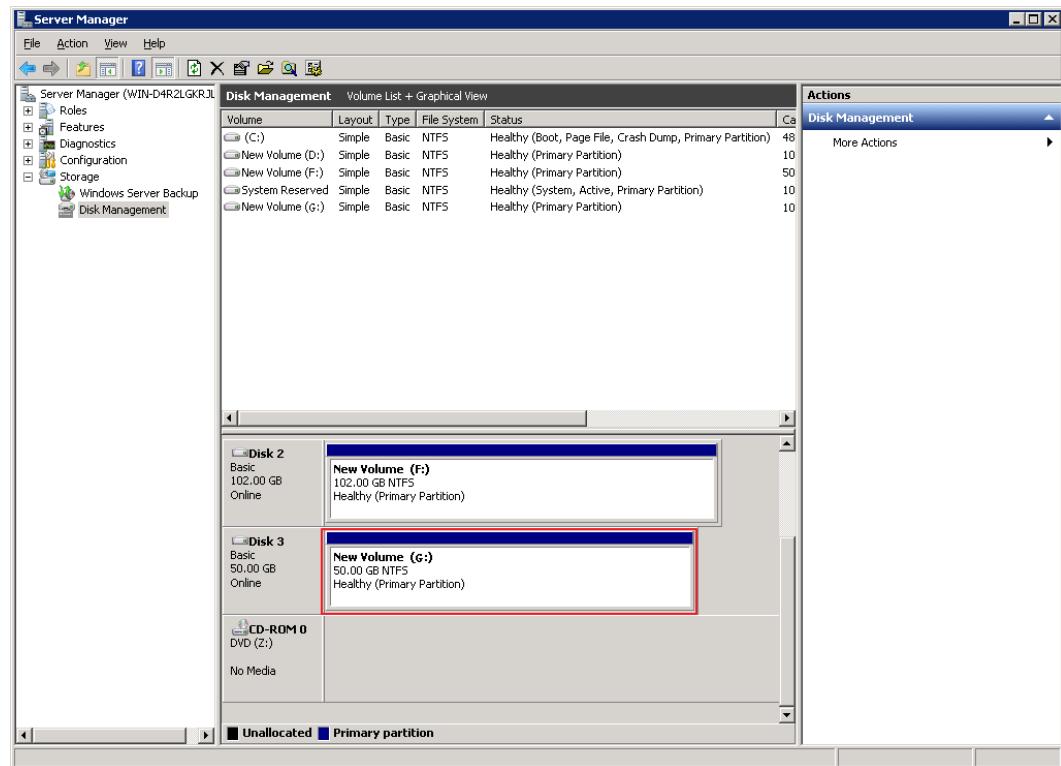
**Step 7** Click **Finish**.

The **Server Manager** dialog box is displayed. You have completed configuring LUN expansion on the application server.

**----End**

## Result

In the **Server Manager** dialog box, view the capacity of disk G after expansion, as shown in [Figure 5-45](#).

**Figure 5-45** Operation result

### 5.14.2.5.2 Expanding a LUN on an Application Server in SUSE

After expanding a LUN on its storage system, perform the expansion configuration on the corresponding application server for it to identify and use the expanded storage space. This task uses an application server running SUSE 11.0 as an example to describe how to expand a LUN on an application server. For application servers running other versions of SUSE operating systems, adjust the operations based on actual conditions.

#### Prerequisites

A LUN has been expanded on the storage system.

#### Context

In the example of the section, the capacity of the LUN to be expanded is 25 GB and it will be expanded to 50 GB. The drive letter of the mapped disk on the application server is **sdf**. The actual drive letter may be different.

#### Procedure

##### Step 1 Scan for disks on the SUSE application server.

1. Scan for disks.
  - If the UltraPath software is installed, run **hot\_add** command.
  - If the UltraPath software is not installed, perform the following operations:
2. Run **lsscsi** to obtain the ID of the host where the LUN resides. 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.

3. Run the **echo '---' > /sys/class/scsi\_host/hostN/scan** command, where *N* indicates the host ID obtained in the preceding step.

After the scanning is complete, the disk capacity remains 25 GB.

4. Run **echo 1 > /sys/block/sdf/device/rescan** 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 on the application server. The actual drive letter may be different.

**Step 2** Run **fdisk -l** to view the 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** To add the file system of the LUN to the new storage space, run **resize2fs /dev/sdf**.

- 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

### 5.14.2.5.3 Using LVM to Expand a LUN in SUSE

After expanding a LUN on its storage system, perform the expansion configuration on the corresponding application server for it to identify and use the expanded storage space. This section uses SUSE 11.0 as an example to describe how to non-disruptively expand a LUN 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 expansion has completed on the storage system.
- A physical volume to be expanded has been determined.

## Context

In the example of the section, **sdb5** is a physical volume in the drive letter of the disk mapped from the LUN on the application server. The primal capacity of **sdb5** is 104 MB, and the capacity after expansion is 120 MB.

## Procedure

**Step 1** On the application server, view 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    0B/0B        Array8.1   --
1tagei       sdb          WMQ_LUN_TEST_003
60022a11000beb2a0421c2a2000002d1 Normal  3.00GB      0A/0A
Array8.1     --
2            sdc          WMQ_LUN_TEST_004 60022a11000beb2a0421c365000002d2
Normal  3.00GB    0B/0B        Array8.1   --
3            sdd          WMQ_LUN_TEST_005 60022a11000beb2a0421c4bd000002d3
Normal  3.00GB    0A/0A        Array8.1   --
-----
```

**Lun WWN** is the WWN of a LUN and **Disk** is the drive letter of a disk mapped from the LUN on the application server.

**Step 2** Run the **echo 1 > /sys/block/sdb5/device/rescan** command to rescan for disks.



**sdb5** is a physical volume in the drive letter of the disk mapped from the LUN on the application server. Adjust configuration operations based on an actual physical volume to be expanded.

**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 a logical volume.

```
lvextend -L +16M /dev/testvg/testlv
Extending logical volume testlv to 120.00 MB
Logical volume testlv successfully resized
```

**testlv** is a 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

### 5.14.2.5.4 Expanding a LUN on an Application Server in Red Hat

After expanding a LUN on its storage system, perform the expansion configuration on the corresponding application server for it to identify and use the expanded storage space. This task uses an application server running Red Hat 6.4 as an example to describe how to expand a LUN on an application server. For application servers running other versions of Red Hat operating systems, adjust the operations based on actual conditions.

#### Prerequisites

A LUN has been expanded on the storage system.

#### Context

In the example of the section, the capacity of the LUN to be expanded is 25 GB and it will be expanded to 50 GB. The drive letter of the mapped disk on the application server is **sdh**. The actual drive letter may be different in practice.

#### Procedure

**Step 1** Scan for disks on the Red Hat application server.

1. Scan for disks.

- If the UltraPath software is installed, run **hot\_add** command.
- If the UltraPath software is not installed, perform the following operations:
  - i. Run **lsscsi** command to obtain the ID of the host where the LUN resides. 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/hostN/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.

After the scanning is complete, the disk capacity becomes 50 GB.



**sdh** indicates the drive letter of the to-be-expanded LUN on the application server. Replace it with the actual drive letter.

**Step 2** Run **fdisk -l** to view the 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** To add the file system of the LUN to the new storage space, run **resize2fs /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

### 5.14.2.5.5 Expanding a LUN on an Application Server in Solaris

After expanding a LUN on its storage system, perform the expansion configuration on the corresponding application server for it to identify and use the expanded storage space. This task uses an application server running Solaris 10 as an example to describe how to expand a LUN on an application server. For application servers running other versions of Solaris operating systems, adjust the operations based on actual conditions.

#### Prerequisites

- A LUN 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-based 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 **cfgadm -al** 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 **umount /mnt/** to unmount corresponding disks of the LUN that you want to expand on the application server.

/mnt/ indicates the mount directory of disks of the LUN.

#### NOTE

If disks of the LUN that you want to expand are not mounted, skip this operation.

**Step 3** Run **format** 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 driver letter mapped by the LUN to the application server.

**Step 4** After **Specify disk (enter its number)**, enter the corresponding ID **3** 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 **type** 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 **partition** and then run **print** 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 **mount /dev/dsk/c10t5d1s6 /mnt** to mount the disk.**Step 10** Run **growfs -M /mnt /dev/rdsk/c10t5d1s6** 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 **df -k** 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

### 5.14.2.5.6 Expanding a LUN on an Application Server in AIX

After expanding a LUN on its storage system, perform the expansion configuration on the corresponding application server for it to identify and use the expanded storage space. This task uses an application server running AIX 6.1 as an example to describe how to expand a

LUN on an application server. For application servers running other versions of AIX operating systems, adjust the operations based on actual conditions.

## Prerequisites

- A LUN 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 that you want to expand 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 and perform the follow-up operations. In the command, **diskName** indicates the disk of 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 **cfdmgr -v** 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 **lsdev -Cc disk** command to view the information about 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 **upadm show lun** 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, run the **upadm show lun** command to check 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 **umount /mnt/lv1** to unmount the file system.

In the command output, **/mnt/lv1** indicates the mount directory of the file system.

**Step 5** Run **varyoffvg vg1** to deactivate volume group **vg1**.

In the command output, **vg1** indicates the name of the volume group corresponding to the LUN that you want to expand.

**Step 6** Run **bootinfo -s hdiskX** 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, if the unit is MB, the capacity is 51,200 MB (50 GB) that is the same as the expansion result displayed on the storage system.

**Step 7** Run **varyonvg vg1** to activate volume group **vg1**.

**Step 8** Refresh the capacity of the volume group corresponding to the LUN that you want to expand.

1. Run **chvg -g vg1** to refresh the volume group of the LUN that you want to expand.

```
# 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 **lsvg vg1** to view parameters related to the volume group.

```
# 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 PVs:      64  
MAX PPs per PV:   2032          AUTO SYNC:    no  
LTG size (Dynamic): 256 kilobyte(s) BB POLICY:  relocatable  
HOT SPARE:        no
```

In the command output, pay attention to the **PP SIZE** parameter. If you want to create or modify a logical volume, you need to refer to the parameter to determine the size of the logical volume. In the example of this section, the value of **PP SIZE** is 32 MB.

**Step 9** Modify the capacity of the logical volume to meet the need for expanding the file system.

1. Run **lslv lv1** to view parameters related to the logical volume.

```
# 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
INTRAPOLICY: 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
```

**lv1** indicates the name of a logical volume on the volume group. Pay attention to the **MAX LPs**, **LPs**, and **PP SIZE** parameters in the command output, as these values 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 the example of this section, 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 **smit lv**.

```
# 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.

* LOGICAL VOLUME name [ ] [Entry Fields] +
```

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 need to 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 need to adjust the maximum number of logical partitions to ensure that the capacity of the logical volume is equal to or larger than 48 GB. For example, if the capacity of the file system needs to be expanded to 48 GB (49,152 MB), the maximum number of logical partitions must be not smaller than 1536 (49,152/32).

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 **chfs -a size=48G /mnt/lv1** to expand the file system of the volume group.

```
# 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 **mount /mnt/lv1** to mount the file system again.

----End

### 5.14.2.5.7 Expanding a LUN on an Application Server in HP-UX

After expanding a LUN on its storage system, perform the expansion configuration on the corresponding application server for it to identify and use the expanded storage space. This task uses an application server running HP-UX 11i v3 as an example to describe how to expand a LUN on an application server. For application servers running other versions of HP-UX operating systems, adjust the operations based on actual conditions.

#### Prerequisites

- A LUN has been expanded on the storage system.
- Services on the LUN to be expanded have been stopped.

#### Context

In this example, the capacity of the LUN will be expanded from 25 GB to 50 GB and its mount directory is **/test/**.

#### Procedure

**Step 1** Scan for LUNs on the HP-UX application server.

1. Run **ioscan** command to scan for hardware.
2. Run **ioscan -funNC disk** to view 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 view LUNs detected by the application server.

**Step 2** Run **umount /test/** to unmount the file system of the LUN.

**/test/** indicates the mount directory of the file system.

**Step 3** Run **extendfs -F vxfs /dev/disk/disk399** to expand the file system of the LUN.

**vxfs** indicates the file system type.

**Step 4** Run **mount /dev/disk/disk399 /test/** to mount the file system of the LUN.

**Step 5** Run **bdf** to view the file system capacity after it is expanded.

```
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

#### 5.14.2.5.8 Expanding a LUN on an Application Server in VMware ESX

After expanding a LUN on its storage system, perform the expansion configuration on the corresponding application server for it to identify and use the expanded storage space. This task uses an application server running VMware ESXi 5.1.0 as an example to describe how to expand a LUN on an application server. For application servers running other versions of VMware ESX operating systems, adjust the operations based on actual conditions.

#### Prerequisites

A LUN has been expanded on the storage system.

#### Context

In the example of the section, the capacity of the LUN to be expanded is 25 GB and it will be expanded to 50 GB. The ID of the LUN to be expanded is **14**.

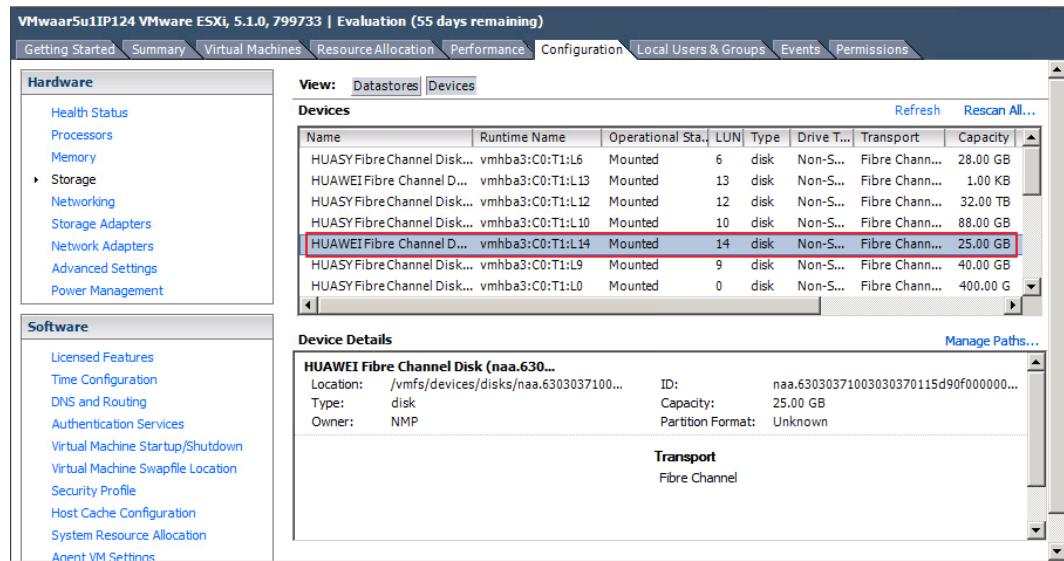
#### Procedure

**Step 1** In vSphere Client, click the **Configuration** tab.

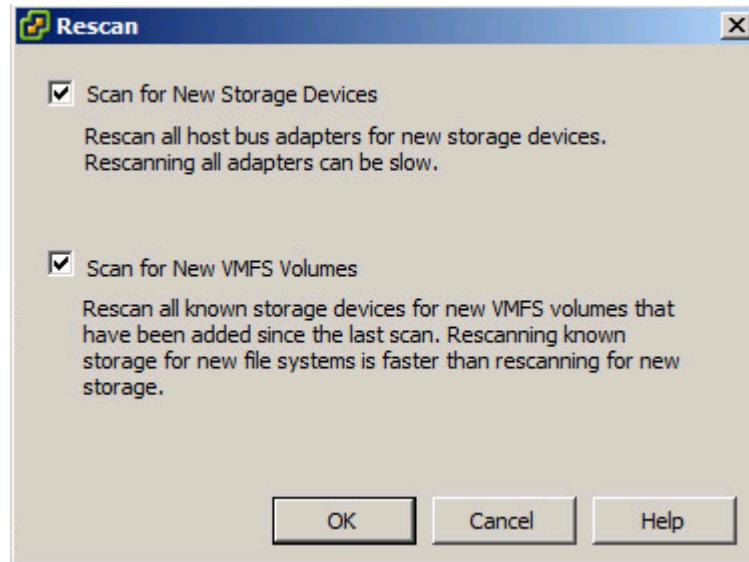
**Step 2** On the left navigation bar, click **Storage**.

**Step 3** On the **Storage** page, click the **Devices** tab.

On the **Devices** page, view the device mapped from the LUN to be expanded on the application server, as shown in [Figure 5-46](#).

**Figure 5-46** Device mapped from the LUN to be expanded on the application server**Step 4** On the Devices page, click Rescan All.

The Rescan dialog box is displayed, as shown in **Figure 5-47**.

**Figure 5-47** Rescan 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 5-48**, the scanning is ongoing.

**Figure 5-48** Scanning ongoing

Recent Tasks								
Name	Target	Status	Details	Initiated by	vCenter Server	Requested Start Ti...	Start Time	Completed Time
Rescan VMFS		In Progress		Administrator	win232.zcyunhvs...	8/19/2013 6:47:46 PM	8/19/2013 6:47...	
Rescan all HBAs		In Progress		Administrator	win232.zcyunhvs...	8/19/2013 6:46:58 PM	8/19/2013 6:46...	

- If the task status is **Completed** as shown in **Figure 5-49**, the scanning is completed.

**Figure 5-49** Scanning completed

Recent Tasks								
Name	Target	Status	Details	Initiated by	vCenter Server	Requested Start Ti...	Start Time	Completed Time
Rescan VMFS		Completed		Administrator	win232.zcyunhvs...	8/19/2013 6:47:46 PM	8/19/2013 6:47...	8/19/2013 6:47:58 PM
Rescan all HBAs		Completed		Administrator	win232.zcyunhvs...	8/19/2013 6:46:58 PM	8/19/2013 6:46...	8/19/2013 6:47:46 PM

**Step 6** On the Storage page, click the **Datastores** tab.

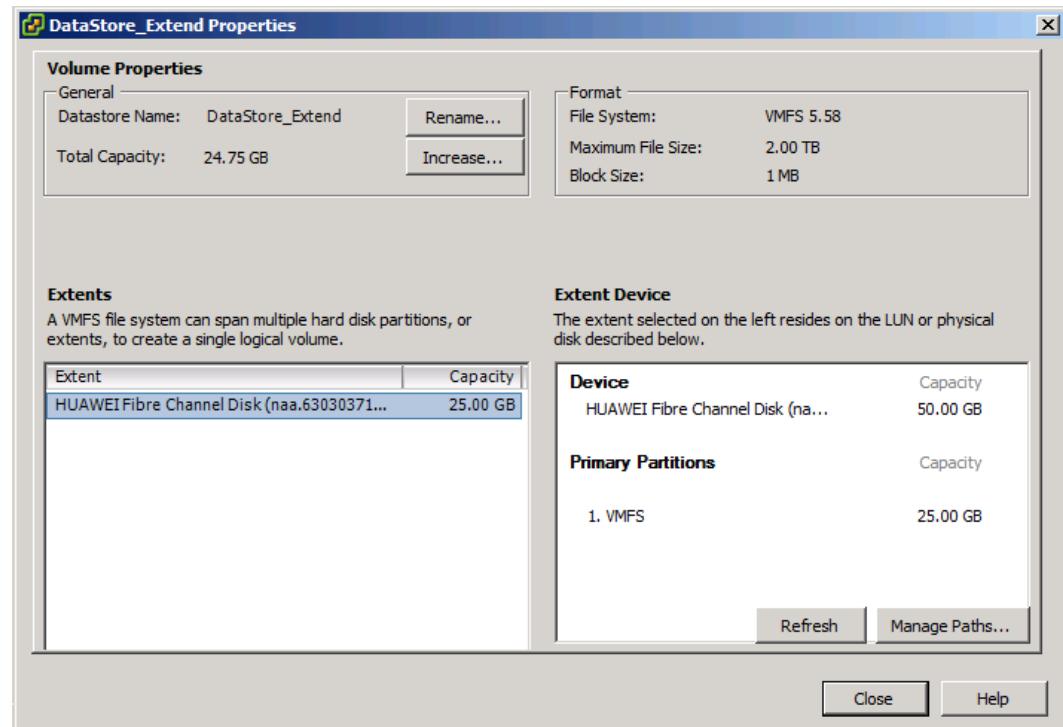
On the **Datastores** page, view the datastore mapped from the LUN to be expanded on the application server, as shown in **Figure 5-50**.

**Figure 5-50** Device mapped from the LUN to be expanded on the application server

Identification	Device	Drive Type	Capacity	Free	Type	Last Update
DataStore_Extend	HUAWEI Fibre Ch...	Non-SSD	24.75 GB	23.83 GB	VMFSS	6/29/2013 11:29:40 AM
DataStore_T_400	HUASY Fibre Cha...	Non-SSD	399.75 GB	102.65 GB	VMFSS	6/29/2013 11:29:40 AM
DataStore_T_50	HUASY Fibre Cha...	Non-SSD	49.75 GB	8.80 GB	VMFSS	6/29/2013 11:29:40 AM
DataStore_T_50...	HUASY Fibre Cha...	Non-SSD	49.75 GB	48.80 GB	VMFSS	6/29/2013 11:29:40 AM
DataStore_T_500...	HUASY Fibre Cha...	Non-SSD	499.75 GB	418.79 GB	VMFSS	6/29/2013 11:29:40 AM
DataStore_T_OS	HUASY Fibre Cha...	Non-SSD	199.75 GB	58.68 GB	VMFSS	6/29/2013 11:29:40 AM
datastore1(1)	LSILOGIC Serial A...	Non-SSD	131.00 GB	130.05 GB	VMFSS	6/29/2013 11:29:40 AM

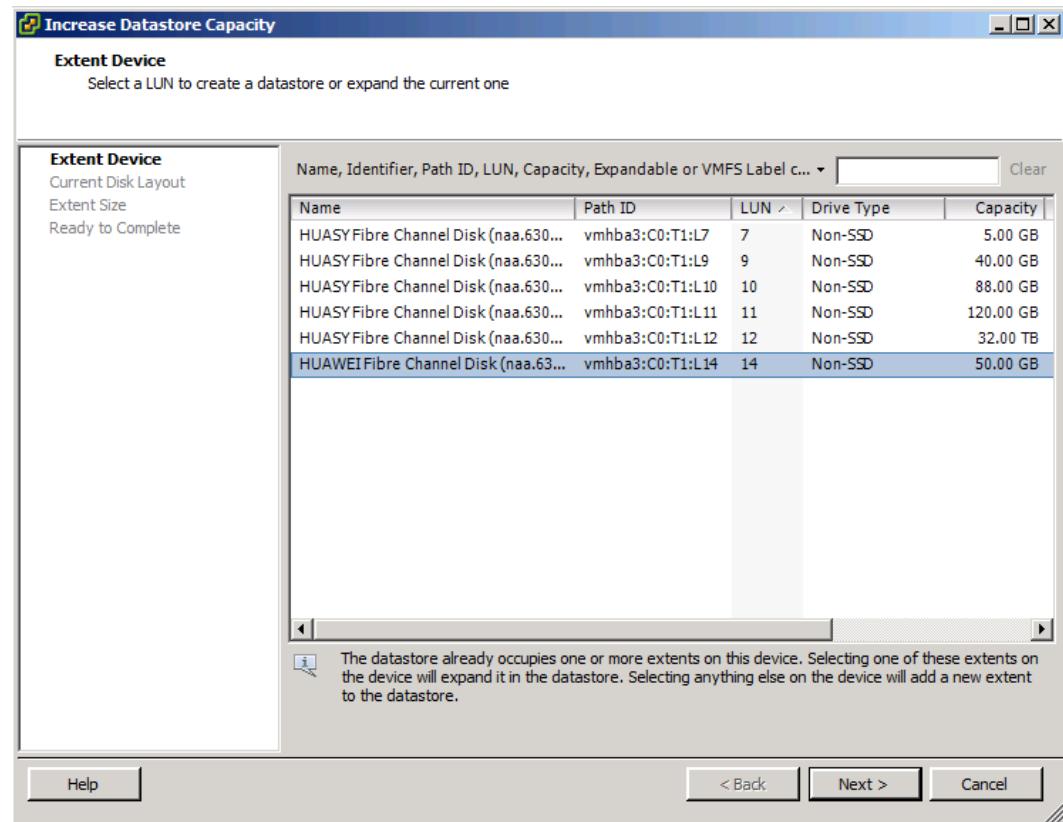
**Step 7** Right-click the datastore corresponding to the LUN to be expanded, and choose **Properties** from the shortcut menu.

The **DataStore\_Extend Properties** dialog box is displayed, as shown in **Figure 5-51**.

**Figure 5-51 DataStore\_Extend Properties dialog box**

**Step 8** In the Volume Properties area, click **Increase**.

The **Increase Datastore Capacity** dialog box is displayed, as shown in [Figure 5-52](#).

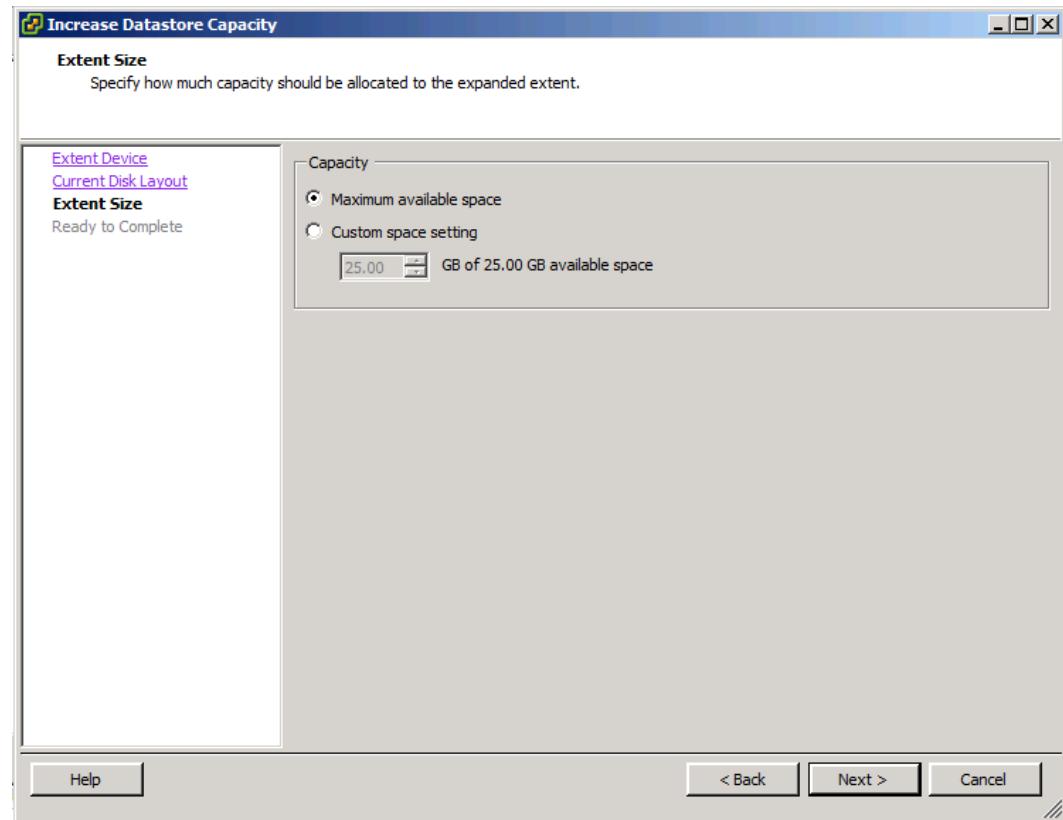
**Figure 5-52 Increase Datastore Capacity dialog box**

**Step 9** Select the datastore corresponding to the LUN to be expanded and click **Next**.

**Step 10** View the current disk distribution and click **Next**.

**Step 11** Set the size of the expansion data area. The maximum storage space is recommended, as shown in **Figure 5-53**. Click **Next**.

**Figure 5-53** Setting the size of the expansion data area



**Step 12** Click **Finish**.

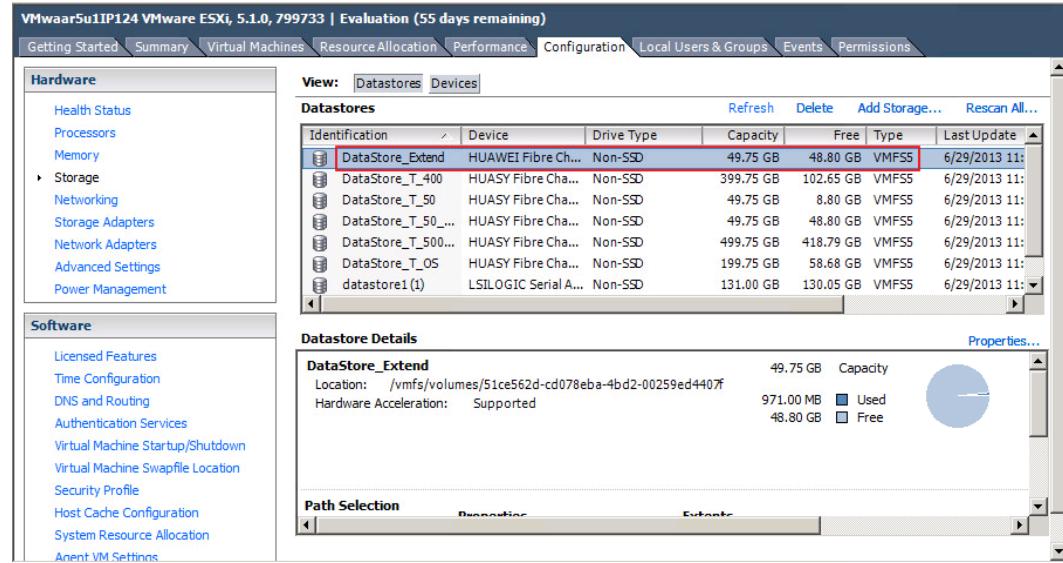
The **DataStore\_Extend Properties** dialog box is displayed.

**Step 13** Click **Close**.

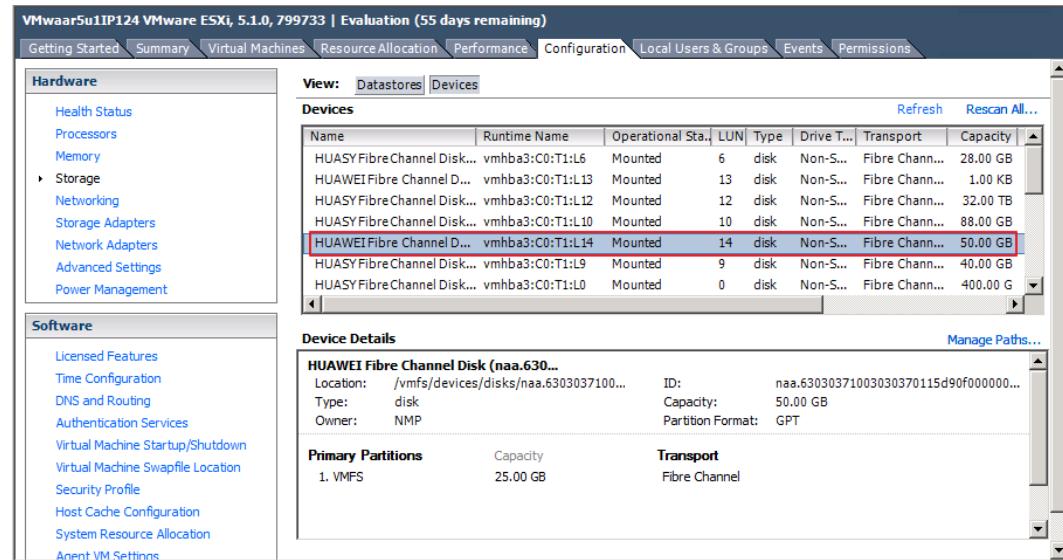
----End

## Result

- On the **Datastores** tab of **Storage** page, view the expanded datastore, as shown in [Figure 5-54](#).

**Figure 5-54** Datastore mapped from the expanded LUN on the application server

- On the **Devices** tab of **Storage** page, view the expanded device, as shown in [Figure 5-55](#).

**Figure 5-55** Device mapped from the expanded LUN on the application server

### 5.14.2.5.9 Expanding a LUN on an Application Server in Hyper-V

After expanding a LUN on its storage system, perform the expansion configuration on the corresponding application server for it to identify and use the expanded storage space. Using Windows Server 2016 Hyper-V cluster as an example, this section describes how to add LUNs at the application server side. For LUN expansion in Hyper-V clusters of other versions, adjust the operations based on actual conditions.

## Prerequisites

LUN expansion has completed on the storage system.

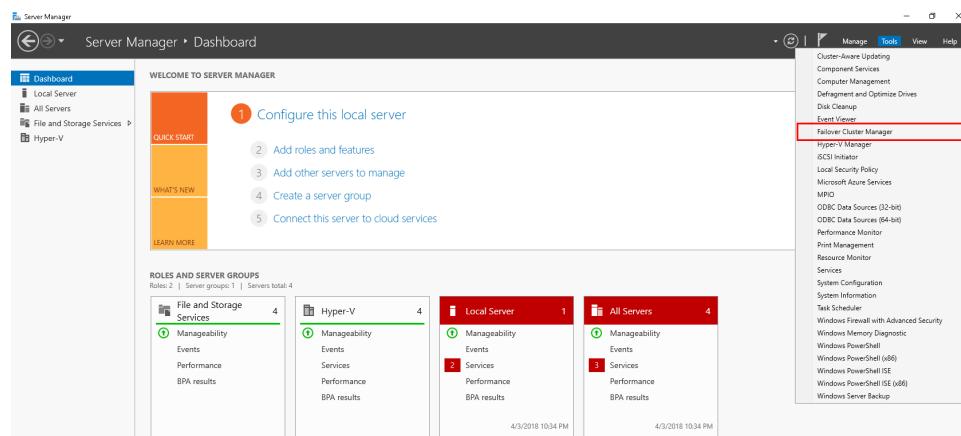
## Context

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. Its original capacity is 25 GB and the capacity after expansion is 58 GB.

## Procedure

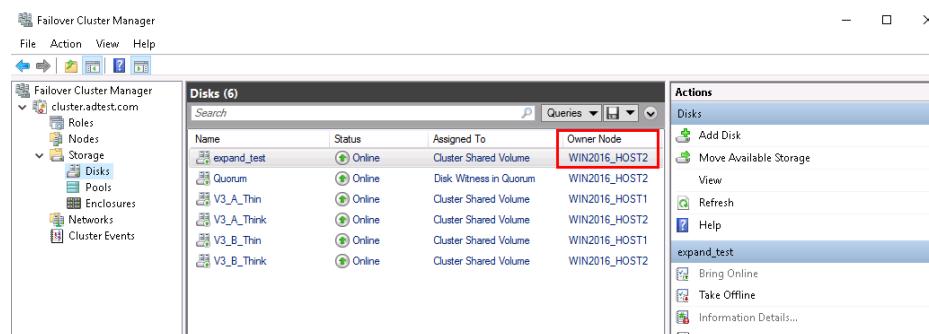
**Step 1** Query the **Owner Node** of the shared volume of the cluster to be expanded.

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** from the shortcut menu.  
The **Server Manager** dialog box is displayed.
3. Choose **Tools > Failover Cluster Manager**.  
The **Failover Cluster Manager** dialog box is displayed.



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 to be expanded.

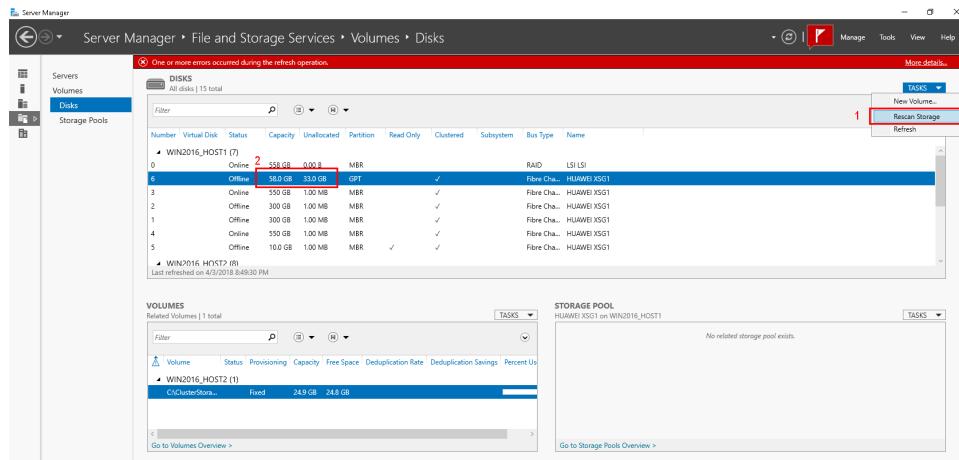
In this example, the Owner Node of the shared volume of the cluster to be expanded is WIN2016\_HOST2.



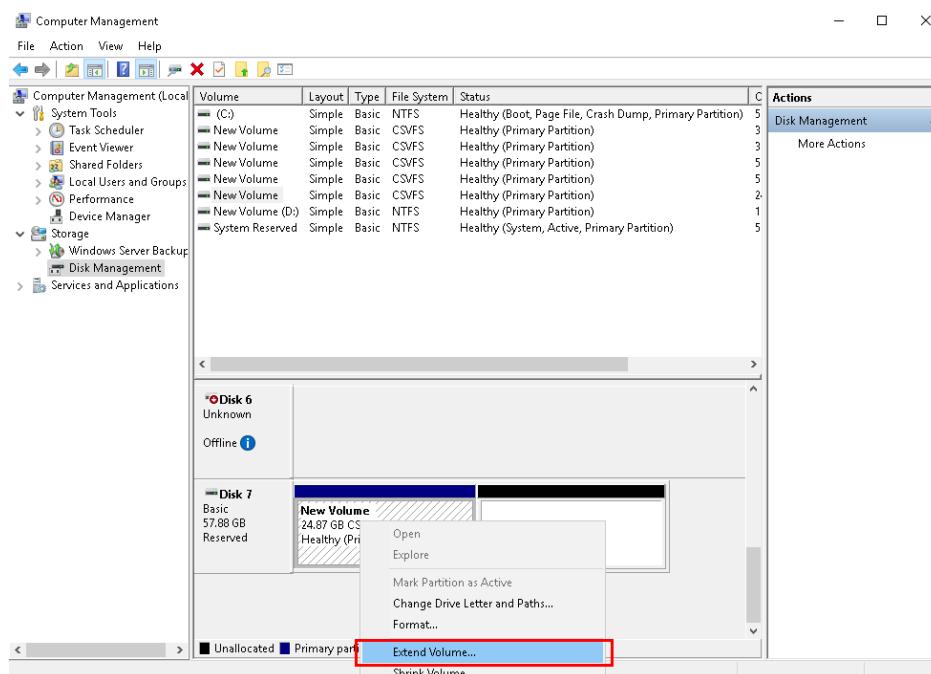
**Step 2** Perform volume capacity expansion on the Owner Node of the shared volume of the cluster to be expanded. The following procedure takes the WIN2016\_HOST2 application server as an example.

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.

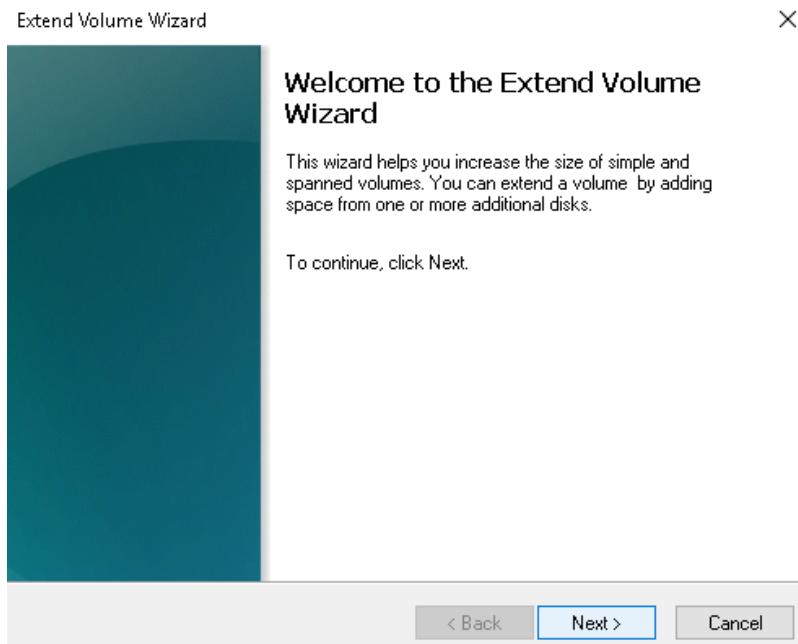
After the scanning is complete, check the capacity of the partitions to be expanded in the **DISKS** area. In this example, the total capacity of the partitions to be expanded is 58 GB in which 33 GB is the unallocated capacity.



4. On the **Server Manager** page, choose **Tools > Computer Management**.  
The **Computer Management** dialog box is displayed.
5. Expand **Storage > Disk Management** in the navigation tree.

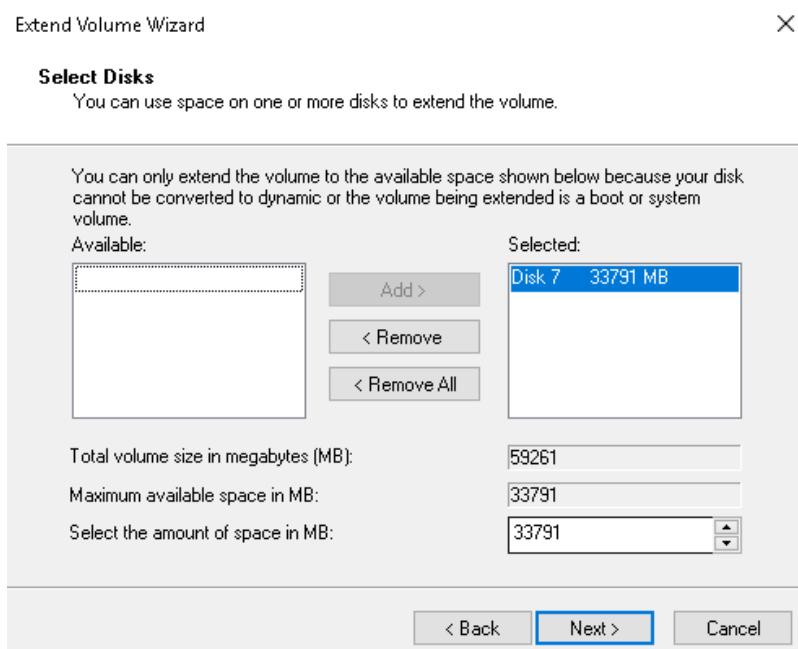


6. Right-click **Disk 7** and choose **Extend Volume...** from the shortcut menu.  
The **Extend Volume Wizard** dialog box is displayed.



7. Click **Next**.

The **Select Disks** page is displayed.



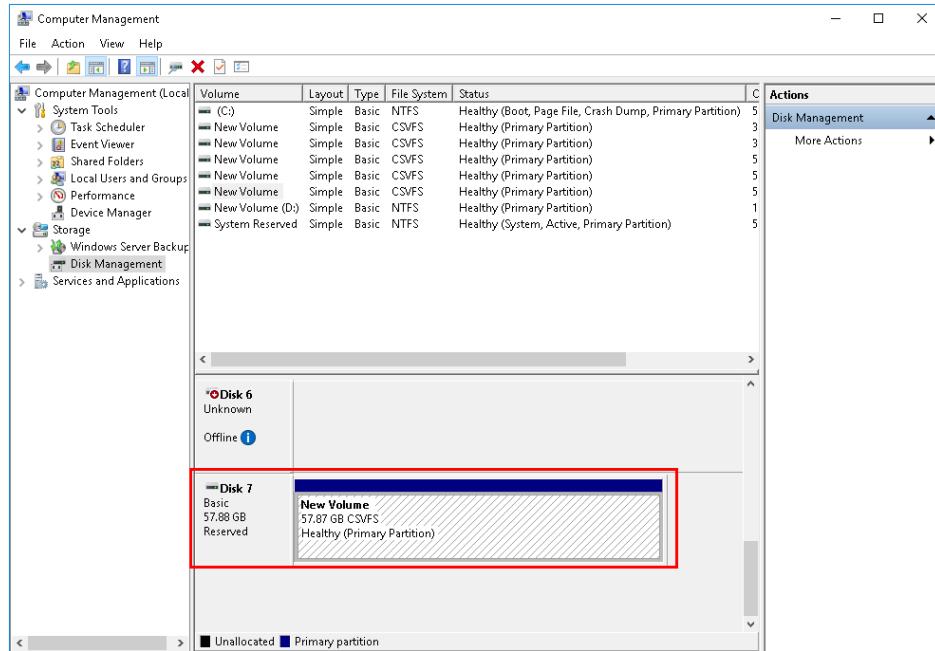
**NOTE**

- Disk 7 is the disk mapped from the LUN to be expanded on the application server.
- You can change the space for capacity expansion in the **Select the amount of space in MB** field based on the capacity requirements. By default, it equals the maximum available space.

8. Click **Next**.
9. Click **Finish**. The partition expansion of the application server is complete.

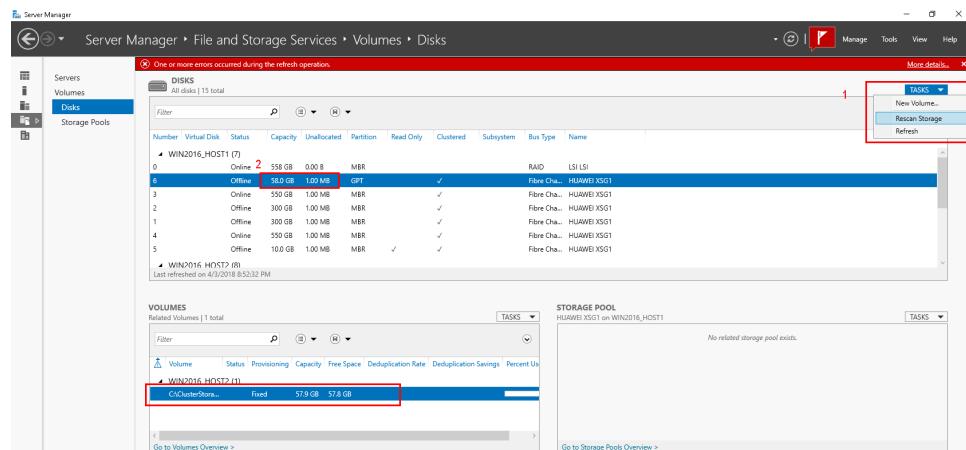
**NOTE**

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.

**Step 3** Scan and check the result of shared volume capacity expansion.

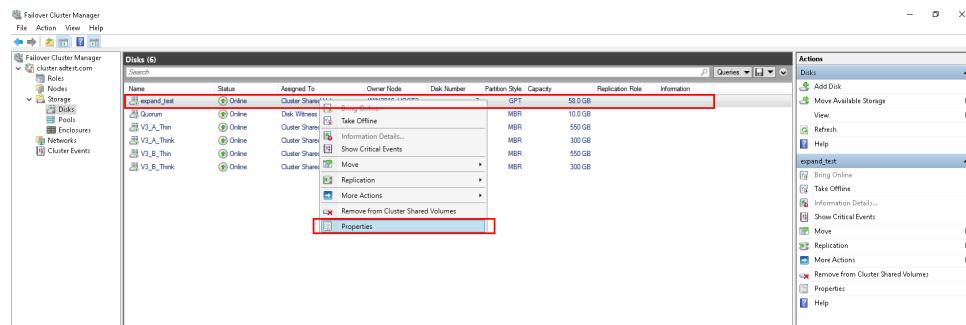
- On the **Server Manager** page, click **TASK** and choose **Rescan Storage** from the shortcut menu to scan disks of all application servers in the cluster.

After the scanning is complete, check the capacity after capacity expansion in the **DISKS** area. In this example, the total capacity after disk scanning is 58 GB.

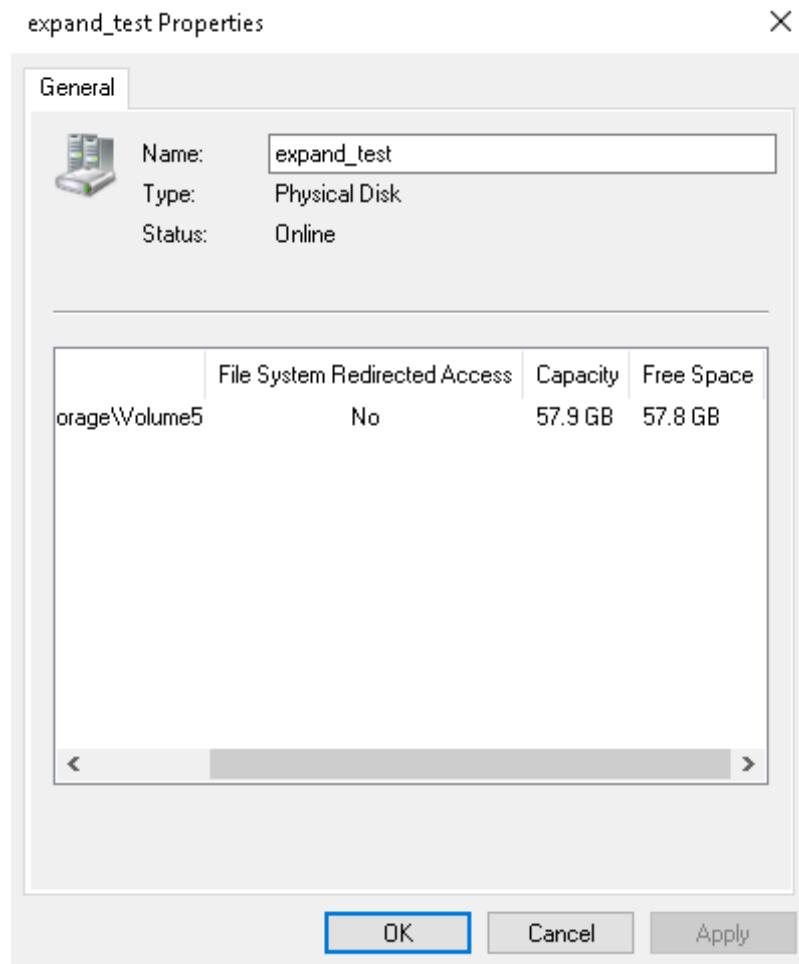


- On the **Failover Cluster Manager** page, right-click the shared volume of the cluster to be expanded and choose **Properties** from the shortcut menu.

The **Properties** dialog box is displayed.

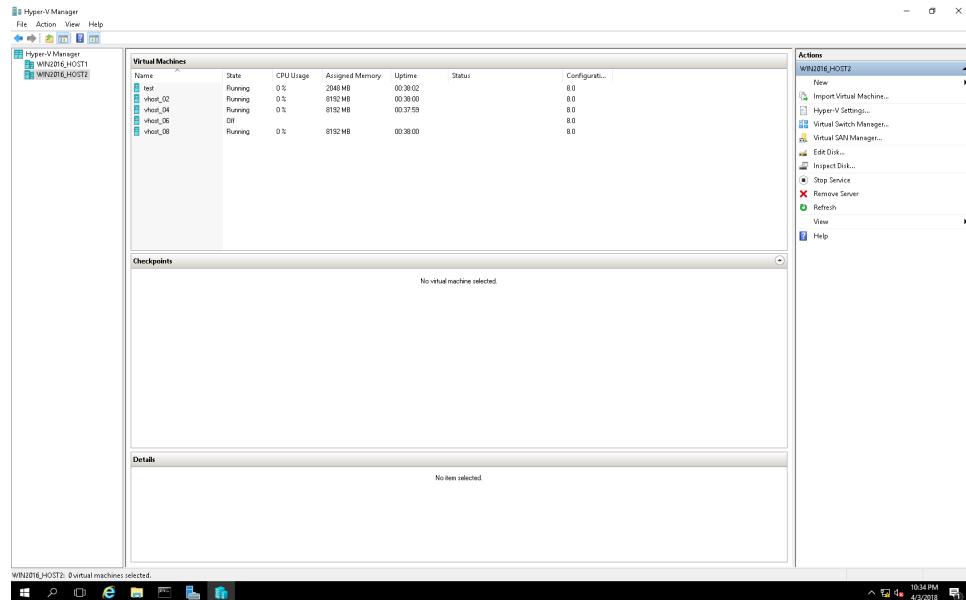


3. If the volume status is **Online** and the total volume capacity is the expected capacity after expansion, the volume is successfully expanded.



**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.

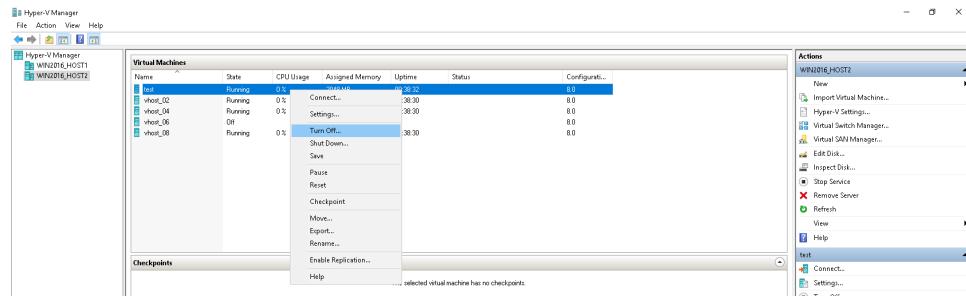
1. On the **Server Manager** page, choose **Tools > Hyper-V Manager**.  
The **Hyper-V Manager** dialog box is displayed.



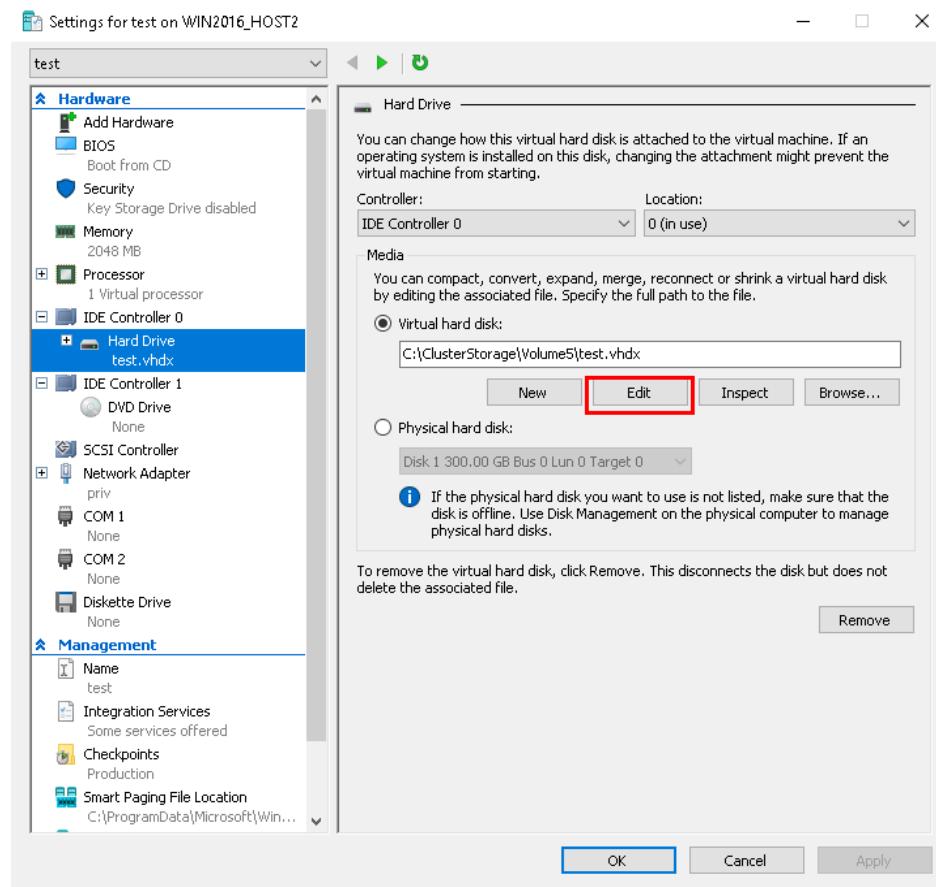
2. (Optional) Stop the VM. Right-click the VM to be expanded and choose **Turn Off** from the shortcut menu.

**NOTE**

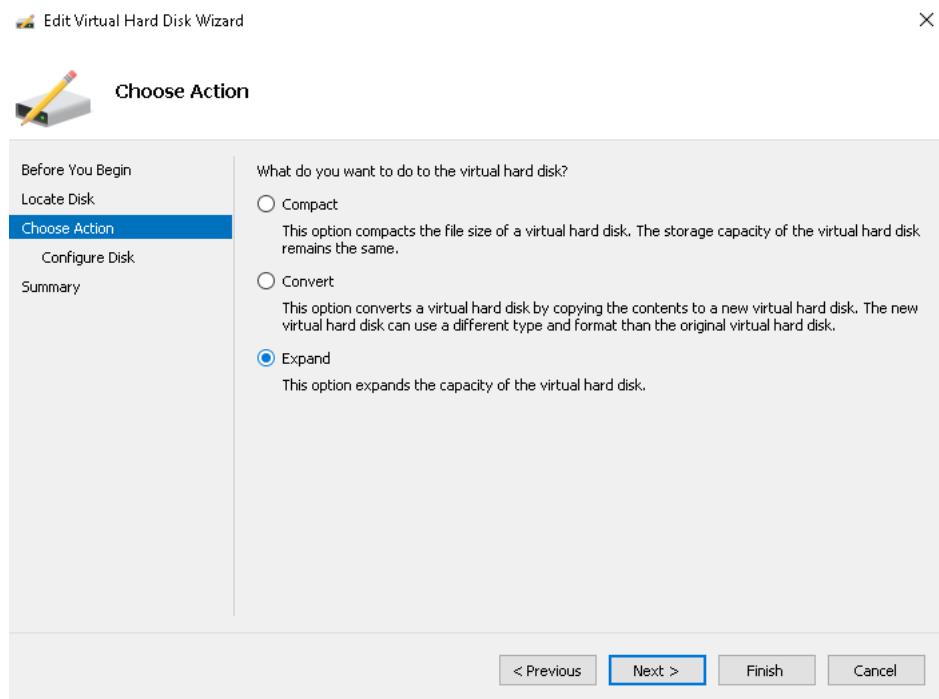
- For a VM that uses the IDE disk controller, you must stop the VM before performing capacity expansion.
- For Windows Server 2012 R2 and later operating systems, if the VM uses the SCSI disk controller, skip this step.
- For operating systems earlier than Windows Server 2012 R2, if the VM uses the SCSI disk controller, you must stop the VM before capacity expansion.



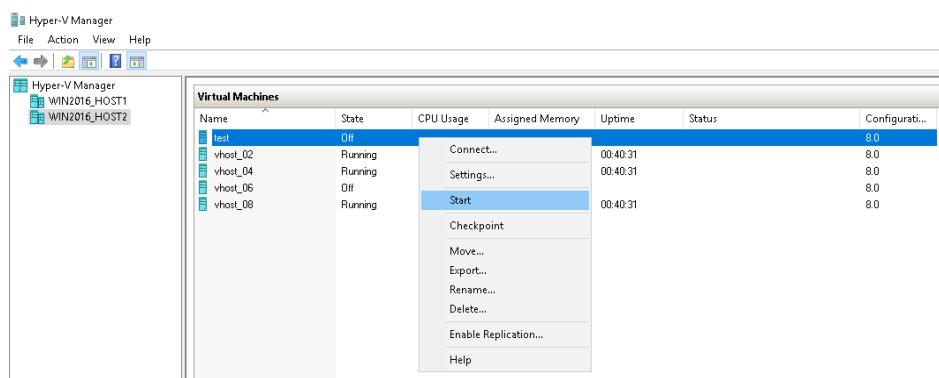
3. Right-click the VM name, and choose **Settings** from the shortcut menu.

**Figure 5-56** 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**.

**Figure 5-57** 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 of the Hyper-V VM is completed.
7. If the VM is stopped, perform the following operations: Right-click the VM to be expanded and choose **Start** from the shortcut menu to restart the VM.



----End

#### 5.14.2.5.10 Expanding a LUN on an Application Server in FusionCompute

After expanding a LUN on its storage system, perform the expansion configuration on the corresponding application server for it to identify and use the expanded storage space. Using FusionCompute 6.3.0 as an example, this section describes how to add LUNs at the application server side. For LUN expansion in FusionCompute application servers of other versions, adjust the operations based on actual conditions.

## Prerequisites

LUN expansion has completed on the storage system.

A maximum of 64 capacity expansion operations can be performed on a datastore, and the total datastore capacity cannot be greater than 64 TB.

The datastore type is virtualized SAN storage.

## Procedure

### Step 1 Scan for storage devices.

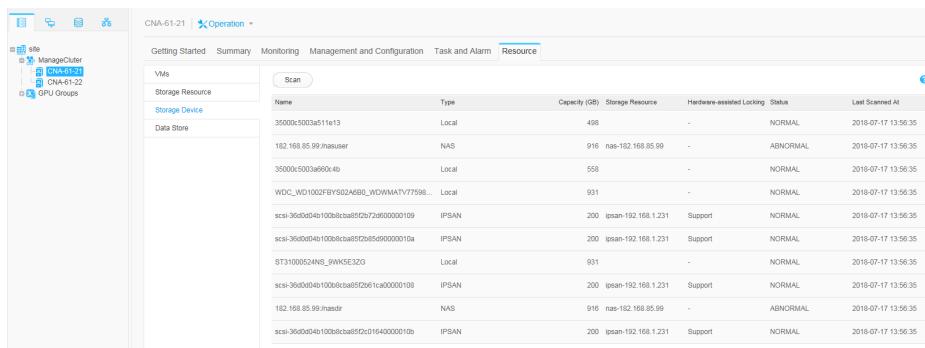
1. Log in to FusionCompute.
2. Click **Host and Cluster**.

The **Host and Cluster** page is displayed.

3. In the navigation tree, choose site > Cluster > Host.

In the middle function pane, choose **Resource > Storage Device**.

The storage device list is displayed.



Name	Type	Capacity (GB)	Storage Resource	Hardware-assisted Locking	Status	Last Scanned At
35000c5003a511e13	Local	498	-	-	NORMAL	2018-07-17 13:56:35
182.168.85.99.masuer	NAS	916	nas-182.168.85.99	-	ABNORMAL	2018-07-17 13:56:35
35000c5003a6004b0	Local	558	-	-	NORMAL	2018-07-17 13:56:35
WDC_WD1002BYS02A6BL_WDWMATV7798...	Local	931	-	-	NORMAL	2018-07-17 13:56:35
scsi-360d04b100b6cafa5f2b72d600000109	IPSAN	200	ipsan-192.168.1.231	Support	NORMAL	2018-07-17 13:56:35
scsi-360d04b100b6cafa5f2b72d60000010a	IPSAN	200	ipsan-192.168.1.231	Support	NORMAL	2018-07-17 13:56:35
ST100052ANS_9WKE5EZO	Local	931	-	-	NORMAL	2018-07-17 13:56:35
scsi-360d04b100b6cafa5f2b72d61ca00000108	IPSAN	200	ipsan-192.168.1.231	Support	NORMAL	2018-07-17 13:56:35
182.168.85.99.jnaddr	NAS	916	nas-182.168.85.99	-	ABNORMAL	2018-07-17 13:56:35
scsi-360d04b100b6cafa5f2d016400000010b	IPSAN	200	ipsan-192.168.1.231	Support	NORMAL	2018-07-17 13:56:35

4. Click **Scan**.

The **Information** dialog box is displayed.

5. Click **OK**. The system starts to scan for storage devices.

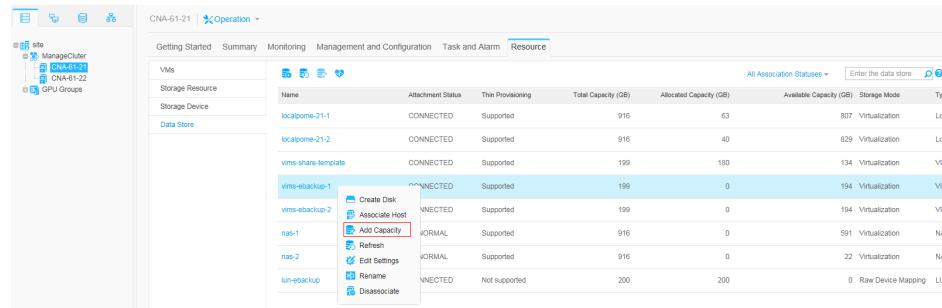


Click **click here** in the **Information** dialog box. On the **Task Center** page that is displayed, check the scan progress.

After the scan is complete, you can view the capacity of IP SAN storage that is the storage system's LUN mapped 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.



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

## 5.14.3 Adding LUNs for Storage Space Expansion

You can add LUNs to expand capacity for existing services, so that application servers can use added storage space.

### 5.14.3.1 Adding LUNs at the Storage Side

Create new LUNs and map them to application servers' LUN groups so that application servers can use the added storage space.

#### Prerequisites

- Communication is normal between a storage system and an application server that requires expanded storage space.
- You have confirmed an application server to which a new LUN is mapped and the size of the LUN.
- The storage system has a storage pool that provides sufficient storage space to create LUNs.
- If a Fibre Channel network is used, ensure that the world wide name (WWN) of a Fibre Channel initiator has been obtained.
- If an Internet Small Computer Systems Interface (iSCSI) network is used, ensure that the iSCSI qualified name (IQN) of an 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
<b>initiator_type=?</b>	Initiator type.	Possible values are <b>FC</b> and <b>iSCSI</b> , where: - <b>iSCSI</b> : indicates an iSCSI initiator. - <b>FC</b> : indicates a Fibre Channel initiator.
<b>wwn=?</b>	WWN of a Fibre Channel initiator. This parameter is available only when <b>initiator_type=?</b> is <b>FC</b> .	To obtain the value, run the <b>show initiator</b> command without parameters.
<b>iscsi_iqn_name=?</b>	IQN of an iSCSI initiator. This parameter is available only when <b>initiator_type=?</b> is <b>iSCSI</b> .	To obtain the value, run the <b>show initiator</b> command without parameters.

```
admin:/>show initiator initiator_type=FC wwn=100000109b1c80ba
      WWN          : 100000109b1c80ba
      Running Status : Online
      Free          : No
      Alias         : --
      Host ID       : 0
      Multipath Type: Default
      Failover Mode : --
      Path Type     : --
      Special Mode Type : --
```

The value of **Host ID** is the ID of a 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 **show host\_group mapping\_view host\_group\_id=?** 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 **show mapping\_view lun\_group mapping\_view\_id=?** 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** In the navigation tree on the right, click \_\_\_\_\_.

The **Provisioning** page is displayed.

**Step 3** Create LUNs.

1. In the **Block Storage Service** area, click **LUN**.  
Go to the LUN management page
2. Click **Create**.  
The **Create LUN** page is displayed.
3. Set parameters as required by the added LUN. **Table 5-33** describes the parameters.

**Table 5-33** Main parameters for creating a LUN

Parameter	Description
Capacity	Indicates the actual storage space assigned to the LUN. The capacity you set is the actual capacity that can be used by 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 4** Add the newly created LUNs to a LUN group.

1. On the LUN management page, click the **LUN Group** tab.  
Go to the LUN group page.
2. Select a LUN group to which you want to add the LUNs and click **Add Object**.  
Go to the **Add Object** page.
3. In the **Available LUN** area, select the newly created LUNs, click , and add the LUNs to the **Selected LUN** area.
4. Click **OK**.

----End

### 5.14.3.2 Adding LUNs at the Application Server Side

#### 5.14.3.2.1 Adding LUNs at the Application Server Side (in Windows)

After creating LUNs and adding them to a LUN group at the storage system side, you need to perform necessary configurations at the application server side to identify and use the added storage space. Using Windows Server 2008 as an example, this section describes how to add LUNs at the application server side. 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 at the storage side.

## Procedure

**Step 1** Log in to the application server as **administrator**.

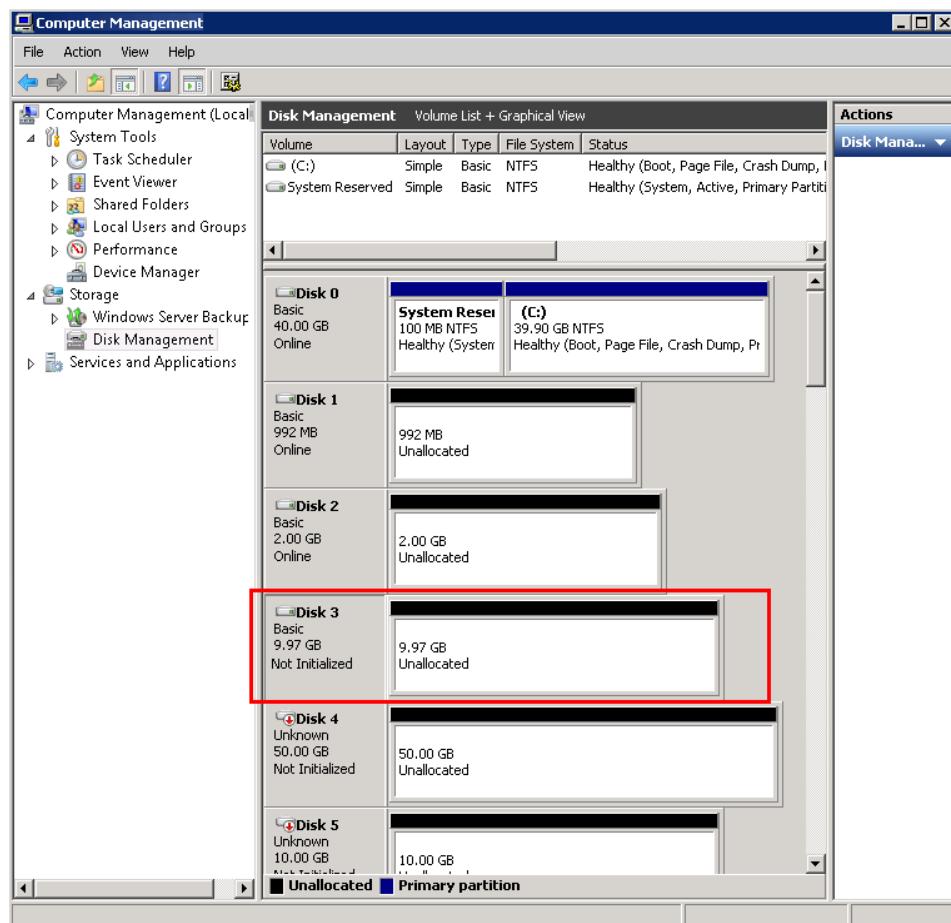
**Step 2** Go to the **Server Manager** dialog box.

Right-click **Computer** and choose **Manage** from the shortcut menu.

**Step 3** In the navigation tree, click **Disk Management** and scan for new logical disks.

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 in the right area (using Disk 3 as an example), as shown in the red square in **Figure 5-58**. (The display varies with the disk size).

**Figure 5-58** Viewing new logical disks



- If no new logical disk is detected, perform the following operations:
  1. Choose **Server Manager > Diagnostics > Device Manager > Disk Drives**.
  2. Right-click **Disk Drives** and choose **Scan for hardware changes** from the shortcut menu.

3. Rescan for logical disks. If no new logical disk is detected, troubleshoot the fault and rescan for logical disks.

 **NOTE**

If no mapped disk is detected, possible causes are:

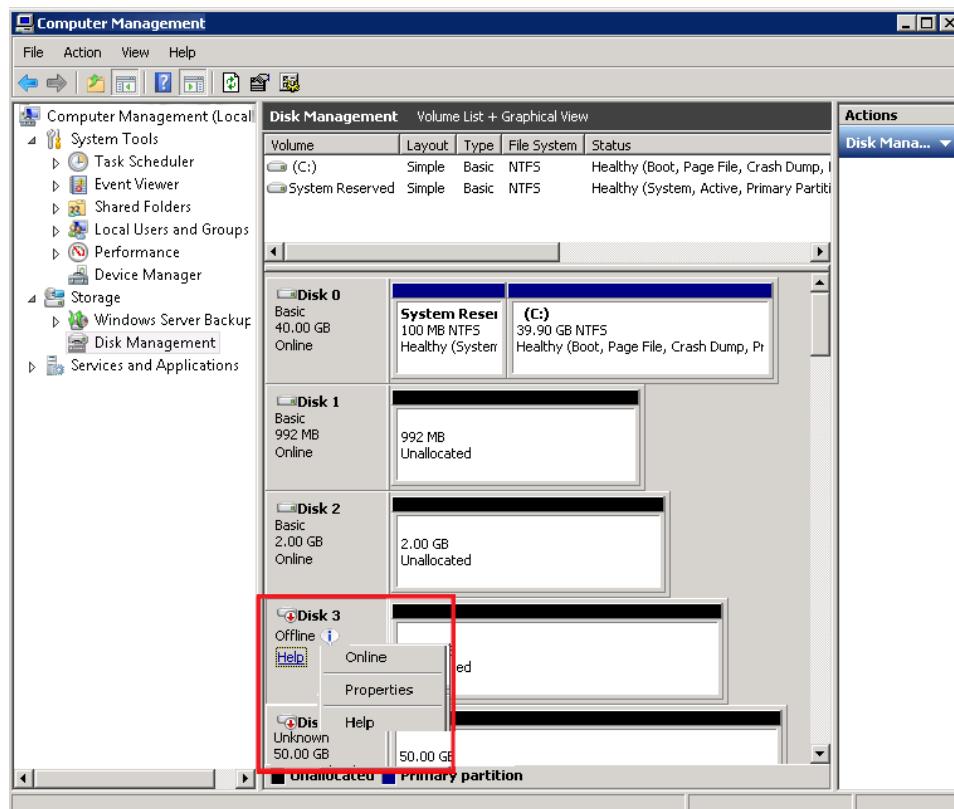
- The application server is not correctly connected to the storage system after the network cable has been removed and reinserted.
- The link between the application server and storage system is down.
- The rate of the Fibre Channel host port is inconsistent with that of the Fibre Channel HBA on the 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*.

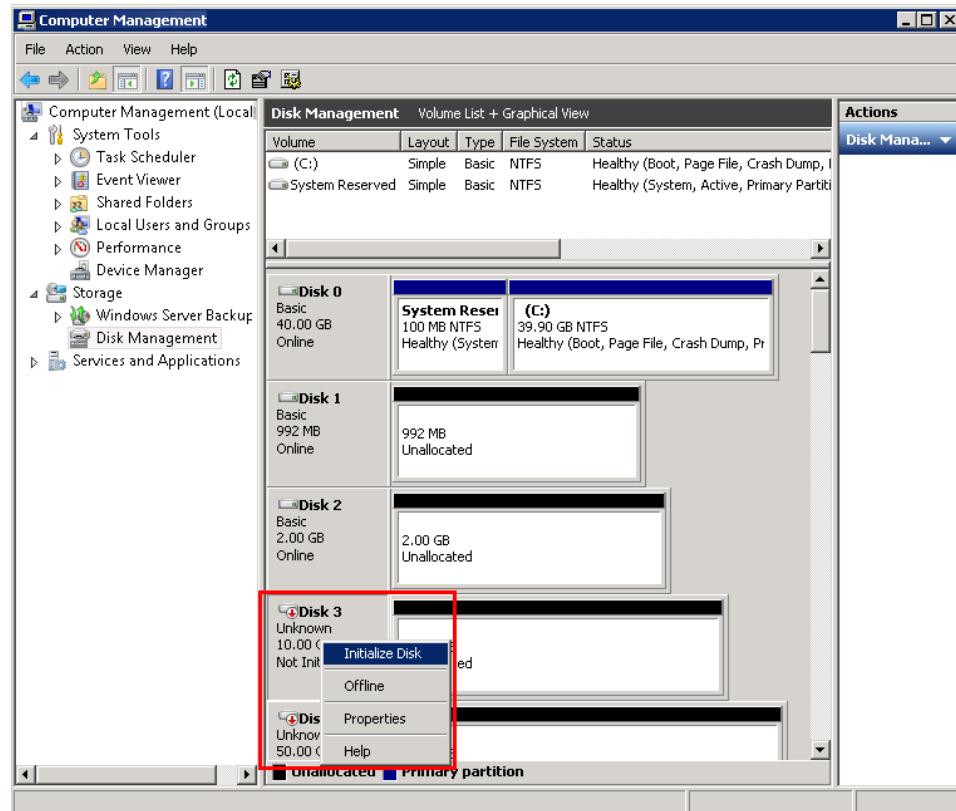
**Step 4** Initialize the new logical disks.

1. Right-click **Disk 3** (as shown in the red square in [Figure 5-59](#)) and choose **Online** from the shortcut menu. The status of **Disk 3** is **Not Initialized**.

**Figure 5-59** Online disk list



2. Right-click **Disk 3** (as shown in the red square in [Figure 5-60](#)) and choose **Initialize Disk** from the shortcut menu.

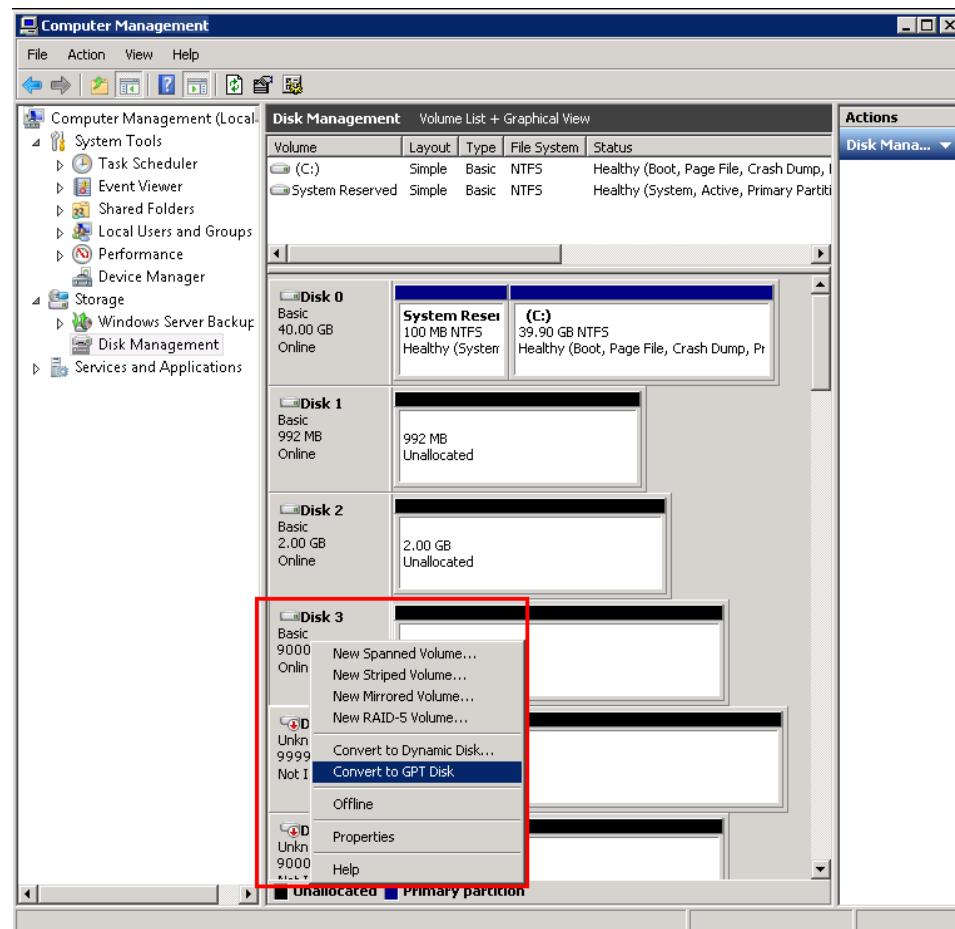
**Figure 5-60** Initializing disks

3. In the **Initialize Disk** dialog box that is displayed, select the logical disks that you want to initialize and click **OK**.

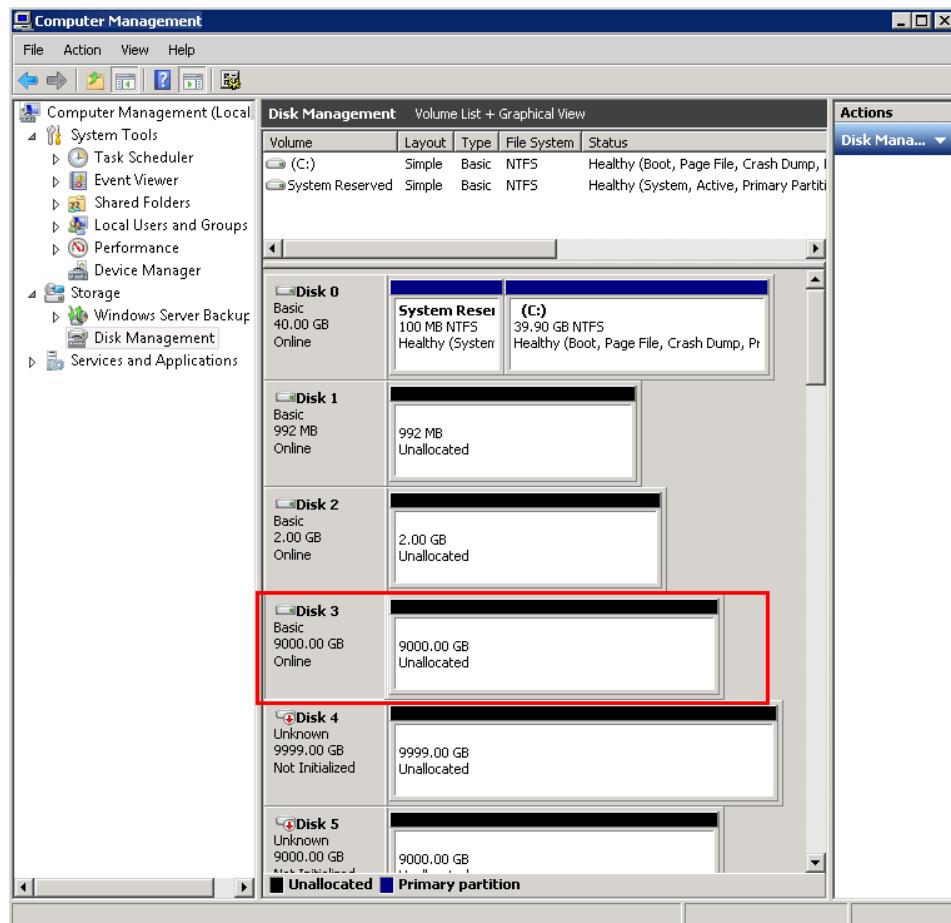
Wait about one minute. When the status of **Disk 3** becomes **Online**, the initialization is successful.

**Step 5 Optional:** If a new logical disk is larger than 2 TB, convert it into a GPT disk; otherwise, it is inaccessible.

1. Right-click **Disk 3** and choose **Convert to GPT Disk** from the shortcut menu, as shown in the red square in **Figure 5-61**.

**Figure 5-61** Converting a logical disk into a GPT disk

After a successful conversion, two partitions of a logical disk will form into one, as shown in the red square in [Figure 5-62](#).

**Figure 5-62** Successful conversion of a logical disk into a GPT disk**Step 6** Partition and format the logical disks.**NOTE**

After formatting the logical disks for the first time, do not read or write a 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

#### 5.14.3.2.2 Adding LUNs at the Application Server Side (in SUSE)

After creating LUNs and adding them to a LUN group at the storage system side, you need to perform necessary configurations at the application server side to identify and use the added storage space. Using SUSE 11.0 as an example, this section describes how to add LUNs at the application server side. 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 at the storage side.

- 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 names of the volume group and logical volume to be expanded and the file system mount directory are **thin**, **lvthin**, and **/dev/thin/lvthin** respectively.

## Procedure

### Step 1 Scan for disks on the application server.

1. Run the **upadmin show vlun** command to view the current number of LUNs. 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    0B/0B      Huawei.Storage
      1       sdc      SUSE11_LUN_02  6200bc71001faad3017fc65b00000008
Normal 50.00GB    0B/0B      Huawei.Storage
```

2. Run the **hot\_add** command to scan for disks.

3. Run the **upadmin show vlun** command to view the current number of 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    0B/0B      Huawei.Storage
      1       sdc      SUSE11_LUN_02  6200bc71001faad3017fc65b00000008
Normal 50.00GB    0B/0B      Huawei.Storage
      2       sdd      SUSE11_LUN_03  6200bc71001faad302429b1a0000000b
Normal 50.00GB    0A/0A      Huawei.Storage
```

### Step 2 Run the **pvcreate /dev/sdd** command to create a physical volume (PV).

```
# pvcreate /dev/sdd
Physical volume "/dev/sdd" successfully created
```

### Step 3 Run the **vgextend thin /dev/sdd** command to expand the volume group (VG).

```
# 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 (LV).

```
# 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

### 5.14.3.2.3 Adding LUNs at the Application Server Side (in AIX)

After creating LUNs and adding them to a LUN group at the storage system side, you need to perform necessary configurations at the application server side to identify and use the added storage space. Using AIX 6.1 as an example, this section describes how to add LUNs at the application server side. 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 at the storage side.
- 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 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 view the capacity of the volume group to be expanded whose name is **thinvg**.

**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 0B/
0B Huawei.Storage 210235G7FC10D8000001
3 2 hdisk3 aix7_LUN_002
6200BC71001FAAD300E99052000000E Available Yes 50GB 0A/
0A Huawei.Storage 210235G7FC10D8000001
4 3 hdisk4 aix7_LUN_003
6200bc71001faad301045cae000000f Available Yes 50GB 0A/
0A Huawei.Storage 210235G7FC10D8000001
```

**Step 6** Run the **extendvg thinvg hdisk4** command to expand the volume group (VG).

**Step 7** Run the **chfs -a size=+49G /thin** command to expand the file system.

----End

## 5.14.4 Expanding a File System

This section describes how a user with super administrator permissions expands storage space on DeviceManager and allocates the expanded capacity to an application server. Both automatic and manual capacity expansion modes are supported.

### Prerequisites

- The storage system is working properly.
- The size to which you want the file system to grow is determined before manual capacity expansion.
- Clone file systems and file systems with deduplication and compression enabled do not support automatic capacity expansion.

### Procedure

**Step 1** Check whether the storage pool of the file system to be expanded has sufficient free space to meet the expansion need.

1. Log in to DeviceManager.



2. Choose **Provisioning > Storage Pool**. Check the total capacity, used capacity, and free capacity of the storage pool that houses the file system to be expanded.
  - If the free capacity is sufficient, go to **Step 5**.
  - If the free capacity is insufficient, record the disk domain of the storage pool and go to **Step 2**.

**Step 2** Return to the **Provisioning** page and click **Disk Domain**. Check the total capacity, allocated capacity, and free capacity of the disk domain.

- If the free capacity meets the expansion need, go to **Step 4**.
- If the free capacity does not meet the expansion need, go to **Step 3**.

**Step 3** Expand the disk domain.

1. In the **Disk Domain** area, right-click the disk domain that you want to expand and choose **Expand**.
2. On the page for expanding the disk domain, select the type and number of disks for expansion, and ensure that the disk domain has enough free space to meet the expansion need.
  - All available disks  
All available disks can be used for expansion.
  - Specifying a disk type  
The disk type and quantity are specified for expansion.
  - Manually selecting disks  
Disks are manually selected and added for expansion.

 **NOTE**

The capacity of a disk to be added must not be smaller than the minimum capacity of existing disks in a disk domain. For example, if the disk domain contains both 600 GB and 900 GB disks, then the capacity of a disk to be added must not be smaller than 600 GB.

3. Click **OK**.

The **Success** dialog box is displayed.

4. Click **OK**.

**Step 4** Expand the storage pool.

1. In the **Storage Pool** area, select the storage pool that you want to expand and click **Modify Capacity**.
2. On the page for modifying capacity, choose **Expand capacity** and select the storage tier. In **Capacity**, enter the value of the capacity that you want to add and select the unit.
3. Click **OK**. The **Warning** dialog box is displayed. Select **I have read and understand the consequences associated with performing this operation** and click **OK**.  
The **Execution Result** dialog box is displayed.
4. Click **Close**.

**Step 5** Expand the file system.

- Manual capacity expansion

 **Provisioning > File System.**

The **File System** page is displayed.

- b. Select a file system that you want to expand, click **More**, and select **Modify Capacity**.

The **Modify File System Capacity** dialog box is displayed.

- c. Expand the file system.

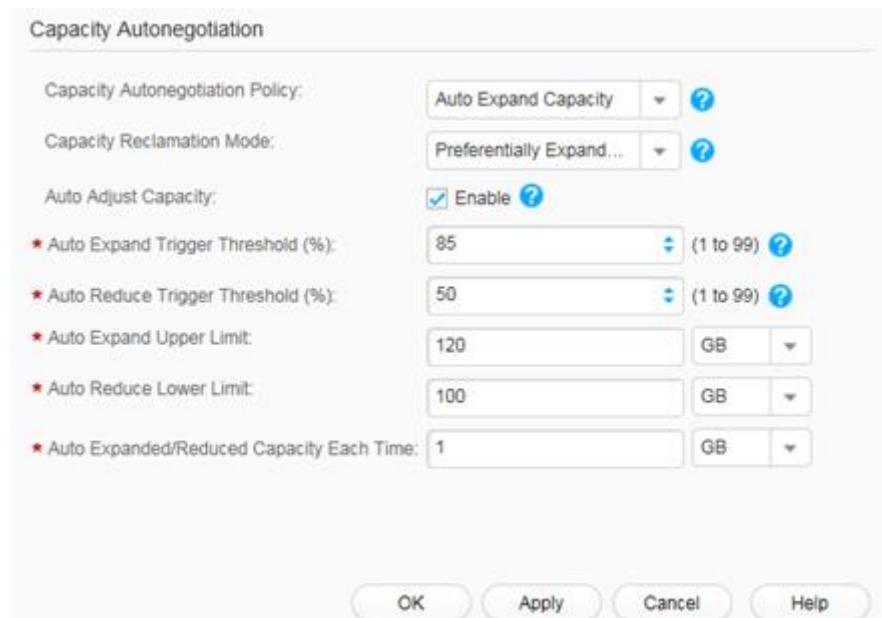
- In **Capacity of the File System Capacity** area, enter the value of the capacity to which you want the file system to expand and select the unit.

 **NOTE**

The value must be smaller than the maximum capacity.

- For a thick file system, the maximum capacity is the total of the file system capacity and the free capacity of the storage pool that houses the file system.
  - For a thin file system, the maximum capacity is the specifications limit.
- Select **Use all the free capacity of the owning storage pool for expansion**.
- a. Click **OK**.
- The **Execution Result** dialog box is displayed.
- b. Click **Close**. The file system is expanded.
- Automatic capacity expansion
-  **NOTE**
- Enable the automatic capacity expansion function for the file system. Then, the storage system checks the available capacity of the file system at an interval of 20 seconds. If the system detects that the available capacity reaches the threshold for triggering automatic capacity expansion, it automatically deletes snapshots or expands the file system based on the user-defined policy.
- 
1. Choose  **Provisioning > File System.**
- Issue 07 (2018-07-30)
- Copyright © Huawei Technologies Co., Ltd.
- 371

- The **File System** page is displayed.
2. Select the file system for which you want to set the capacity autonegotiation policy and click **Properties**.
- The **File System Properties** dialog box is displayed.
3. Choose **More > Advanced**.
- The **Capacity Autonegotiation** dialog box is displayed.
4. In **Capacity Autonegotiation Policy**, select **Auto Expand Capacity** or **Auto Reduce or Expand Capacity** and set capacity autonegotiation parameters, as described in [Table 5-34](#).



**Table 5-34** Capacity autonegotiation parameters

Parameter	Description	Value
Capacity Autonegotiation Policy	<p>The following capacity autonegotiation policies are available:</p> <ul style="list-style-type: none"><li>- <b>Not Use Capacity</b> <b>Autonegotiation:</b> The storage capacity used by a file system is fixed and is not flexibly adjusted by the storage system.</li><li>- <b>Auto Expand Capacity:</b> 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.</li><li>- <b>Auto Reduce or Expand Capacity:</b> 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 triggered 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 for data writes.</li></ul>	[Example] Auto Expand Capacity

Parameter	Description	Value
Capacity Reclamation Mode	<p>The following capacity reclamation modes are available:</p> <ul style="list-style-type: none"><li>- <b>Preferentially Expand Capacity:</b> Expand the file system capacity.</li><li>- <b>Preferentially Delete Old Snapshot:</b> Delete old snapshots to reclaim space for increasing the file system capacity. If HyperReplication and HyperMetro are configured for storage systems, the capacity autonegotiation policy of the primary storage system will be synchronized to the secondary storage system. If <b>Preferentially Delete Old Snapshot</b> is adopted, ensure that <b>Delete Obsolete Read-Only Snapshots</b> is enabled for the secondary storage system.</li></ul>	[Example] Preferentially Expand Capacity
Auto Adjust Capacity	After you select <b>Auto Adjust Capacity</b> , the automatic capacity expansion or shrinking policy for a file system will take effect during the service running.	[Example] Enable
Auto Expand Trigger Threshold (%)	When the ratio of the used capacity to the total capacity of the file system is greater than the preset value, the storage system automatically triggers file system capacity expansion.	[Value range] The value is an integer ranging from 1 to 99. [Example] 85
Auto Reduce Trigger Threshold (%)	When the ratio of the used capacity to the total capacity of the file system is smaller than the preset value, the storage system automatically triggers file system space reclamation and reduces file system capacity.	[Value range] The value is an integer ranging from 1 to 99. [Example] 50
Auto Expand Upper Limit	Set the upper limit for automatic expansion.	[Value range] File system capacity to 16 PB. [Example] 120 GB

Parameter	Description	Value
Auto Reduce Lower Limit	Set the lower limit for automatic shrinking.	[Value range] 1 GB to <b>Auto Expand Upper Limit</b> . [Example] 100 GB
Auto Expanded/ Reduced Capacity Each Time	Set the capacity to be expanded or shrunk for each time.	[Value range] 64 MB to 100 GB. [Example] 1 GB

5. Click **OK**.

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

----End

## Follow-up Procedure

Verify and use the expanded storage space.

On the **File System** page, click the newly expanded file system and view its **Total Capacity**. If the capacity is expanded to the correct value, the capacity expansion is successful. If the capacity expansion is unsuccessful, troubleshoot the fault based on alarm information.

## 5.14.5 Shrinking a File System

This section describes how a user with super administrator permissions shrinks storage space on DeviceManager. Both automatic and manual capacity shrinking modes are supported.

### Prerequisites

- The storage system is working properly.
- The size to which you want the file system to shrink is determined before manual capacity shrinking.
- Clone file systems and file systems with deduplication and compression enabled do not support automatic capacity shrinking.

### Procedure

**Step 1** Log in to DeviceManager.

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

The **File System** page is displayed.

**Step 3** Shrink the file system.

- Manual capacity shrinking

- a. Select a file system that you want to shrink, click **More**, and select **Modify Capacity**.

The **Modify File System Capacity** dialog box is displayed.

- b. In **Capacity** of the **File System Capacity** area, enter the value of the capacity to which you want the file system to shrink and select the unit.

 **NOTE**

The value must be greater than or equal to the minimum capacity. For a thick file system, the minimum capacity is the total of the reserved capacity (mainly for snapshots) and the used capacity of the file system.

- c. Click **OK**.

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

- d. Click **Close**. The file system is shrunk.

● Automatic capacity shrinking

 **NOTE**

Enable the automatic shrinking function for the file system. Then, the storage system checks the available capacity of the file system at an interval of 20 seconds. If the system detects that the available capacity reaches the threshold for triggering automatic capacity shrinking, it automatically shrinks the file system.



- a. Choose  **Provisioning > File System**.

The **File System** page is displayed.

- b. Select the file system for which you want to set the capacity autonegotiation policy and click **Properties**.

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

- c. Choose **More > Advanced**.

The **Capacity Autonegotiation** dialog box is displayed.

- d. In **Capacity Autonegotiation Policy**, select **Auto Reduce or Expand Capacity** and set capacity autonegotiation parameters, as described in [Table 5-35](#).

The screenshot shows the **Capacity Autonegotiation** dialog box. It includes fields for **Capacity Autonegotiation Policy** (set to **Auto Reduce or Expand...**), **Capacity Reclamation Mode** (set to **Preferentially Expand...**), and **Auto Adjust Capacity** (with **Enable** checked). There are also fields for **Auto Expand Trigger Threshold (%)** (85), **Auto Reduce Trigger Threshold (%)** (50), **Auto Expand Upper Limit** (120 GB), **Auto Reduce Lower Limit** (100 GB), and **Auto Expanded/Reduced Capacity Each Time** (1 GB). At the bottom are buttons for **OK**, **Apply**, **Cancel**, and **Help**.

**Table 5-35** Capacity autonegotiation parameters

Parameter	Description	Value
Capacity Autonegotiation Policy	<p>The following capacity autonegotiation policies are available:</p> <ul style="list-style-type: none"><li>■ <b>Not Use Capacity</b> <b>Autonegotiation:</b> The storage capacity used by a file system is fixed and is not flexibly adjusted by the storage system.</li><li>■ <b>Auto Expand Capacity:</b> 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.</li><li>■ <b>Auto Reduce or Expand Capacity:</b> 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 triggered 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 for data writes.</li></ul>	[Example] Auto Reduce or Expand Capacity

Parameter	Description	Value
Capacity Reclamation Mode	<p>The following capacity reclamation modes are available:</p> <ul style="list-style-type: none"><li>■ <b>Preferentially Expand Capacity:</b> Expand the capacity to increase the file system capacity.</li><li>■ <b>Preferentially Delete Old Snapshot:</b> Delete old snapshots to reclaim space for increasing the file system capacity. If HyperReplication and HyperMetro are configured for storage systems, the capacity autonegotiation policy of the primary storage system will be synchronized to the secondary storage system. If <b>Preferentially Delete Old Snapshot</b> is adopted, ensure that <b>Delete Obsolete Read-Only Snapshots</b> is enabled for the secondary storage system.</li></ul>	[Example] Preferentially Expand Capacity
Auto Adjust Capacity	After you select <b>Auto Adjust Capacity</b> , the automatic capacity expansion or shrinking policy for a file system will take effect during the service running.	[Example] Enable
Auto Expand Trigger Threshold (%)	When the ratio of the used capacity to the total capacity of the file system is greater than the preset value, the storage system automatically triggers file system capacity expansion.	[Value range] The value is an integer ranging from 1 to 99. [Example] 85
Auto Reduce Trigger Threshold (%)	When the ratio of the used capacity to the total capacity of the file system is smaller than the preset value, the storage system automatically triggers file system space reclamation and reduces file system capacity.	[Value range] The value is an integer ranging from 1 to 99. [Example] 50

Parameter	Description	Value
Auto Expand Upper Limit	Set the upper limit for automatic expansion.	[Value range] File system capacity to 16 PB.  [Example] 120 GB
Auto Reduce Lower Limit	Set the lower limit for automatic shrinking.	[Value range] 1 GB to <b>Auto Expand Upper Limit</b> .  [Example] 100 GB
Auto Expanded/ Reduced Capacity Each Time	Set the capacity to be expanded or shrunk for each time.	[Value range] 64 MB to 100 GB.  [Example] 1 GB

- e. Click **OK**.

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

----End

## Follow-up Procedure

Verify and use the storage space.

On the **File System** page, click the shrunk file system and view its **Total Capacity**. If the capacity is shrunk to the correct value, the capacity shrinking is successful. If the capacity shrinking is unsuccessful, troubleshoot the fault based on alarm information.

## 5.14.6 Emergency Rollback Procedure

### 5.14.6.1 Emergency Rollback Procedure (in 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 operations such as reclaiming the added LUNs, WWNs, and ports and 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 expanding capacity by adding LUNs.

- This section uses Windows Server 2008 as an example to show the rollback procedure on Windows-based application servers.

## Procedure

**Step 1 Optional:** Reclaim new LUNs from an 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 **lun\_group\_id** and **lun\_id\_list** respectively.
3. Run the **show lun\_group lun** command to view LUNs contained in the LUN group. Specify the LUN group using **lun\_group\_id**.  
The LUN group does not contain the new LUNs.

**Step 2 Optional:** Reclaim new WWNs from an 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**.  
The information does not contain the new initiator information.

**Step 3 Optional:** Reclaim new ports from an 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 **port\_group\_id**, **port\_type**, and **port\_id\_list** 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 **port\_group\_id**.  
The port group does not contain the new ports.

**Step 4** Scan for disks on the application server.

1. As an administrator, log in to the Windows Server 2008 application server.
2. On the desktop, click **Start** and choose **Administrative Tools > Server Manager** from the shortcut menu.  
The **Server Manager** dialog box is displayed.
3. On the left navigation bar of the **Server Manager** dialog box, right-click **Disk Management** and choose **Rescan Disks** from the shortcut menu.
4. In UltraPath's CLI of the application server, run the **upadm show vln** and **upadm show path** commands to view the device information about UltraPath.  
The command outputs do not contain information about the added disks.

**Step 5** Check the host'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

### 5.14.6.2 Emergency Rollback Procedure (in 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 operations such as reclaiming the added LUNs, WWNs, and ports and 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 expanding capacity by adding LUNs.

#### Procedure

**Step 1 Optional:** Reclaim new LUNs from an 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 **lun\_group\_id** and **lun\_id\_list** respectively.
3. Run the **show lun\_group lun** command to view LUNs contained in the LUN group. Specify the LUN group using **lun\_group\_id**.  
The LUN group does not contain the new LUNs.

**Step 2 Optional:** Reclaim new WWNs from an 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 **host\_id**.  
The information does not contain the new initiator information.

**Step 3 Optional:** Reclaim new ports from an 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 **port\_group\_id**, **port\_type**, and **port\_id\_list** 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 **port\_group\_id**.  
The port group does not contain the new ports.

**Step 4** Scan for disks on the application server.

1. Run the **hot\_add** command to rescan for disks.
2. Run the **upadmin show vlun** and **upadmin show path** commands to view the device information about UltraPath.
3. Run the **fdisk -l** command to view the disk information about the host.

The command outputs in [Step 4.2](#) and [Step 4.3](#) do not contain information about the added 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

### 5.14.6.3 Emergency Rollback Procedure (in 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 operations such as reclaiming the added LUNs, WWNs, and ports and 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 expanding capacity 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.  
**hdiskX** 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 an 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 **lun\_group\_id** and **lun\_id\_list** respectively.
3. Run the **show lun\_group lun** command to view LUNs contained in the LUN group.  
Specify the LUN group using **lun\_group\_id**.

The LUN group does not contain the new LUNs.

**Step 3 Optional:** Reclaim new WWNs from an 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 **host\_id**.

The information does not contain the new initiator information.

**Step 4 Optional:** Reclaim new ports from an 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 **port\_group\_id**, **port\_type**, and **port\_id\_list** 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 **port\_group\_id**.

The port group does not contain the new ports.

**Step 5** Scan for disks on the application server.

1. Run the **cfgmgr** command to rescan for disks.
2. Run the **upadm show v lun** and **upadm show path** commands to view the device information about UltraPath.
3. Run the **fdisk -l** command to view the disk information about the host.

The command outputs in **Step 5.2** and **Step 5.3** do not contain information about the added disks.

**Step 6** Check the host's running status after the rollback.

1. Run the **erpt** 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

#### 5.14.6.4 Emergency Rollback Procedure (in 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 operations such as reclaiming the added LUNs, WWNs, and ports and scanning for disks on the application server.

#### Context

The method to reclaim new LUNs described in this section is for expanding capacity by adding LUNs.

#### Procedure

**Step 1 Optional:** Reclaim new LUNs from an 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 **lun\_group\_id** and **lun\_id\_list** respectively.
3. Run the **show lun\_group lun** command to view LUNs contained in the LUN group. Specify the LUN group using **lun\_group\_id**.  
The LUN group does not contain the new LUNs.

**Step 2 Optional:** Reclaim new WWNs from an 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 **host\_id**.  
The information does not contain the new initiator information.

**Step 3 Optional:** Reclaim new ports from an 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 **port\_group\_id**, **port\_type**, and **port\_id\_list** 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 **port\_group\_id**.  
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

# 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 Query the Mapping Between Host Disks and LUNs When the UltraPath Software Is Not Installed?](#)

[6.2 How Can I Modify the Outdated Password for Default User Maintainer of the SVP's Windows VM?](#)

[6.3 How Can I Expand the Capacity of a LUN Used in the HyperMetro Feature? \(Applicable to V300R006C00/C10\)](#)

[6.4 How Can I Expand the Capacity of a LUN Used in the HyperMetro Feature? \(Applicable to V300R006C20 and Later\)](#)

[6.5 How Can I Expand the Capacity of a LUN Used in a Remote Replication Pair? \(Applicable to V300R006C00/C10\)](#)

[6.6 How Can I Expand the Capacity of a LUN Used in a Remote Replication Pair? \(Applicable to V300R006C20 and Later\)](#)

[6.7 How Can I Use Self-Signed Certificates to Fix the Privacy Error Displayed When I Attempt to Log In to DeviceManager?](#)

## 6.1 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 a LUN mapped to the host.

1. Log in to the command-line interface (CLI) of the storage system as the 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 WWNs 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 the 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.

- 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.

- 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 WWNs 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 ID of the LUN mapped to the host.

- Log in to the command-line interface (CLI) of the storage system as the super administrator.
- 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.

- 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.

- Run the **lsdev -Cc disk** command to query scanned disk information.
- Run the **lsattr -El hdiskX** command to query the information about disk **hdskx**. 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 the 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 the 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.

```
-bash-3.2# echo | format
Searching for disks...done

AVAILABLE DISK SELECTIONS:
  0. c1t0d0 <SUN146G cyl 14087 alt 2 hd 24 sec 848>
    /pci@0/pci@0/pci@2/scsi@0/sd@0,0
  1. c2t20000022a109c6ce01 <HUAWEI-S2600T-4202 cyl 1090 alt 2 hd 38 sec 64>
    /pci@0/pci@0/pci@0/pci@0/pci@a/QLGC,qlc@0/Fp@0,0/ssd@w20000022a109c6ce,1
  2. c2t20000022a109c6ce02 <HUAWEI-S2600T-4202 cyl 2182 alt 2 hd 38 sec 64>
    /pci@0/pci@0/pci@0/pci@0/pci@a/QLGC,qlc@0/Fp@0,0/ssd@w20000022a109c6ce,2
  3. c2t20000022a109c6ce03 <HUAWEI-S2600T-4202 cyl 10920 alt 2 hd 38 sec 64>
    /pci@0/pci@0/pci@0/pci@0/pci@a/QLGC,qlc@0/Fp@0,0/ssd@w20000022a109c6ce,3
  4. c2t20000022a109c6ce04 <HUAWEI-S2600T-4202 cyl 6398 alt 2 hd 64 sec 256>
    /pci@0/pci@0/pci@0/pci@0/pci@a/QLGC,qlc@0/Fp@0,0/ssd@w20000022a109c6ce,4
  5. c2t20000022a109c6ce05 <HUAWEI-S2600T-4202 cyl 10920 alt 2 hd 38 sec 64>
    /pci@0/pci@0/pci@0/pci@0/pci@a/QLGC,qlc@0/Fp@0,0/ssd@w20000022a109c6ce,5
  6. c2t20000022a109c6ce06 <HUAWEI-S2600T-4202 cyl 6398 alt 2 hd 64 sec 256>
    /pci@0/pci@0/pci@0/pci@0/pci@a/QLGC,qlc@0/Fp@0,0/ssd@w20000022a109c6ce,6
  7. c2t20000022a109c6ce07 <HUAWEI-S2600T-4202 cyl 21843 alt 2 hd 38 sec 64>
    /pci@0/pci@0/pci@0/pci@0/pci@a/QLGC,qlc@0/Fp@0,0/ssd@w20000022a109c6ce,7
  8. c2t20000022a109c6ce08 <HUAWEI-S2600T-4202 cyl 12798 alt 2 hd 64 sec 256>
    /pci@0/pci@0/pci@0/pci@0/pci@a/QLGC,qlc@0/Fp@0,0/ssd@w20000022a109c6ce,8
```

**Step 3** On DeviceManager, view the host LUN ID of the LUN mapped to the host.

1. Log in to DeviceManager.

2. Choose  Provisioning >  Host.
3. Choose the host queried in Step 1, 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

## 6.2 How Can I Modify the Outdated Password for Default User Maintainer of the SVP's Windows VM?

### Question

You cannot log in to a normal storage system from a remote desktop if the password for default user **maintainer** of the Windows VM is outdated. In this case, how do you modify the password for user **maintainer** so that you can log into the storage system using the new password?

### Answer

If the KVM is configured, perform the following:

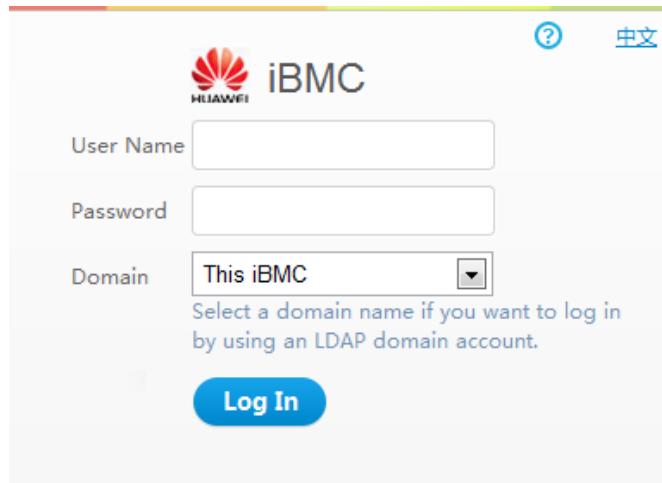
1. Start the KVM.
2. Go to the login page of the Windows operating system built in the SVP.
  - a. Use the **svp\_user** account and its password to log in to the host where SVP resides.
  - b. On the host desktop, choose **Applications > System > Terminal > Xterm**.
  - c. In the command window that is displayed, run **vncviewer -fullscreen 127.0.0.1:1**.  
Go to the login page of the Windows operating system built in the SVP.
3. Modify the password for user **maintainer**.
  - a. Type **maintainer** and the existing password, and press **Enter**.
  - b. The system prompts that the password is outdated and you need to modify it. Press **OK**.
  - c. On the page that is displayed, type the new password and type it again. Then press **Enter**.
  - d. A message indicating that the password has been changed is displayed. Click **OK**.  
The password is modified successfully. You can use the new password to log in to Windows VMs remotely.

If the KVM is not configured, perform the following:

1. Log in to the iBMC system.
  - a. Run a web browser on your maintenance terminal.
  - b. In the address box, type **https://xxx.xxx.xxx.xxx** and press **Enter**. In the address, **xxx.xxx.xxx.xxx** indicates the IP address of the Mgmt management network port used to manage the SVP. The default IP address is **192.168.2.100**.

Log in to the iBMC login page, as shown in [Figure 6-1](#).

**Figure 6-1** iBMC login page



- c. On the iBMC login page, type the user name and password. By default, the user name is **root** and the password is **Huawei12#%**.

 **NOTE**

Your user name will be locked after five consecutive failures to log in with wrong passwords. Log in again five minutes later.

- d. In the **Domain** drop-down list box, select **This iBMC**.
  - e. Click **Log In**.  
The **Information Summary** page is displayed.
2. Go to the login page of the Windows operating system built in the SVP.
    - a. Choose **Remote > Remote Connection**.
    - b. Click **Remote Virtual Console (Shared Mode)** or **Remote Virtual Console (Private Mode)**.  
Go to the interface for logging in to the host where SVP resides.
    - c. Use the **svp\_user** account and its password to log in to the host where SVP resides.
    - d. On the host desktop, choose **Applications > System > Terminal > Xterm**.
    - e. In the command window that is displayed, run **vncviewer -fullscreen 127.0.0.1:1**.  
Go to the login page of the Windows operating system built in the SVP.
  3. Modify the password for user **maintainer**.
    - a. Type **maintainer** and the existing password, and press **Enter**.
    - b. The system prompts that the password is outdated and you need to modify it. Press **OK**.
    - c. On the page that is displayed, type the new password and type it again. Then press **Enter**.
    - d. A message indicating that the password has been changed is displayed. Click **OK**.  
The password is modified successfully. You can use the new password to log in to Windows VMs remotely.

## 6.3 How Can I Expand the Capacity of a LUN Used in the HyperMetro Feature? (Applicable to V300R006C00/C10)

### Question

How can I expand the capacity of a LUN used in HyperMetro?

### Answer

Before expanding the capacities of HyperMetro LUNs, you must delete the HyperMetro pair where the LUNs reside. The following describes how to expand the capacities of HyperMetro LUNs.

#### NOTE

The primary LUN refers to the one that provides services, whereas the secondary LUN refers to the one that stops providing services.

- Use offline expansion if the CPU usage and disk usage exceed 50%, the HyperMetro replication bandwidth is insufficient, or the distance between data centers exceeds 25 km.
  - a. Stop upper-layer services.
  - b. Remove the primary and secondary LUNs from their owning LUN groups.
  - c. Pause the HyperMetro pair.

- d. Delete the HyperMetro pair.
- e. Expand the capacities of the primary and secondary LUNs.

 **NOTE**

The primary and secondary LUNs must have the same capacity after expansion.

- f. Re-create the HyperMetro pair using the primary and secondary LUNs.

 **NOTE**

- Select **The data at the local and remote ends is consistent. Synchronization is not required after the creation is complete.**
- To ensure that the data synchronization direction of the HyperMetro pair remains unchanged after the expansion, you must create the HyperMetro pair on the same storage array on which you created the original HyperMetro pair before the expansion. For example, if you created the HyperMetro pair on the storage array at the preferred site before capacity expansion, create it again on the storage array at the preferred site after capacity expansion.

- g. Add the primary and secondary LUNs to the original LUN groups.
- h. On the host, scan for LUNs.
- i. Restart services.

 **NOTE**

For details about how to remove/add the primary and secondary LUNs from/to their owning LUN groups, and pause, delete, or create the HyperMetro pair, see *HyperMetro Feature Guide*.

- Use online expansion if the CPU usage and disk usage are less than 50%, the HyperMetro replication bandwidth is sufficient, or the distance between data centers is within 25 km.
  - a. Pause the HyperMetro pair.

 **NOTE**

In the **Pause HyperMetro Pair** dialog box, select **Non-Preferred**.

- b. Remove the secondary LUN from its owning LUN group.
- c. Delete the HyperMetro pair.
- d. Expand the capacities of the primary and secondary LUNs.

 **NOTE**

The primary and secondary LUNs must have the same capacity after expansion.

- e. On the storage array of the preferred site, create a HyperMetro pair using the primary and secondary LUNs.

 **NOTE**

Select **Local and remote data is inconsistent. After the creation is complete, data is automatically synchronized.**

- f. Add the secondary LUNs to the original LUN group.
- g. On the host, scan for LUNs.

 **NOTE**

For details about how to remove/add the secondary LUN from/to its owning LUN group, and pause, delete, or create the HyperMetro pair, see *HyperMetro Feature Guide*.

## 6.4 How Can I Expand the Capacity of a LUN Used in the HyperMetro Feature? (Applicable to V300R006C20 and Later)

### Question

How can I expand the capacity of a LUN used in HyperMetro?

### Answer

To expand the capacity of HyperMetro LUNs, perform the following operations:

 **NOTE**

The primary LUN refers to the one that provides services, whereas the secondary LUN refers to the one that stops providing services.

1. Pause the HyperMetro pair.
2. Expand the capacities of the primary and secondary LUNs.

 **NOTE**

The primary and secondary LUNs must have the same capacity after expansion.

3. On the host, scan for LUNs.
4. Manually synchronize the HyperMetro pair.

 **NOTE**

For details about how to pause and synchronize the HyperMetro pair, see *HyperMetro Feature Guide*.

## 6.5 How Can I Expand the Capacity of a LUN Used in a Remote Replication Pair? (Applicable to V300R006C00/C10)

### Question

How can I expand the capacity of a LUN used in a remote replication pair?

### Answer

To perform LUN capacity expansion in the remote replication feature, you must delete the remote replication pair.

1. Split the remote replication pair.

If the remote replication pair has been added to a consistency group, perform the following:

- a. Split the remote replication consistency group.
- b. Remove the remote replication pair.

 **NOTE**

After the remote replication pair is removed, the remote replication consistency group is in split state. Synchronize the remote replication consistency group manually to avoid data inconsistency between the primary and secondary ends.

2. Remove the remote replication pair.

 **NOTE**

If you remove the remote replication pair in an asynchronous remote replication scenario, do not select **Forcibly ensure data consistency for the secondary resource**; otherwise, the operation will trigger a rollback if the pair being synchronized is split and the secondary LUN cannot be expanded during the rollback.

3. Perform capacity expansion for the primary LUN and the secondary LUN respectively.

 **NOTE**

The primary LUN and the secondary LUN should have the same capacity after the expansion.

4. Select the primary LUN and the secondary LUN after expansion to rebuild a remote replication pair.

 **NOTE**

- When creating a remote replication pair, set **Initial Synchronization to Data is inconsistent between the primary and secondary resources. After the remote replication task is created, manually perform data synchronization**.
- If a remote replication pair is in a consistency group before the capacity expansion, add it to the consistency group again.

5. Scan the primary LUN on the host.

6. Synchronize the remote replication manually.

 **NOTE**

For details about how to split the remote replication pair, delete the remote replication pair, create a new remote replication pair and manually start synchronization for the remote replication pair, see *HyperReplication Feature Guide*.

## 6.6 How Can I Expand the Capacity of a LUN Used in a Remote Replication Pair? (Applicable to V300R006C20 and Later)

### Question

How can I expand the capacity of a LUN used in a remote replication pair?

### Answer

1. Split the remote replication pair.

 **NOTE**

If the remote replication pair for which you want to perform capacity expansion has been added to a consistency group, split the consistency group first and synchronize the consistency group manually after the capacity expansion.

2. Expand the capacity of the primary LUN and the secondary LUN respectively.

 **NOTE**

The primary and secondary LUNs must have the same capacity after expansion.

3. Scan the primary LUN on the host.
4. Start the remote replication pair synchronization manually.

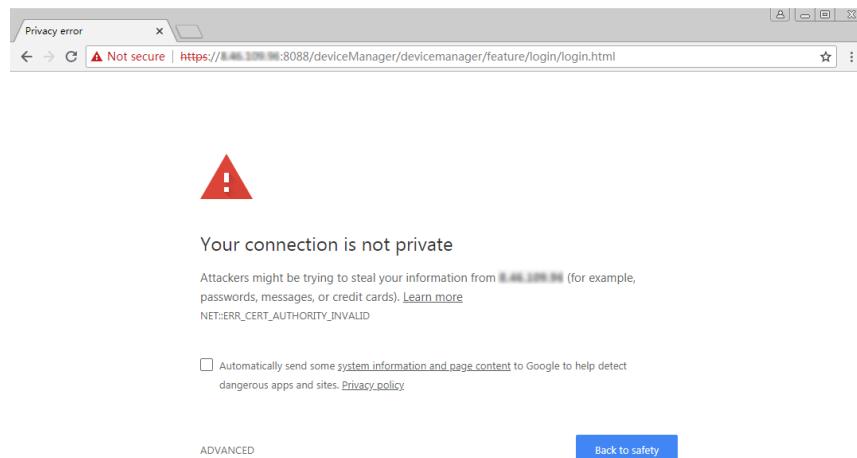
 **NOTE**

For details about how to split the remote replication pair and manually start synchronization for the remote replication pair, see *HyperReplication Feature Guide*.

## 6.7 How Can I Use Self-Signed Certificates to Fix the Privacy Error Displayed When I Attempt to Log In to DeviceManager?

### Question

How can I use self-signed certificates to fix the privacy error displayed when I attempt to log in to DeviceManager?



### Answer

You can replace the default security certificates of the DeviceManager server and user browser with self-signed security certificates and private key files to eliminate the privacy error displayed when you log in to DeviceManager. The configuration procedure is as follows:

**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 0.9.8j or later.  

```
CTU1000047802:~ # openssl version
OpenSSL 0.9.8j-fips 07 Jan 2009
```
2. Run the **find / -name openssl.cnf** command to identify the location of the **openssl.cnf** file.

Generally, the **openssl.cnf** file is under **/etc/ssl**.

```
CTU1000047802:/ # cd /etc/ssl
CTU1000047802:/etc/ssl # ls
```

```
ca.key ca.pem cacert.pem cert.csr certs demoCA openssl.cnf private  
private.key
```

3. Open the **openssl.cnf** file and check the default CA directory.

```
CTU1000047802:/etc/ssl # cat openssl.cnf
```

```
[ CA_default ]  
  
dir = ./demoCA  
certs = $dir/certs  
crl_dir = $dir/crl  
database = $dir/index.txt  
unique_subject = no  
new_certs_dir = $dir/newcerts  
  
# Where everything is kept  
# Where the issued certs are kept  
# Where the issued crl are kept  
# database index file.  
# Set to 'no' to allow creation of  
# several certificates with same subject.  
# default place for new certs.
```

4. Add the **subjectAltName** option to [v3\_req] in the **openssl.cnf** file.

The IP address is the management IP address of the storage system, XX.XX.109.96 in this example.

```
[ v3_req ]  
  
# Extensions to add to a certificate request  
  
basicConstraints = CA:FALSE  
keyUsage = nonRepudiation, digitalSignature, keyEncipherment  
subjectAltName = IP:XX.XX.109.96  
[ v3_ca ]
```

## Step 2 Use the OpenSSL tool to generate CA private key and CA certificate files.

1. Create directories and files related to certificate files.

```
CTU1000047802:/ # mkdir new9  
CTU1000047802:/ # cd new9  
CTU1000047802:/new9 # mkdir demoCA  
CTU1000047802:/new9 # mkdir demoCA/csr demoCA/private demoCA/jks demoCA/  
newcerts  
CTU1000047802:/new9 # touch demoCA/index.txt  
CTU1000047802:/new9 # echo 03 > ./demoCA/serial
```

2. Generate a CA private key file.

```
CTU1000047802:/new9 # openssl genrsa -out ./demoCA/private/ca.key 1024  
Generating RSA private key, 1024 bit long modulus  
.....+++++  
.....+++++  
e is 65537 (0x10001)
```

3. Generate a CA certificate file.

```
CTU1000047802:/new9 # openssl req -new -x509 -sha256 -extensions v3_ca -key ./  
demoCA/private/ca.key -out ./demoCA/newcerts/RootCA.crt -subj '/C=CN/  
ST=SiChuan/O=Huawei/L=ChengDu/CN=*.*.*/OU=IT Product Line' -days 5475
```

**CN** is the common name for the CA certificate. To avoid certificate alarms, set this parameter to **\*.\*.\*.**.

## Step 3 Generate certificate files for the DeviceManager server.

1. Generate a key file.

```
CTU1000047802:/new9 # openssl genrsa -out ./demoCA/private/  
deviceManager_key.pem 2048  
Generating RSA private key, 2048 bit long modulus  
.....++  
.....+++++  
e is 65537 (0x10001)
```

2. Generate a certificate request file.

```
CTU1000047802:/new9 # openssl req -new -sha256 -extensions v3_req -key ./  
demoCA/private/deviceManager_key.pem -out ./demoCA/csr/deviceManager.csr -  
subj '/C=CN/ST=SiChuan/O=Huawei/L=ChengDu/CN=XX.XX.109.96/OU=IT Product Line'  
-days 3650
```

**CN** is the common name for the DeviceManager server certificate. To avoid certificate alarms, set this parameter to the management IP address of the storage system, XX.XX.109.96 in this example.

3. Use the CA certificate to sign the key.

```
CTU1000047802:/new9 # openssl ca -batch -in ./demoCA/csr/deviceManager.csr -cert ./demoCA/newcerts/RootCA.crt -keyfile ./demoCA/private/ca.key -out ./demoCA/newcerts/deviceManager_cert.pem -days 3650 -md sha256 -extensions v3_req
Using configuration from /etc/ssl/openssl.cnf
Check that the request matches the signature
Signature ok
Certificate Details:
    Serial Number: 3 (0x3)
    Validity
        Not Before: Jul 30 02:42:35 2018 GMT
        Not After : Jul 27 02:42:35 2028 GMT
    Subject:
        countryName          = CN
        stateOrProvinceName = SiChuan
        organizationName    = Huawei
        organizationalUnitName = IT Product Line
        commonName           = XX.XX.109.96
    X509v3 extensions:
        X509v3 Basic Constraints:
            CA:FALSE
        X509v3 Key Usage:
            Digital Signature, Non Repudiation, Key Encipherment
        X509v3 Subject Alternative Name:
            IP Address:XX.XX.109.96
Certificate is to be certified until Jul 27 02:42:35 2028 GMT (3650 days)
Write out database with 1 new entries
Data Base Updated
```

**Step 4** Replace certificates.

1. Use an FTP tool (such as FileZilla) to connect to the Linux environment where the OpenSSL tool is located and export the generated certificates and key file to the local PC.
  - RootCA.crt
  - deviceManager\_cert.pem
  - deviceManager\_key.pem

 **NOTE**

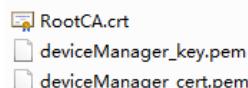
- The **RootCA.crt** and **deviceManager\_cert.pem** files are stored in the **newcerts** folder.

```
CTU1000047802:/new9/demoCA/newcerts # ls
03.pem  RootCA.crt  deviceManager_cert.pem
```

- The **deviceManager\_key.pem** file is stored in the **private** folder.

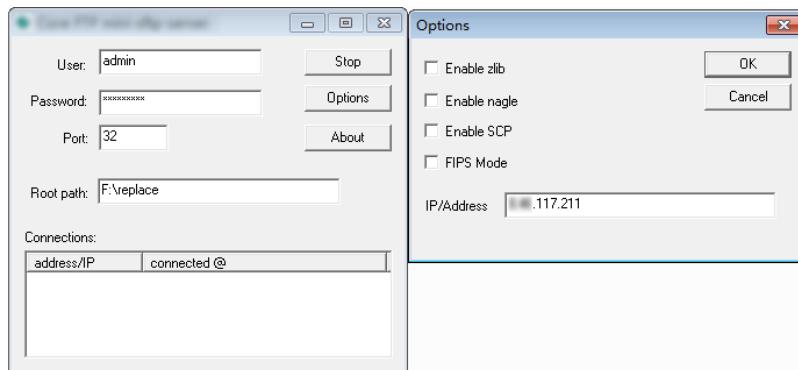
```
CTU1000047802:/new9/demoCA/private # ls
ca.key  deviceManager_key.pem
```

In this example, the three files are exported to **F:\replace**.



2. Use an FTP server tool to share the three exported files.

Specify the user, password, and port number of the FTP server. Set the share path to the directory where the three exported files are saved, **F:\replace** in this example. Set the IP address to the IP address of the local computer, XX.XX.117.211 in this example.



### 3. Import the generated self-signed certificates to the storage system.

Log in to the storage system using the CLI. Run the **import ssl\_certificate** command to import the shared certificate and key files, **deviceManager\_cert.pem** and **deviceManager\_key.pem** in this example.

```
admin:/>import ssl_certificate ip=XX.XX.117.211 user=admin password=*****
cert_file=deviceManager_cert.pem key_file=deviceManager_key.pem port=32
protocol=SFTP
DANGER: You are about to use an unencrypted SSL certificate to replace the
current SSL certificate. Security risks may exist in the unencrypted
certificate. This operation will cause DeviceManager automatically to
restart, interrupting services. The certificate you are about to import has
the following security risks: a certificate loading error (the certificate
fails to be loaded, the certificate key fails to be obtained, certificate
public information fails to be obtained, the certificate signature algorithm
fails to be obtained).
Suggestion:
1. Use an encrypted certificate to replace the current certificate.
2. Before running the command, confirm that you want to replace the SSL
certificate.
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. Restart DeviceManager.

```
admin:/>change user_mode current_mode user_mode=developer
DANGER: You are about to switch to the developer view. Commands in this view
must be run under the guidance of R&D engineers. You can choose whether to
run this command. If you run this command to switch to the developer view, it
means that you know risks of running commands in the developer view. Device
vendors are not responsible for any loss or damage caused to the user or
others by running commands in the developer view.
1. Running the command in the developer view may cause system reset, restart,
offline, service interruption, data loss, and data inconsistency.
2. Running the command in the developer view may cause the performance to
decrease.
3. Running the command in the developer view to delete or remove
configurations may have impact on the service and data.
4. Running the command in the developer view may cause system alarms.
Suggestion: Run this command under the guidance of R&D engineers.
Have you read danger alert message carefully?(y/n)y
Are you sure you really want to perform the operation?(y/n)y
developer:/>reboot ism
DANGER: You are about to restart the DeviceManager for the storage system.
This operation causes the DeviceManager unavailable temporarily.
Suggestion: Before performing this operation, ensure that all users have exit
the DeviceManager.
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.
```

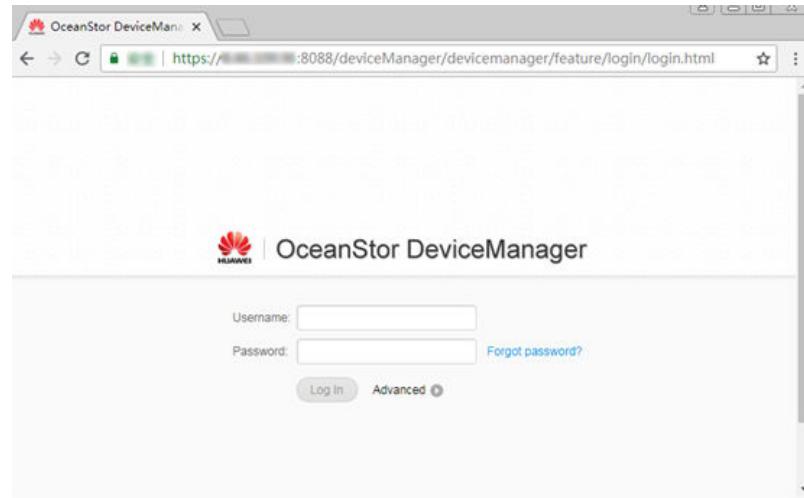
### 5. Import the certificate file to the browser.

The following uses Google Chrome (67.0) as an example.

 **NOTE**

For details about how to replace the security certificates of other browsers, see section "Importing a Security Certificate" in the DeviceManager Online Help.

- a. Open Google Chrome and choose **Settings > Advanced > Manage Certificate > Trusted Root Certification Authorities > Import**. The **Certificate Import Wizard** dialog box is displayed.
- b. Select and import the certificate file (**RootCA.crt** in this example) as prompted.
- c. Restart the browser after the certificate is successfully imported.
- d. Log in to the storage system again. No privacy error is generated.



----End

# A Permission Matrix for Self-defined Roles (Applicable to V300R006C20 and Earlier Versions)

Functional Module	Function	Function Description	Role Group
pool	disk_domain	Creates, deletes, modifies, and queries disk domains.	System group <sup>a</sup>
	disk_domain_READONLY	Queries information about disk domains.	System group
	storage_pool	Creates, deletes, modifies, and queries storage pools.	System group
	storage_pool_READONLY	Queries information about storage pools.	System group, vStore group <sup>b</sup>
	disk_READONLY	Queries information about disks.	System group
	enclosure_READONLY	Queries information about engines or disk enclosures.	System group
vstore	vstore	Creates, deletes, modifies, and queries vStores.	System group
	vstore_READONLY	Querying information about vStores.	System group
lun	lun	Creates, modifies, deletes, and queries LUNs.	System group, vStore group
	lun_READONLY	Queries information about LUNs.	System group, vStore group
	remote_resource	Manages the query of remote resources (file systems and LUNs).	System group, vStore group
	remote_resource_READONLY	Queries remote resources (file systems and LUNs).	System group, vStore group

Functional Module	Function	Function Description	Role Group
mapping_view	initiator	Creates, deletes, modifies, and queries initiators.	System group
	initiator_READONLY	Query information about initiators.	System group
	target	Creates, deletes, modifies, and queries targets.	System group
	target_READONLY	Queries information about targets.	System group
	isns	Configures, deletes, and queries the IP address of an iSNS server.	System group
	isns_READONLY	Queries the IP address of an iSNS server	System group
	mapping_view	Creates, deletes, modifies, and queries mapping views.	System group
	mapping_view_READONLY	Queries information about mapping views.	System group
	lun_group	Creates, deletes, modifies, and queries LUN groups, as well as adds objects (LUNs and snapshots) to and removes objects from LUN groups.	System group
	lun_group_READONLY	Queries information about LUN groups.	System group
	host_group	Creates, deletes, modifies, and queries host groups, and adds hosts to or removes hosts from host groups.	System group
	host_group_READONLY	Queries information about host groups.	System group
	host	Creates, deletes, modifies, and queries hosts, and adds initiators to or removes initiators from hosts.	System group
	host_READONLY	Queries information about hosts.	System group
	port_group	Creates, deletes, modifies, and queries port groups.	System group
	port_group_READONLY	Queries information about port groups.	System group
file_system	file_system	Creates, deletes, modifies, and queries file systems.	System group, vStore group
	file_system_READONLY	Query information about file systems.	System group, vStore group

Functional Module	Function	Function Description	Role Group
quota	quota_tree	Creates, deletes, modifies, and queries quota trees in file systems.	System group, vStore group
	quota_tree_READONLY	Queries quota trees in file systems.	System group, vStore group
	quota	Creates, deletes, modifies, and queries quota in file systems.	System group, vStore group
	quota_READONLY	Queries quota in file systems.	System group, vStore group
share	share	Creates, deletes, modifies, and queries shared services.	System group, vStore group
	share_READONLY	Queries information about shared services.	System group, vStore group
file_storage_service	nfs_service	Configures and queries NFS service information.	System group, vStore group
	nfs_service_READONLY	Queries NFS service information.	System group, vStore group
	cifs_service	Configures and queries CIFS service information.	System group, vStore group
	cifs_service_READONLY	Queries CIFS service information.	System group, vStore group
	http_service	Configures and queries HTTP service information.	System group
	http_service_READONLY	Queries HTTP service information.	System group
	ftp_service	Configures and queries FTP service information.	System group
	ftp_service_READONLY	Queries FTP service information.	System group
resource_user	domain	Configures and queries domain authentication information.	System group, vStore group
	domain_READONLY	Queries domain authentication information.	System group, vStore group
	resource_user	Creates, deletes, modifies, and queries authenticated users.	System group, vStore group
	resource_user_READONLY	Queries information about authenticated users.	System group, vStore group

Functional Module	Function	Function Description	Role Group
network	port	Adds, deletes, modifies, and queries ports.	System group
	port_READONLY	Queries information about ports.	System group, vStore group
	logical_port	Creates, deletes, modifies, and queries logical ports, as well as adds routes to or deletes routes from logical ports.	System group
	logical_port_READONLY	Queries information about logical ports.	System group, vStore group
	vlan	Creates, deletes, modifies, and queries VLANs.	System group
	vlan_READONLY	Queries information about VLANs.	System group, vStore group
	failover_group	Creates, modifies, deletes, and queries failover groups, as well as adds members to or removes members from failover groups.	System group
	failover_group_READONLY	Queries information about failover groups.	System group, vStore group
	controller_READONLY	Queries information about controllers.	System group
	interface_module_READONLY	Queries information about interface modules.	System group
local_data_protection	dns_zone <sup>d</sup>	Creates, deletes, modifies, and queries DNS Zone.	System group
	dns_zone_READONLY <sup>d</sup>	Queries information about DNS Zone.	System group, vStore group
	remote_device	Creates, deletes, modifies, and queries remote devices, as well as adds links to or deletes links from remote devices.	System group
	remote_device_READONLY	Queries information about remote devices.	System group, vStore group
remote_resource	remote_resource	Manages the query of remote resources (file systems and LUNs).	System group
	remote_resource_READONLY	Queries remote resources (file systems and LUNs).	System group, vStore group

Functional Module	Function	Function Description	Role Group
	mirror_lun	Creates, deletes, modifies, and queries mirror LUNs, as well as adds mirror copies to or removes mirror copies from mirror LUNs.	System group
	mirror_lun_READONLY	Queries information about mirror LUNs.	System group
	lun_snapshot	Creates, deletes, modifies, queries, activates, recreates, rolls back, cancels the rollback of, and creates copies for LUN snapshots.	System group
	lun_snapshot_READONLY	Queries information about LUN snapshots.	System group
	lun_clone	Creates, deletes, modifies, queries, consistently splits, synchronizes, and reversely synchronizes clones, as well as adds pairs to or removes pairs from clones.	System group
	lun_clone_READONLY	Queries information about clones.	System group
	fs_snapshot	Creates, deletes, modifies, queries, rolls back, and cancels the rollback of file system snapshots.	System group, vStore group
	fs_snapshot_READONLY	Query information about file system snapshots.	System group, vStore group
	lun_copy	Creates, deletes, modifies, queries, suspends, continues, and stops LUN copy.	System group
	lun_copy_READONLY	Queries information about LUN copy.	System group
remote_data_protection	remote_device	Creates, deletes, modifies, and queries remote devices, as well as adds links to or deletes links from remote devices.	System group
	remote_device_READONLY	Queries information about remote devices.	System group, vStore group
	remote_resource	Manages the query of remote resources (file systems and LUNs).	System group
	remote_resource_READONLY	Queries remote resources (file systems and LUNs).	System group, vStore group

Functional Module	Function	Function Description	Role Group
	hyper_vault	Creates, deletes, modifies, and queries HyperVault.	System group, vStore group
	hyper_vault_readonly	Queries information about HyperVault.	System group, vStore group
	remote_replication	Deletes, modifies, queries, synchronizes, and splits remote replication pairs, as well as switches primary/secondary resources and enables or cancels secondary resource protection for remote replication pairs.	System group, vStore group
	remote_replication_READONLY	Queries information about remote replication.	System group, vStore group
	ndmp_service	Modifies and queries NDMP service configuration.	System group, vStore group
	ndmp_service_READONLY	Queries NDMP service configuration.	System group, vStore group
	lun_group	Creates, deletes, modifies, and queries LUN groups, as well as adds objects (LUNs and snapshots) to and removes objects from LUN groups.	System group
	lun_group_READONLY	Queries information about LUN groups.	System group
	consistency_group	Creates, deletes, modifies, queries, synchronizes, and verifies consistency groups.	System group
	consistency_group_READONLY	Queries information about consistency groups.	System group
	remote_replication_vstore_pair <sup>d</sup>	Deletes, modifies, queries, synchronizes, and splits remote replication vStore pairs, as well as switches primary/secondary resources and enables or cancels secondary resource protection for remote replication vStore pairs.	System group
	remote_replication_vstore_pair_READONLY <sup>d</sup>	Queries information about remote replication vStore pairs.	System group, vStore group

Functional Module	Function	Function Description	Role Group
hyper_metro	remote_device	Creates, deletes, modifies, and queries remote devices, as well as adds links to or deletes links from remote devices.	System group
	remote_device_READONLY	Queries information about remote devices.	System group, vStore group
	remote_resource	Manages the query of remote resources (file systems and LUNs).	System group
	remote_resource_READONLY	Queries remote resources (file systems and LUNs).	System group, vStore group
	hyper.metro_consistency_group	Creates, deletes, modifies, queries, starts, and stops HyperMetro consistency groups.	System group
	hyper.metro_consistency_group_READONLY	Queries information about HyperMetro consistency groups.	System group, vStore group
	hyper.metro_domain	Creates, deletes, modifies, and queries HyperMetro domains, as well as adds quorum servers to or removes quorum servers from HyperMetro domains.	System group
	hyper.metro_domain_READONLY	Queries information about HyperMetro domains.	System group, vStore group
	hyper.metro_pair	Creates, deletes, modifies, and queries HyperMetro pairs, as well as configures consistency check for HyperMetro pairs.	System group, vStore group
	hyper.metro_pair_READONLY	Queries information about HyperMetro pairs.	System group, vStore group
hyper.metro_vstore	hyper.metro_vstore_pair	Creates, deletes, modifies, and queries HyperMetro vStore pairs, as well as configures consistency check for HyperMetro vStore pairs.	System group
	hyper.metro_vstore_pair_READONLY	Queries information about HyperMetro vStore pairs.	System group, vStore group
quorum_server	quorum_server	Creates, deletes, modifies, and queries quorum servers, as well as adds links to or removes links from quorum servers.	System group

Functional Module	Function	Function Description	Role Group
	quorum_server_READONLY	Queries information about quorum servers.	System group, vStore group
resource_performance_tuning	smart_qos	Creates, modifies, deletes, and queries SmartQoS policies, as well as adds objects (LUNs and file systems) to or removes objects from SmartQoS policies.	System group
	smart_qos_READONLY	Queries information about SmartQoS policies.	System group
	smart_tier	Configures and queries SmartTier policies (data migration policies or I/O monitoring policies).	System group
	smart_tier_READONLY	Queries information about SmartTier policies.	System group
	smart_partition	Creates, modifies, deletes, and queries smart partitions, as well as adds objects (LUNs and file systems) to or removes objects from smart partitions.	System group
	smart_partition_READONLY	Queries information about smart partitions.	System group
	disk_READONLY	Queries information about disks.	System group
	enclosure_READONLY	Queries information about engines or disk enclosures.	System group
	smart_cache	Creates, modifies, deletes, and queries SmartCaches, as well as adds objects (LUNs and file systems) to or removes objects from SmartCache.	System group
	smart_cache_READONLY	Queries information about SmartCache.	System group
smart_virtualization	smart_migration	Creates, deletes, modifies, queries, consistently splits, and splits LUN migration.	System group
	smart_migration_READONLY	Queries information about LUN migration.	System group
smart_virtualization	remote_resource	Manages the query of remote resources (file systems and LUNs).	System group, vStore group
	remote_resource_READONLY	Queries remote resources (file systems and LUNs).	System group, vStore group

Functional Module	Function	Function Description	Role Group
	remote_device	Creates, deletes, modifies, and queries remote devices, as well as adds links to or deletes links from remote devices.	System group
	remote_device_READONLY	Queries information about remote devices.	System group, vStore group
	port	Adds, deletes, modifies, and queries ports.	System group
	port_READONLY	Queries information about ports.	System group
performance	performance	Configures and queries performance statistics policies.	System group
	performance_READONLY	Queries information about performance statistics policies.	System group
	cifs_service_READONLY	Queries CIFS service information.	System group
	nfs_service_READONLY	Queries NFS service information.	System group
	lun_copy_READONLY	Queries information about LUN copy.	System group
	share_READONLY	Queries information about shared services.	System group
	controller_READONLY	Queries information about controllers.	System group
	smart_qos_READONLY	Queries information about SmartQoS policies.	System group
	disk_domain_READONLY	Queries information about disk domains.	System group
	storage_pool_READONLY	Queries information about storage pools.	System group
	smart_partition_READONLY	Queries information about smart partitions.	System group
	host_READONLY	Queries information about hosts.	System group
	remote_device_READONLY	Queries information about remote devices.	System group
	remote_replication_READONLY	Queries information about remote replication.	System group

Functional Module	Function	Function Description	Role Group
	file_system_readonly	Query information about file systems.	System group
	lun_READONLY	Queries information about LUNs.	System group
	port_READONLY	Queries information about ports.	System group
	lun_snapshot_READONLY	Queries information about LUN snapshots.	System group
	disk_READONLY	Queries information about disks.	System group
	enclosure_READONLY	Queries information about engines or disk enclosures.	System group
<p>a: Permissions that can only be configured for system roles</p> <p>b: Permissions that can be configured for both system and vStore roles</p> <p>d: Function is supported by V300R006C10/C20</p>			

# B Permission Matrix for Self-defined Roles (Applicable to V300R006C30)

Functional Module	Function	Function Description	Role Group
pool	disk_domain	Creates, deletes, modifies, and queries disk domains.	System group <sup>a</sup>
	disk_domain_READONLY	Queries information about disk domains.	System group
	storage_pool	Creates, deletes, modifies, and queries storage pools.	System group
	storage_pool_READONLY	Queries information about storage pools.	System group, vStore group <sup>b</sup>
	disk_READONLY	Queries information about disks.	System group
	enclosure_READONLY	Queries information about engines or disk enclosures.	System group
vstore	vstore	Creates, deletes, modifies, and queries vStores.	System group
	vstore_READONLY	Querying information about vStores.	System group
lun	lun	Creates, modifies, deletes, and queries LUNs.	System group, vStore group
	lun_READONLY	Queries information about LUNs.	System group, vStore group
	remote_resource	Manages the query of remote resources (file systems and LUNs).	System group, vStore group
	remote_resource_READONLY	Queries remote resources (file systems and LUNs).	System group, vStore group

Functional Module	Function	Function Description	Role Group
mapping_view	initiator	Creates, deletes, modifies, and queries initiators.	System group, vStore group
	initiator_READONLY	Query information about initiators.	System group, vStore group
	target	Creates, deletes, modifies, and queries targets.	System group
	target_READONLY	Queries information about targets.	System group, vStore group
	isns	Configures, deletes, and queries the IP address of an iSNS server.	System group
	isns_READONLY	Queries the IP address of an iSNS server	System group
	mapping_view	Creates, deletes, modifies, and queries mapping views.	System group, vStore group
	mapping_view_READONLY	Queries information about mapping views.	System group, vStore group
	lun_group	Creates, deletes, modifies, and queries LUN groups, as well as adds objects (LUNs and snapshots) to and removes objects from LUN groups.	System group, vStore group
	lun_group_READONLY	Queries information about LUN groups.	System group, vStore group
	host_group	Creates, deletes, modifies, and queries host groups, as well adds hosts to or removes hosts from host groups.	System group, vStore group
	host_group_READONLY	Queries information about host groups.	System group, vStore group
	host	Creates, deletes, modifies, and queries hosts, as well adds initiators to or removes initiators from hosts.	System group, vStore group
	host_READONLY	Queries information about hosts.	System group, vStore group
	port_group	Creates, deletes, modifies, and queries port groups.	System group
	port_group_READONLY	Queries information about port groups.	System group, vStore group

Functional Module	Function	Function Description	Role Group
file_system	file_system	Creates, deletes, modifies, and queries file systems.	System group, vStore group
	file_system_readonly	Query information about file systems.	System group, vStore group
quota	quota_tree	Creates, deletes, modifies, and queries quota trees in file systems.	System group, vStore group
	quota_tree_READONLY	Queries quota trees in file systems.	System group, vStore group
	quota	Creates, deletes, modifies, and queries quota in file systems.	System group, vStore group
	quota_READONLY	Queries quota in file systems.	System group, vStore group
share	share	Creates, deletes, modifies, and queries shared services.	System group, vStore group
	share_READONLY	Queries information about shared services.	System group, vStore group
file_storage_service	nfs_service	Configures and queries NFS service information.	System group, vStore group
	nfs_service_READONLY	Queries NFS service information.	System group, vStore group
	cifs_service	Configures and queries CIFS service information.	System group, vStore group
	cifs_service_READONLY	Queries CIFS service information.	System group, vStore group
	http_service	Configures and queries HTTP service information.	System group
	http_service_READONLY	Queries HTTP service information.	System group
	ftp_service	Configures and queries FTP service information.	System group
	ftp_service_READONLY	Queries FTP service information.	System group
resource_user	domain	Configures and queries domain authentication information.	System group, vStore group
	domain_READONLY	Queries domain authentication information.	System group, vStore group

Functional Module	Function	Function Description	Role Group
	resource_user	Creates, deletes, modifies, and queries authenticated users.	System group, vStore group
	resource_user_READONLY	Queries information about authenticated users.	System group, vStore group
network	port	Adds, deletes, modifies, and queries ports.	System group
	port_READONLY	Queries information about ports.	System group, vStore group
	logical_port	Creates, deletes, modifies, and queries logical ports, as well as adds routes to or deletes routes from logical ports.	System group
	logical_port_READONLY	Queries information about logical ports.	System group, vStore group
	vlan	Creates, deletes, modifies, and queries VLANs.	System group
	vlan_READONLY	Queries information about VLANs.	System group, vStore group
	failover_group	Creates, modifies, deletes, and queries failover groups, as well as adds members to or removes members from failover groups.	System group
	failover_group_READONLY	Queries information about failover groups.	System group, vStore group
	controller_READONLY	Queries information about controllers.	System group
	interface_module_READONLY	Queries information about interface modules.	System group
local_data_protection	dns_zone	Creates, deletes, modifies, and queries DNS Zone.	System group
	dns_zone_READONLY	Queries information about DNS Zone.	System group, vStore group
	remote_device	Creates, deletes, modifies, and queries remote devices, as well as adds links to or deletes links from remote devices.	System group
	remote_device_READONLY	Queries information about remote devices.	System group, vStore group

Functional Module	Function	Function Description	Role Group
	remote_resource	Manages the query of remote resources (file systems and LUNs).	System group
	remote_resource_READONLY	Queries remote resources (file systems and LUNs).	System group, vStore group
	mirror_lun	Creates, deletes, modifies, and queries mirror LUNs, as well as adds mirror copies to or removes, splits, synchronizes or modify mirror copies from mirror LUNs.	System group, vStore group
	mirror_lun_READONLY	Queries information about mirror LUNs.	System group, vStore group
	lun_snapshot	Creates, deletes, modifies, queries, activates, recreates, rolls back, cancels the rollback of, and creates copies for LUN snapshots.	System group, vStore group
	lun_snapshot_READONLY	Queries information about LUN snapshots.	System group, vStore group
	lun_clone	Creates, deletes, modifies, queries, consistently splits, synchronizes, and reversely synchronizes clones, as well as adds pairs to or removes pairs from clones.	System group
	lun_clone_READONLY	Queries information about clones.	System group
	lun_clone_vstore	Creates, deletes, modifies, queries, consistently splits, and synchronizes clones, as well as adds pairs to or removes pairs from clones.	System group, vStore group
	lun_clone_vstore_READONLY	Queries information about clones.	System group, vStore group
	fs_snapshot	Creates, deletes, modifies, queries, rolls back, and cancels the rollback of file system snapshots.	System group, vStore group
	fs_snapshot_READONLY	Query information about file system snapshots.	System group, vStore group
	lun_copy	Creates, deletes, modifies, adds, removes, queries, suspends, continues, and stops LUN copy.	System group, vStore group
	lun_copy_READONLY	Queries information about LUN copy.	System group, vStore group

Functional Module	Function	Function Description	Role Group
remote_data_protection	remote_device	Creates, deletes, modifies, and queries remote devices, as well as adds links to or deletes links from remote devices.	System group
	remote_device_READONLY	Queries information about remote devices.	System group, vStore group
	remote_resource	Manages the query of remote resources (file systems and LUNs).	System group
	remote_resource_READONLY	Queries remote resources (file systems and LUNs).	System group, vStore group
	hyper_vault	Creates, deletes, modifies, and queries HyperVault.	System group, vStore group
	hyper_vault_READONLY	Queries information about HyperVault.	System group, vStore group
	remote_replication	Deletes, modifies, queries, synchronizes, and splits remote replication pairs, as well as switches primary/secondary resources and enables or cancels secondary resource protection for remote replication pairs.	System group, vStore group
	remote_replication_READONLY	Queries information about remote replication.	System group, vStore group
	ndmp_service	Modifies and queries NDMP service configuration.	System group, vStore group
	ndmp_service_READONLY	Queries NDMP service configuration.	System group, vStore group
	lun_group	Creates, deletes, modifies, and queries LUN groups, as well as adds objects (LUNs and snapshots) to and removes objects from LUN groups.	System group
	lun_group_READONLY	Queries information about LUN groups.	System group
	consistency_group	Creates, deletes, modifies, queries, synchronizes, and verifies consistency groups.	System group, vStore group
	consistency_group_READONLY	Queries information about consistency groups.	System group, vStore group

Functional Module	Function	Function Description	Role Group
	remote_replicatio_n_vstore_pair	Deletes, modifies, queries, synchronizes, and splits remote replication vStore pairs, as well as switches primary/secondary resources and enables or cancels secondary resource protection for remote replication vStore pairs.	System group
	remote_replicatio_n_vstore_pair_re adonly	Queries information about remote replication vStore pairs.	System group, vStore group
hyper_metro	remote_device	Creates, deletes, modifies, and queries remote devices, as well as adds links to or deletes links from remote devices.	System group
	remote_device_r eadonly	Queries information about remote devices.	System group, vStore group
	remote_resource	Manages the query of remote resources (file systems and LUNs).	System group
	remote_resource_r eadonly	Queries remote resources (file systems and LUNs).	System group, vStore group
	hyper.metro_consistency_group	Creates, deletes, modifies, queries, starts, stops HyperMetro consistency groups, and adds objects (HyperMetro) to or removes objects (HyperMetro).	System group, vStore group
	hyper.metro_consistency_group_r eadonly	Queries information about HyperMetro consistency groups.	System group, vStore group
	hyper.metro_domain	Creates, deletes, modifies, and queries HyperMetro domains, as well as adds quorum servers to or removes quorum servers from HyperMetro domains.	System group
	hyper.metro_domain_READONLY	Queries information about HyperMetro domains.	System group, vStore group
	hyper.metro_pair	Creates, deletes, modifies, and queries HyperMetro pairs, as well as configures consistency check for HyperMetro pairs.	System group, vStore group
	hyper.metro_pair_READONLY	Queries information about HyperMetro pairs.	System group, vStore group

Functional Module	Function	Function Description	Role Group
	hyper_metro_vstore_pair	Creates, deletes, modifies, and queries HyperMetro vStore pairs, as well as configures consistency check for HyperMetro vStore pairs.	System group
	hyper_metro_vstore_pair_READONLY	Queries information about HyperMetro vStore pairs.	System group, vStore group
	quorum_server	Creates, deletes, modifies, and queries quorum servers, as well as adds links to or removes links from quorum servers.	System group
	quorum_server_READONLY	Queries information about quorum servers.	System group, vStore group
resource_performance_tuning	smart_qos	Creates, modifies, deletes, and queries SmartQoS policies, as well as adds objects (LUNs and file systems) to or removes objects from SmartQoS policies.	System group
	smart_qos_READONLY	Queries information about SmartQoS policies.	System group
	smart_tier	Configures and queries SmartTier policies (data migration policies or I/O monitoring policies).	System group
	smart_tier_READONLY	Queries information about SmartTier policies.	System group
	smart_partition	Creates, modifies, deletes, and queries smart partitions, as well as adds objects (LUNs and file systems) to or removes objects from smart partitions.	System group
	smart_partition_READONLY	Queries information about smart partitions.	System group
	disk_READONLY	Queries information about disks.	System group
	enclosure_READONLY	Queries information about engines or disk enclosures.	System group
	smart_cache	Creates, modifies, deletes, and queries SmartCaches, as well as adds objects (LUNs and file systems) to or removes objects from SmartCache.	System group

Functional Module	Function	Function Description	Role Group
	smart_cache_rea donly	Queries information about SmartCache.	System group
	smart_migration	Creates, deletes, modifies, queries, consistently splits, and splits LUN migration.	System group, vStore group
	smart_migration_ readonly	Queries information about LUN migration.	System group, vStore group
smart_virtua lization	remote_resource	Manages the query of remote resources (file systems and LUNs).	System group, vStore group
	remote_resource_ _readonly	Queries remote resources (file systems and LUNs).	System group, vStore group
	remote_device	Creates, deletes, modifies, and queries remote devices, as well as adds links to or deletes links from remote devices.	System group
	remote_device_r eadonly	Queries information about remote devices.	System group, vStore group
	port	Adds, deletes, modifies, and queries ports.	System group
	port_READONLY	Queries information about ports.	System group
performance	performance	Configures and queries performance statistics policies.	System group
	performance_rea donly	Queries information about performance statistics policies.	System group
	cifs_service_read only	Queries CIFS service information.	System group
	nfs_service_read only	Queries NFS service information.	System group
	lun_copy_readon ly	Queries information about LUN copy.	System group
	share_readonly	Queries information about shared services.	System group
	controller_readon ly	Queries information about controllers.	System group
	smart_qos_reado nly	Queries information about SmartQoS policies.	System group
	disk_domain_rea donly	Queries information about disk domains.	System group

Functional Module	Function	Function Description	Role Group
	storage_pool_READONLY	Queries information about storage pools.	System group
	smart_partition_READONLY	Queries information about smart partitions.	System group
	host_READONLY	Queries information about hosts.	System group
	remote_device_READONLY	Queries information about remote devices.	System group
	remote_replication_READONLY	Queries information about remote replication.	System group
	file_system_READONLY	Query information about file systems.	System group
	lun_READONLY	Queries information about LUNs.	System group
	port_READONLY	Queries information about ports.	System group
	lun_snapshot_READONLY	Queries information about LUN snapshots.	System group
	disk_READONLY	Queries information about disks.	System group
	enclosure_READONLY	Queries information about engines or disk enclosures.	System group
a: Permissions that can only be configured for system roles			
b: Permissions that can be configured for both system and vStore roles			

# C How to Obtain Help

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

## C.1 Preparations for Contacting Huawei

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

### C.1.1 Collecting Troubleshooting Information

You need to collect troubleshooting information before troubleshooting.

You need to collect the following information:

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

### C.1.2 Making Debugging Preparations

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

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

## C.2 How to Use the Document

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

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

## C.3 How to Obtain Help from Website

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

Contents of the Huawei technical support system are as follows:

- Huawei headquarters technical support department
- Regional office technical support center
- Customer service center
- Technical support website: <http://support.huawei.com/enterprise/>

You can query how to contact the regional offices at <http://support.huawei.com/enterprise/>.

## C.4 Ways to Contact Huawei

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

Huawei Technologies Co., Ltd.

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

Website: <http://enterprise.huawei.com/>

# D Glossary

---

If you want to obtain information about glossaries, visit <http://support.huawei.com/enterprise/>. In the search field, enter a product model, and select a path from the paths that are automatically displayed to go to the document page of the product. Browse or download the *OceanStor V3 Series V300R006 Glossary*.

# E Acronyms and Abbreviations

## Acronyms and Abbreviations

A	
<b>ACL</b>	Access Control List
<b>AD</b>	Active Directory
<b>AES</b>	Advanced Encryption Standard
<b>ANSI</b>	American National Standards Institute
<b>ASCII</b>	American Standard Code for Information Interchange
<b>ASP</b>	Authorized Service Partner
<b>C</b>	
<b>CA</b>	Certificate Authority
<b>CHAP</b>	Challenge Handshake Authentication Protocol
<b>CIFS</b>	Common Internet File System
<b>CLI</b>	Command Line Interface
<b>CPU</b>	Central Processing Unit
<b>D</b>	
<b>DCB</b>	Data Center Bridging
<b>DES</b>	Data Encryption Standard
<b>DHA</b>	Disk Health Analysis
<b>DNS</b>	Domain Name Server
<b>DN</b>	Distinguished Name
<b>DSA</b>	Digital Signature Algorithm

<b>A</b>	
<b>E</b>	
<b>ESN</b>	Equipment Serial Number
<b>ESDP</b>	Electronic Software Delivery Platform
<b>F</b>	
<b>FC</b>	Fibre Channel
<b>FCoE</b>	Fibre Channel over Ethernet
<b>FRU</b>	Field Replaceable Unit
<b>FTP</b>	File Transfer Protocol
<b>G</b>	
<b>GE</b>	Gigabit Ethernet
<b>GPT</b>	GUID Partition Table
<b>GSM</b>	Global System for Mobile Communications
<b>GTS</b>	Global Technical Service
<b>GUI</b>	Graphical User Interface
<b>GUID</b>	Global Universal Identification
<b>H</b>	
<b>HBA</b>	Host Bus Adapter
<b>HD</b>	High Density
<b>HTTP</b>	Hypertext Transfer Protocol
<b>HTTPS</b>	Hypertext Transfer Protocol Secure
<b>I</b>	
<b>IB</b>	Integration Bus
<b>ICAP</b>	Internet Content Adaptation Protocol
<b>I/O</b>	Input/Output
<b>IP</b>	Internet Protocol
<b>IPv4</b>	Internet Protocol version 4
<b>IPv6</b>	Internet Protocol version 6
<b>IQN</b>	iSCSI Qualified Name

A	
<b>ISA</b>	Instrument Society of America
<b>iSCSI</b>	Internet Small Computer Systems Interface
<b>iSNS</b>	Internet Storage Name Service
<b>ISO</b>	International Organization for Standardization
<b>iWARP</b>	Internet wide-area RDMA protocol
<b>J</b>	
<b>JRE</b>	Java Runtime Environment
<b>L</b>	
<b>LACP</b>	Link Aggregation Control Protocol
<b>LDAP</b>	Lightweight Directory Access Protocol
<b>LDAPS</b>	LDAP over SSL
<b>LUN</b>	Logical Unit Number
<b>LVM</b>	Logical Volume Manager
<b>M</b>	
<b>MAC</b>	Media Access Control
<b>MBR</b>	Master Boot Record
<b>MD5</b>	Message Digest Algorithm 5
<b>MIB</b>	Management Information Base
<b>N</b>	
<b>NAS</b>	Network-attached Storage
<b>NDMP</b>	Network Data Management Protocol
<b>NFS</b>	Network File System
<b>NIS</b>	Network Information Services
<b>NL-SAS</b>	Near Line Serial Attached SCSI
<b>NTP</b>	Network Time Protocol
<b>O</b>	
<b>OLTP</b>	Online Transaction Processing
<b>OLAP</b>	Online Analytical Processing

A	
<b>OID</b>	Object Identifier
<b>P</b>	
<b>PO</b>	Purchase Order
<b>PVID</b>	Port VLAN ID
<b>R</b>	
<b>RAID</b>	Redundant Array of Independent Disks
<b>RDMA</b>	Remote Direct Memory Access
<b>RDN</b>	Relative Distinguished Name
<b>REST</b>	Representational State Transfer
<b>RSA</b>	Rivest-Shamir-Adleman
<b>R.H.</b>	Relative Humidity
<b>S</b>	
<b>SAN</b>	Storage Area Network
<b>SAS</b>	Serial Attached SCSI
<b>SCOM</b>	System Center Operations Manager
<b>SCSI</b>	Small Computer System Interface
<b>SFTP</b>	Secure File Transfer Protocol
<b>SHA</b>	Secure Hash Algorithm
<b>SIM</b>	Subscriber Identity Module
<b>S.M.A.R.T</b>	Self-Monitoring, Analysis and Reporting Technology
<b>SMI-S</b>	Storage Management Initiative-Specification
<b>SMTP</b>	Simple Mail Transfer Protocol
<b>SNMP</b>	Simple Network Management Protocol
<b>SSH</b>	Secure Shell
<b>SSL</b>	Secure Sockets Layer
<b>T</b>	
<b>TCP/IP</b>	Transmission Control Protocol/Internet Protocol
<b>TLS</b>	Transport Layer Security

<b>A</b>	
<b>U</b>	
<b>UDP</b>	User Datagram Protocol
<b>USM</b>	User-based Security Model
<b>UTC</b>	Universal Time Coordinated
<b>UUID</b>	Universally Unique Identifier
<b>V</b>	
<b>VASA</b>	vStorage APIs for Storage Awareness
<b>VAAI</b>	vStorage APIs for Array Integration
<b>VG</b>	Volume Group
<b>VLAN</b>	Virtual Local Area Network
<b>VMFS</b>	Virtual Machine File System
<b>VSS</b>	Volume Shadow Copy Service
<b>W</b>	
<b>WORM</b>	Write Once Read Many
<b>WWN</b>	World Wide Name
<b>WWPN</b>	World Wide Port Name