



**OceanStor V3 Series**  
**V300R006**

# **Basic Storage Service Configuration Guide for Bolck**

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

**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

## Purpose

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

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

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



## Intended Audience




This document is intended for:

- Technical support engineers
- Maintenance engineers

## Symbol Conventions

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

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

Symbol	Description
 <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 05 (2018-01-30)

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

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

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

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

Optimized descriptions about the chapter **Planning Disk Domains**.

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

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

Added the coffer disk description.

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

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

Added the OpenStack Cinder Driver configuration description.

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

This is the first official release.

---

# Contents

---

<b>About This Document.....</b>	<b>ii</b>
<b>1 Basic Storage Services.....</b>	<b>1</b>
1.1 Introduction.....	1
1.2 Application Scenarios.....	2
1.3 Basic Concepts.....	3
1.4 Basic Storage Principles.....	5
1.4.1 I/O Processing Procedure Between an Application Server and Storage System.....	5
1.4.2 Operating Principles in a Storage System.....	16
<b>2 Planning Basic Storage Services.....</b>	<b>22</b>
2.1 Planning Process.....	23
2.2 Planning Applications.....	26
2.3 Planning the Capacity.....	27
2.4 Planning Ports and Service Data.....	33
2.5 Planning Disk Domains.....	41
2.6 Planning Storage Pools.....	47
2.7 Planning LUNs.....	54
2.8 (Optional) Planning iSCSI CHAP.....	57
2.9 Planning Management User Accounts.....	58
<b>3 Configuring Basic Storage Services.....</b>	<b>60</b>
3.1 Configuration Process.....	61
3.2 Checking Before Configuration.....	66
3.3 Logging In to the DeviceManager.....	70
3.3.1 Logging In to the DeviceManager Through Web.....	70
3.3.2 Logging In to the DeviceManager Using a Tablet.....	74
3.3.3 Logging In to the DeviceManager Through SVP (18000 Series).....	75
3.3.4 Logging In to the DeviceManager Through Management Network Port (18000 Series).....	78
3.4 Creating a Disk Domain.....	81
3.5 Creating a Storage Pool.....	86
3.6 Creating a LUN.....	96
3.7 Creating a LUN Group.....	113
3.8 Configuring Connectivity between Host and Storage System.....	114
3.8.1 iSCSI Networking.....	114

3.8.1.1 Configuring Ethernet Switches.....	115
3.8.1.2 Configuring an IP Address for the Service Network Port on the Application Server.....	115
3.8.1.2.1 Configuring an IP Address for the Service Network Port on the Application Server (Windows).....	116
3.8.1.2.2 Configuring an IP Address for the Service Network Port on the Application Server (SUSE).....	117
3.8.1.2.3 Configuring an IP Address for the Service Network Port on the Application Server (Red Hat).....	120
3.8.1.2.4 Configuring an IP Address for the Service Network Port on the Application Server (Solaris).....	121
3.8.1.2.5 Configuring an IP Address for the Service Network Port on the Application Server (AIX).....	124
3.8.1.2.6 Configuring an IP Address for the Service Network Port on the Application Server (HP-UX).....	125
3.8.1.2.7 Configuring an IP Address for the Service Network Port on the Application Server (VMware).....	129
3.8.1.3 Configuring an Initiator.....	132
3.8.1.3.1 Configuring an Initiator (Windows).....	133
3.8.1.3.2 Configuring an Initiator (SUSE).....	141
3.8.1.3.3 Configuring an Initiator (Red Hat).....	143
3.8.1.3.4 Configuring an Initiator (Solaris).....	145
3.8.1.3.5 Configuring an Initiator (AIX).....	149
3.8.1.3.6 Configuring an Initiator (HP-UX).....	154
3.8.1.3.7 Configuring an Initiator (VMware).....	157
3.8.1.4 (Optional) Configuring CHAP Authentication.....	162
3.8.1.4.1 Configuring CHAP Authentication (Windows).....	163
3.8.1.4.2 Configuring CHAP Authentication (SUSE).....	169
3.8.1.4.3 Configuring CHAP Authentication (Red Hat).....	170
3.8.1.4.4 Configuring CHAP Authentication (Solaris).....	171
3.8.1.4.5 Configuring CHAP Authentication (AIX).....	172
3.8.1.4.6 Configuring CHAP Authentication (HP-UX).....	173
3.8.1.4.7 Configuring CHAP Authentication (VMware).....	174
3.8.1.5 Setting Ethernet Port Information.....	176
3.8.1.6 (Optional) Adding Routes.....	177
3.8.2 Fibre Channel Networking.....	179
3.8.2.1 Configuring Fibre Channel Switches.....	179
3.8.2.1.1 Querying the Switch Model and Version.....	179
3.8.2.1.2 Configuring Zones.....	183
3.8.2.2 Querying a Host WWPN.....	186
3.8.2.2.1 Querying the WWPN of a Host HBA's Port (Windows).....	186
3.8.2.2.2 Querying the WWPN of a Host HBA's Port (SUSE).....	188
3.8.2.2.3 Querying the WWPN of a Host HBA's Port (Red Hat).....	188
3.8.2.2.4 Querying the WWPN of a Host HBA's Port (Solaris).....	189
3.8.2.2.5 Querying the WWPN of a Host HBA's Port (AIX).....	192
3.8.2.2.6 Querying the WWPN of a Host HBA's Port (HP-UX).....	193
3.8.2.2.7 Querying the WWPN of a Host HBA's Port (VMware).....	195
3.8.2.3 (Optional) Setting Fibre Channel Port Information.....	196
3.8.3 FCoE Networking.....	198
3.8.3.1 Configuring FCoE Switches.....	198

3.8.3.2 Configuring Zones.....	200
3.9 Creating a Host.....	202
3.9.1 Automatically Scanning for a Host.....	202
3.9.2 Manually Creating a Host.....	203
3.9.3 Batch Creating Hosts.....	206
3.10 Creating a Host Group.....	208
3.11 (Optional) Creating a Port Group.....	210
3.12 Creating a Mapping View.....	211
3.13 Configuring LUN Mapping Using a Cipher Machine.....	214
3.14 Making Storage Space Available.....	214
3.14.1 Making Storage Space Available (Windows).....	215
3.14.2 Making Storage Space Available (SUSE).....	225
3.14.3 Making Storage Space Available (Red Hat).....	231
3.14.4 Making Storage Space Available (Solaris).....	236
3.14.5 Making Storage Space Available (AIX).....	240
3.14.6 Making Storage Space Available (HP-UX).....	243
3.14.7 Making Storage Space Available (VMware).....	246
3.14.8 Making Storage Space Available (Hyper-V).....	252
3.15 Performing an Emergency Rollback.....	263
<b>4 Configuring Basic Storage Services (for VMware VVol Scenarios Only).....</b>	<b>265</b>
4.1 Configuration Process.....	267
4.2 Logging In to the DeviceManager.....	269
4.2.1 Logging In to the DeviceManager Through Web.....	270
4.2.2 Logging In to the DeviceManager Using a Tablet.....	273
4.2.3 Logging In to the DeviceManager Through SVP (18000 Series).....	274
4.2.4 Logging In to the DeviceManager Through Management Network Port (18000 Series).....	277
4.3 Creating a Disk Domain.....	280
4.4 Creating a Storage Pool.....	285
4.5 Creating a PE LUN.....	295
4.6 Creating a LUN Group.....	299
4.7 Configuring Connectivity between Host and Storage System.....	300
4.7.1 iSCSI Networking.....	300
4.7.1.1 Configuring Ethernet Switches.....	300
4.7.1.2 Configuring an IP Address for the Service Network Port on the Application Server.....	301
4.7.1.3 Configuring an Initiator.....	303
4.7.1.4 (Optional) Configuring CHAP Authentication.....	307
4.7.1.5 Setting Ethernet Port Information.....	308
4.7.1.6 (Optional) Adding Routes.....	310
4.7.2 Fibre Channel Networking.....	311
4.7.2.1 Configuring Fibre Channel Switches.....	311
4.7.2.1.1 Querying the Switch Model and Version.....	312
4.7.2.1.2 Configuring Zones.....	315

4.7.2.2 Querying a Host WWPN.....	318
4.7.2.3 (Optional) Setting Fibre Channel Port Information.....	319
4.8 Creating a Host.....	321
4.8.1 Automatically Scanning for a Host.....	321
4.8.2 Manually Creating a Host.....	322
4.8.3 Batch Creating Hosts.....	326
4.9 Creating a Host Group.....	328
4.10 (Optional) Creating a Port Group.....	330
4.11 Creating a Mapping View.....	331
4.12 Configuring the VVols Function.....	334
4.13 Using a VVOL Datastore to Create a VM.....	334
<b>5 Creating Storage Resources Based on Applications.....</b>	<b>337</b>
5.1 Configuring Microsoft Exchange.....	337
5.1.1 About Microsoft Exchange.....	337
5.1.2 Creating a Microsoft Exchange Instance.....	338
5.2 Configuring VMware.....	343
5.2.1 About VMware.....	344
5.2.2 Creating a VMware Instance.....	344
5.3 Configuring Hyper-V.....	351
5.3.1 About Hyper-V.....	351
5.3.2 Creating a Hyper-V Instance.....	352
5.4 Configuring Oracle.....	359
5.4.1 About Oracle.....	360
5.4.2 Creating an Oracle Instance.....	360
5.5 Configuring SQL Server.....	366
5.5.1 About SQL Server.....	366
5.5.2 Creating an SQL Server Instance.....	367
<b>6 Managing Basic Storage Services.....</b>	<b>374</b>
6.1 Managing Access Permission of a Storage System.....	375
6.1.1 Configuring a Security Policy for System User.....	375
6.1.2 Configuring Authorized IP Addresses.....	381
6.1.3 Managing Users and Their Access Permissions.....	382
6.1.3.1 Creating a Local User.....	382
6.1.3.2 Creating a Domain User.....	384
6.1.3.3 Managing User Levels.....	386
6.1.3.4 Customizing User Roles.....	388
6.1.3.5 Locking or Unlocking a User.....	390
6.1.3.6 Logging Out a User.....	392
6.2 Managing iSCSI Host Ports.....	393
6.2.1 Viewing Bit Error Statistics.....	393
6.2.2 Managing Routes.....	394
6.2.3 Bonding Ethernet Ports.....	397



6.2.4 Canceling Ethernet Port Bonding.....	399
6.2.5 Viewing Ethernet Port Information.....	399
6.2.6 Modifying an Ethernet Port.....	402
6.2.7 Naming an iSCSI Device and an iSCSI Initiator.....	404
6.2.8 Setting iSNS.....	404
6.3 Managing Fibre Channel Host Ports.....	405
6.3.1 Viewing Bit Error Statistics.....	405
6.3.2 Viewing Fibre Channel Port Information.....	406
6.3.3 Modifying a Fibre Channel Port.....	407
6.4 Managing Disk Domains.....	410
6.4.1 Viewing Disk Domain Information.....	410
6.4.2 Viewing Data Distribution in a Disk Domain.....	412
6.4.3 Deleting an Unencrypted Disk Domain.....	413
6.4.4 Deleting an Encrypted Disk Domain.....	414
6.4.5 Modifying the Hot Spare Policy of a Disk Domain.....	414
6.4.6 Expanding a Disk Domain.....	415
6.4.7 Updating Key of Encrypted Disk Domain.....	416
6.5 Managing Storage Pools.....	417
6.5.1 Viewing Storage Pool Information.....	417
6.5.2 Viewing General Information About a Storage Pool.....	419
6.5.3 Modifying a SmartTier Policy.....	421
6.5.4 Viewing SmartTier Status.....	424
6.5.5 Forecasting Storage Pool Performance.....	427
6.5.6 Modifying the Advanced Properties of a Storage Pool.....	428
6.5.7 Modifying Capacity of a Storage Pool.....	430
6.5.8 Deleting a Storage Pool.....	437
6.6 Managing LUNs.....	437
6.6.1 Viewing LUN Information.....	437
6.6.2 Viewing Owing LUN Group Information.....	443
6.6.3 Modifying the General Properties of a LUN.....	443
6.6.4 Modifying the Advanced Properties of a LUN.....	444
6.6.5 Expanding a LUN on a Storage System.....	450
6.6.6 Expanding a LUN on an Application Server.....	451
6.6.6.1 Expanding a LUN on a Windows-Based Application Server.....	451
6.6.6.2 Expanding a LUN on a SUSE-Based Application Server.....	455
6.6.6.3 Expanding a LUN on a RedHat-Based Application Server.....	456
6.6.6.4 Expanding a LUN on a Solaris-based Application Server.....	458
6.6.6.5 Expanding a LUN on an AIX-based Application Server.....	461
6.6.6.6 Expanding a LUN on an HP-UX-based Application Server.....	466
6.6.6.7 Expanding a LUN on a VMware ESX-Based Application Server.....	467
6.6.7 Deleting a LUN.....	472
6.7 Managing LUN Groups.....	473

6.7.1 Viewing LUN Group Information.....	473
6.7.2 Modifying the General Properties of a LUN Group.....	474
6.7.3 Viewing an Owning Mapping View of a LUN Group.....	475
6.7.4 Adding an Object.....	475
6.7.5 Removing Object.....	476
6.7.6 Deleting a LUN Group.....	476
6.8 Managing Hosts.....	477
6.8.1 Viewing Host Information.....	477
6.8.2 Modifying Host Properties.....	478
6.8.3 Creating an Initiator.....	479
6.8.4 Modifying an Initiator.....	489
6.8.5 Deleting an Initiator.....	502
6.8.6 Adding an Initiator to a Host.....	503
6.8.7 Deleting a Host.....	503
6.9 Managing Host Groups.....	504
6.9.1 Viewing Host Group Information.....	504
6.9.2 Modifying Host Group Information.....	504
6.9.3 Viewing an Owning Mapping View of a Host Group.....	505
6.9.4 Adding a Host.....	506
6.9.5 Deleting a Host Group.....	506
6.10 Managing a Port Group.....	507
6.10.1 Viewing the Information About a Port Group.....	507
6.10.2 Modifying the Properties of a Port Group.....	508
6.10.3 Viewing an Owning Mapping View.....	509
6.10.4 Deleting a Port Group.....	510
6.10.5 Adding a Port.....	510
6.10.6 Removing a Port.....	511
6.11 Managing Mapping Views.....	511
6.11.1 Viewing Mapping View Information.....	511
6.11.2 Modifying the Properties of a Mapping View.....	516
6.11.3 Deleting a Mapping View.....	517
6.11.4 Modifying a Host LUN ID.....	517
<b>7 Appendix OpenStack Cinder Driver Access Methods and Configuration Ideas.....</b>	<b>519</b>
<b>8 FAQ.....</b>	<b>521</b>
8.1 In the SQL Server database scenario, how can I adjust parameters to reduce the I/O latency and achieve the optimal performance?.....	521
8.2 How to create AD domain users and groups on the AD domain controller?.....	521
<b>A Managing Batch Configuration.....</b>	<b>525</b>
A.1 About Batch Configuration.....	525
A.2 Configuration Process.....	525
A.3 Configuring Storage System with CLI Configuration File.....	526
A.3.1 Downloading a Configuration File.....	526

A.3.2 Importing a Configuration File.....	527
A.3.3 Implementing Batch Configuration.....	527
A.3.4 Stopping Batch Configuration.....	528
A.4 Configuring Storage System with Offline Configuration File.....	528
A.4.1 Importing a Offline Configuration File.....	528
A.4.2 Implementing Offline Configuration.....	529
A.4.3 Exporting Implementation Reports.....	530
<b>B Permission Matrix for Self-defined Roles.....</b>	<b>531</b>
<b>C How to Obtain Help.....</b>	<b>541</b>
C.1 Preparations for Contacting Huawei.....	541
C.1.1 Collecting Troubleshooting Information.....	541
C.1.2 Making Debugging Preparations.....	542
C.2 How to Use the Document.....	542
C.3 How to Obtain Help from Website.....	542
C.4 Ways to Contact Huawei.....	542
<b>D Glossary.....</b>	<b>543</b>
<b>E Acronyms and Abbreviations.....</b>	<b>544</b>

# 1 Basic Storage Services

---

## About This Chapter

Configure basic storage services so that application servers can use the storage space provided by a storage system.

### [1.1 Introduction](#)

Storage systems provide increased response speed, scalability, and enhanced self-healing capability.

### [1.2 Application Scenarios](#)

This section describes the application scenarios of basic storage services.

### [1.3 Basic Concepts](#)

Get yourself started with the following basic concepts:

### [1.4 Basic Storage Principles](#)

This section describes the I/O processing procedure between an application server and a storage system and the working principles within a storage system.

## 1.1 Introduction

Storage systems provide increased response speed, scalability, and enhanced self-healing capability.

Storage systems use the block virtualization technology to manage disks, which helps automatically and properly allocate storage resources and provide available storage space for application servers.

Block virtualization is a new redundant array of independent disks (RAID) technology that divides disks into block-level CHUNKs (CKs) and organizes the CKs into multiple RAID groups. When a disk fails, source disks of storage pools in the storage system participate in the reconstruction. This smashes the performance bottleneck in the reconstruction of traditional RAID groups and greatly improves the data reconstruction speed.

Storage pools are containers of storage resources, which originate from disk domains. The storage resources used by application servers are all from storage pools. Benefits of the series include:

- **Increased response speed**  
The storage system supports load balancing across the entire system. Data is distributed among the source disks of storage pools to make full use of the I/O capabilities of the storage system.
- **High scalability**  
As the storage system manages disks and provides storage space for application servers in the form of disk domains, you only need to add disks to the disk domains and expand corresponding storage pools when storage capacity is insufficient.
- **Enhanced self-healing capability**  
The storage system supports concurrent reconstruction across the entire system. Source disks of storage pools participate in reconstruction simultaneously to eliminate the performance bottleneck of traditional RAID groups and notably improve data reconstruction speed.
- **Balance between performance and cost**  
The storage system can automatically detect I/O hotspots and migrate data among storage tiers to achieve the best storage performance by using SmartTier, a dynamic storage tiering feature.

 **NOTE**

- You must purchase a license to use SmartTier. For details about this feature, see the *OceanStor V3 Series V300R006 SmartTier Feature Guide*.
- A storage system with only one type of storage media does not support SmartTier.

## 1.2 Application Scenarios

This section describes the application scenarios of basic storage services.

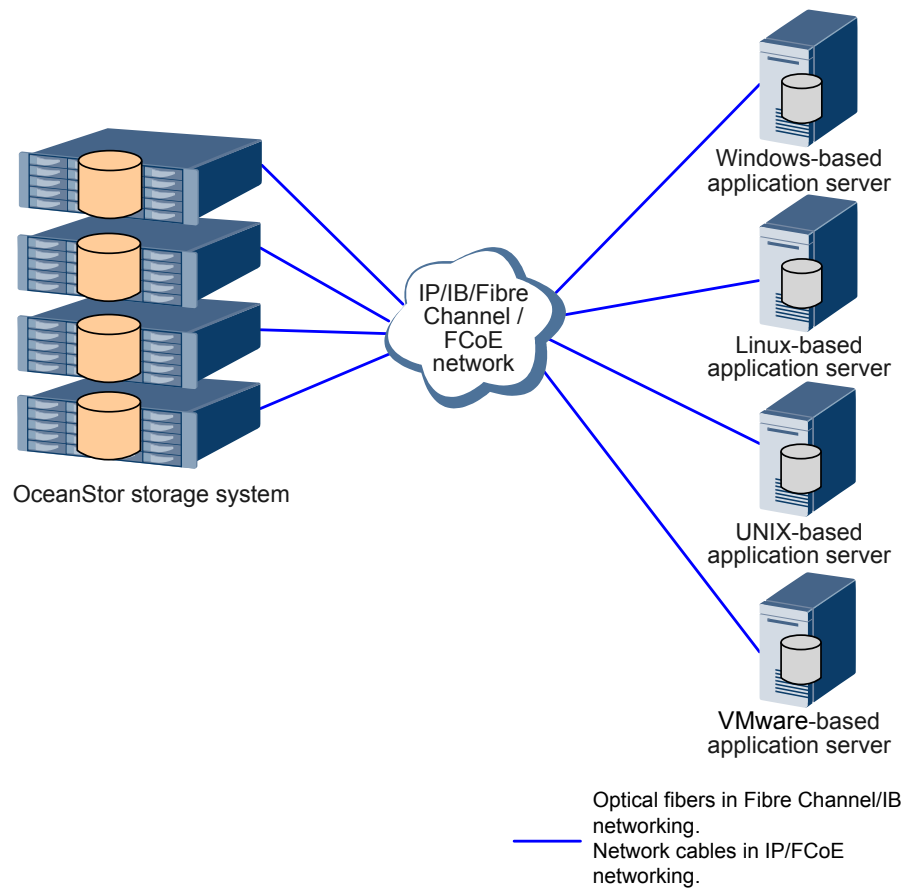
Storage systems can be connected to application servers through an IP, InfiniBand (IB), Fibre Channel, or Fibre Channel over Ethernet (FCoE) network.

- **IP network**  
Strengths: The IP network supports long-distance transmission and can be built and expanded at a low cost. The IP network is widely used.  
Weaknesses: The IP network supports network bandwidth sharing, affecting the data transfer rate between storage systems and application servers.
- **Fibre Channel or IB network**  
Strengths: The Fibre Channel or IB network provides a fast transmission rate and a high bandwidth to ensure data transfer between storage systems and application servers.  
Weaknesses: The Fibre Channel or IB network has a high construction cost and limited transmission distance, and is difficult to expand.

Storage systems can be connected to a variety of application servers including Windows, Linux, UNIX (such as AIX, HP-UX, and Solaris), and VMware application servers.

**Figure 1-1** shows the application scenarios of basic storage services.

Figure 1-1 Application scenarios of basic storage services



## 1.3 Basic Concepts

Get yourself started with the following basic concepts:

- **Disk domain:** consisting of the same or different types of disks. Disk domains are isolated from each other. Therefore, services carried by different disk domains do not affect each other in terms of performance and faults if any.
- **Storage pool:** container of storage resources, which is created under a disk domain. The storage resources used by application servers are from storage pools. Based on the storage media, a storage pool can have three storage tiers, including the high performance tier, performance tier, and capacity tier.
- **Storage tier:** a set of storage media providing the same performance in a storage pool. Storage tiers are used to manage storage media with different performance and provide appropriate storage space for applications having different performance demands.
- **CK:** a set of consecutive physical spaces of a fixed size on a disk.
- **CHUNK Group (CKG):** a logical set of CKs on different disks. A CKG has the properties of a RAID group.
- **Block virtualization:** a new type of RAID technology. Block virtualization divides disks into multiple CKs of a fixed size and organizes them into multiple CKGs. When a disk fails, the disks of the CKG where the CKs in the faulty disk reside also participate in

reconstruction. This significantly increases the disks involved in the reconstruction, eliminating the performance bottleneck in the reconstruction of traditional RAID groups and improving the data reconstruction speed. In addition, block virtualization distributes data to all the disks in a storage system and leverages the I/O processing capability of the storage system.

- **Extent:** a block of a fixed size in a CKG, 4 MB by default. The extent is the smallest unit of a thick LUN, as well as the smallest unit used to calculate the requested space, released space, and relocated data.
- **Grain:** a small block with a fixed size divided from extents. The default size of a grain is 64 KB. When all the disks in a storage pool are Solid State Drives (SSDs), the default size of a grain is 8 KB. Grains are basic units that constitute a thin LUN. Logical Block Addresses (LBAs) in a grain are consecutive.
- **Hot spare space:** space used for faulty block data reconstruction in block virtualization. When a CK is faulty, the system lets a CK of the hot spare space take over and instructs other CKs in the CKG to perform data reconstruction using the hot spare space. This ensures data integrity and read/write performance.
- **Reconstruction:** process of restoring the data saved on a faulty disk to hot spare CKs and replacing the CKs on the faulty disk with the hot spare CKs. During data reconstruction, valid data and parity data must be read and processed to restore the data saved on a faulty disk to hot spare space, thereby ensuring data security and reliability. Traditional reconstruction technologies allow only all disks in the same RAID group as the faulty disk to participate in reconstruction. The RAID 2.0+ technology enables all disks in the same disk domain as the faulty disk to participate in reconstruction, boosting data reconstruction speed and shortening data recovery duration.

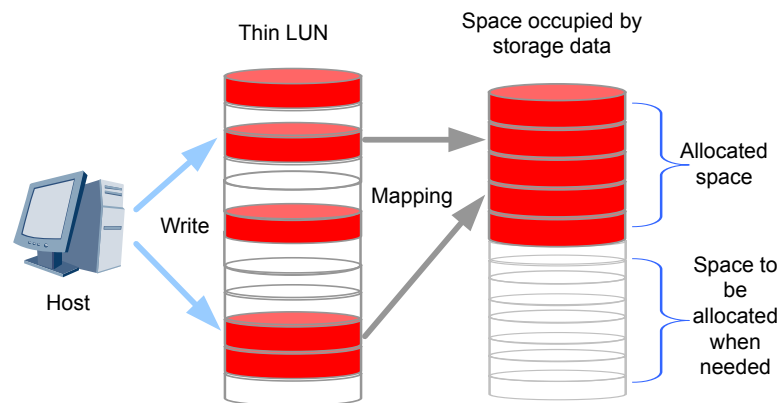
---

 **NOTICE**

Data on other disks will be read for reconstruction. Therefore, to prevent reconstruction failures, service interruption, and data loss, do not remove other disks in the disk domain where the faulty disk resides during reconstruction.

- 
- **SmartThin:** provides a storage management mode that supports on-demand space allocation. Instead of allocating all storage space in advance, it first allocates specified storage space and then dynamically allocates storage resources (thin LUNs) based on users' requirements. [Figure 1-2](#) shows storage space occupation when SmartThin is used.

**Figure 1-2** Storage space occupation when SmartThin is used



SmartThin applies to the following scenarios:

- Core system services that have high requirements for service continuity, such as financial services, use SmartThin for online expansion to ensure non-disruptive operation.
- Services with an unpredictable growth rate, such as email and web disk services, use SmartThin to allocate physical storage space on demand.
- Mixed services, such as carriers' services, that have a variety of storage requirements use SmartThin to contend for physical storage space and achieve optimal configuration of physical storage space.

**NOTE**

After SmartThin is enabled, the storage system can reclaim storage space using standard SCSI commands **unmap** and **writesame**.

## 1.4 Basic Storage Principles

This section describes the I/O processing procedure between an application server and a storage system and the working principles within a storage system.

### 1.4.1 I/O Processing Procedure Between an Application Server and Storage System

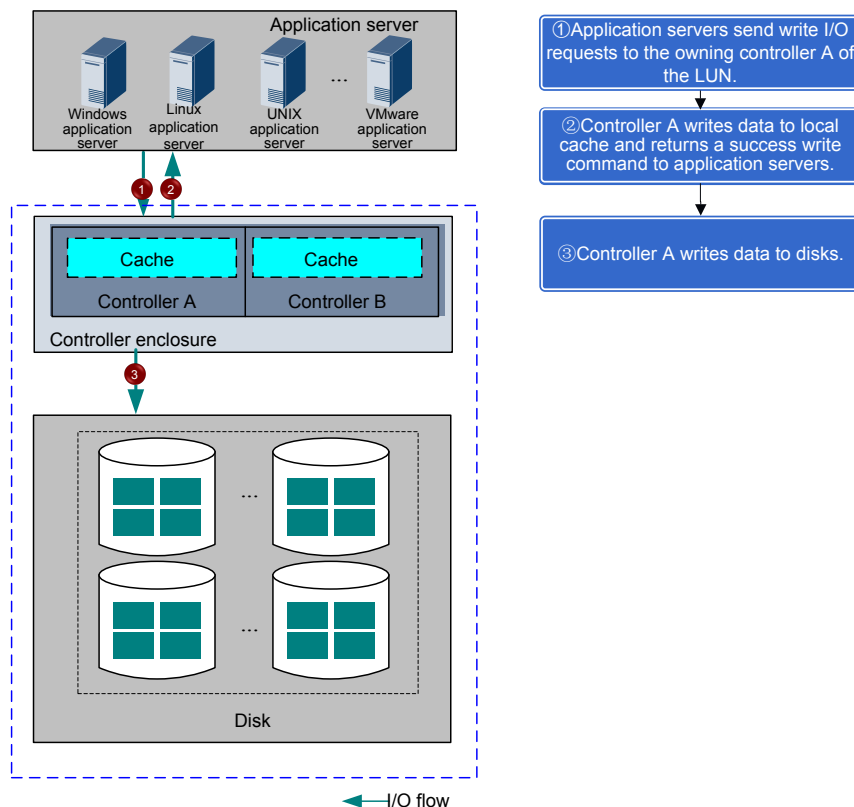
This section describes how I/Os are processed in scenarios where cross-controller load balancing is enabled in UltraPath on an application server and the round-robin load balancing algorithm is used.

#### Scenario 1: Single Controller Enclosure Scenario Where an Application Server Sends a Write I/O Request to a LUN

**Figure 1-3** shows the single controller enclosure scenario where an application server sends a write I/O request to a LUN. The figure on the left shows the principles of delivering a write I/O request from an application server to a LUN in the single controller enclosure scenario. The figure on the right shows the principles in a flowchart.



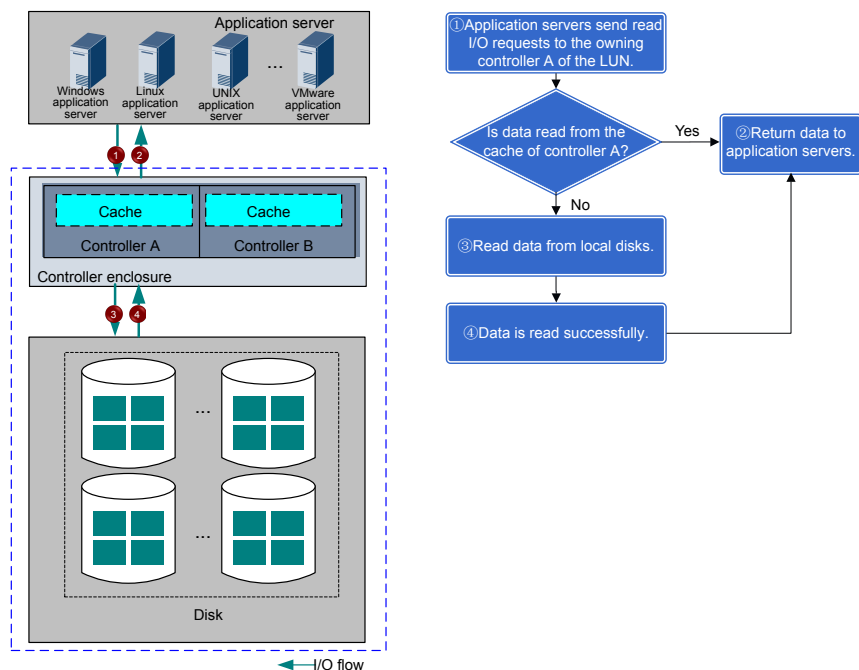
**Figure 1-3** Single controller enclosure scenario where an application server sends a write I/O request to a LUN



## Scenario 2: Single Controller Enclosure Scenario Where an Application Server Sends a Read I/O Request to a LUN

Figure 1-4 shows the single controller enclosure scenario where an application server sends a read I/O request to a LUN. The figure on the left shows the principles of delivering a read I/O request from an application server to a LUN in the single controller enclosure scenario. The figure on the right shows the principles in a flowchart.

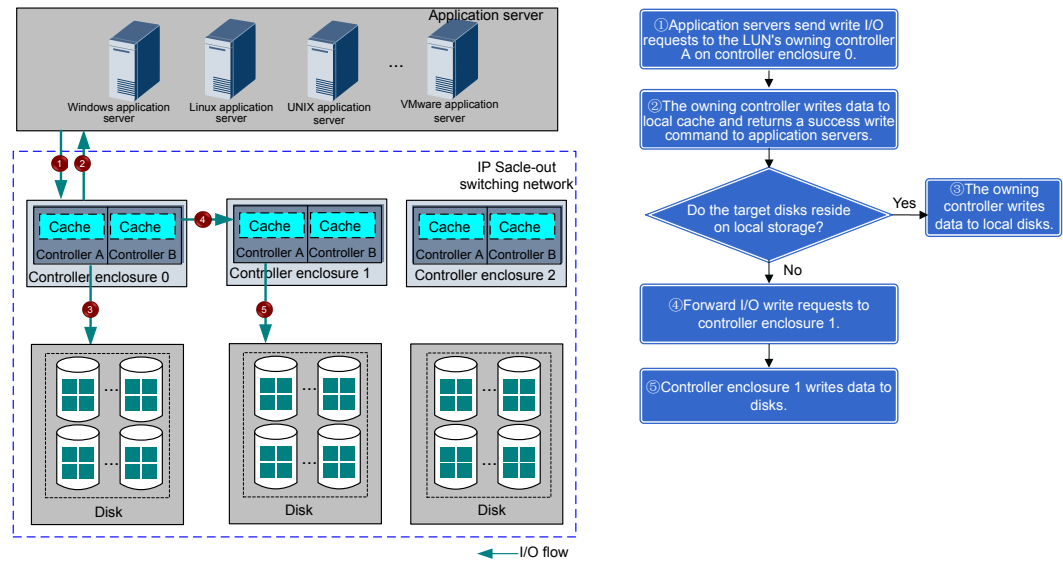
**Figure 1-4** Single controller enclosure scenario where an application server sends a read I/O request to a LUN



### Scenario 3: Multiple-Controller Enclosure Scenario Where an Application Server Sends a Write I/O Request to a LUN

Figure 1-5 shows the multiple-controller enclosure scenario where an application server sends a write I/O request to a LUN whose working and owning controllers are the same. The figure on the left shows the principles of delivering a write I/O request from an application server to a LUN in the scenario of multiple controller enclosures. The figure on the right shows the principles in a flowchart.

**Figure 1-5** Multiple-controller enclosure scenario where an application server sends a write I/O request to a LUN



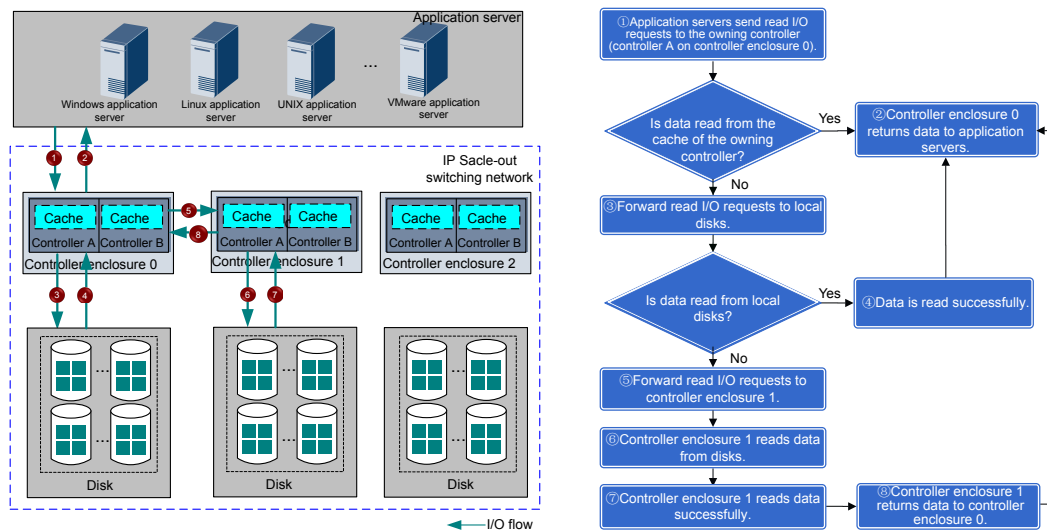
**NOTE**

Scale-out: In scale-out mode, storage systems are expanded by adding nodes such as engines or controllers to satisfy increasing storage requirements. The scale-out technology aims to establish network storage architecture where disk capacities can be expanded on demand. If disk capacities of existing nodes are insufficient, customers can add new nodes to expand capacities. Newly added nodes and existing nodes are connected using switching technologies. From the customers' perspective, the storage system with newly added nodes is still the original storage system. Besides, the scale-out technology implements load balancing among multiple controllers and provides functions such as fault tolerance to improve the processing capability and reliability of the storage system.

**Scenario 4: Multiple-Controller Enclosure Scenario Where an Application Server Sends a Read I/O Request to a LUN**

Figure 1-6 shows the multiple-controller enclosure scenario where an application server sends a read I/O request to a LUN whose working and owning controllers are the same. The figure on the left shows the principles of delivering a read I/O request from an application server to a LUN in the scenario of multiple controller enclosures. The figure on the right shows the principles in a flowchart.

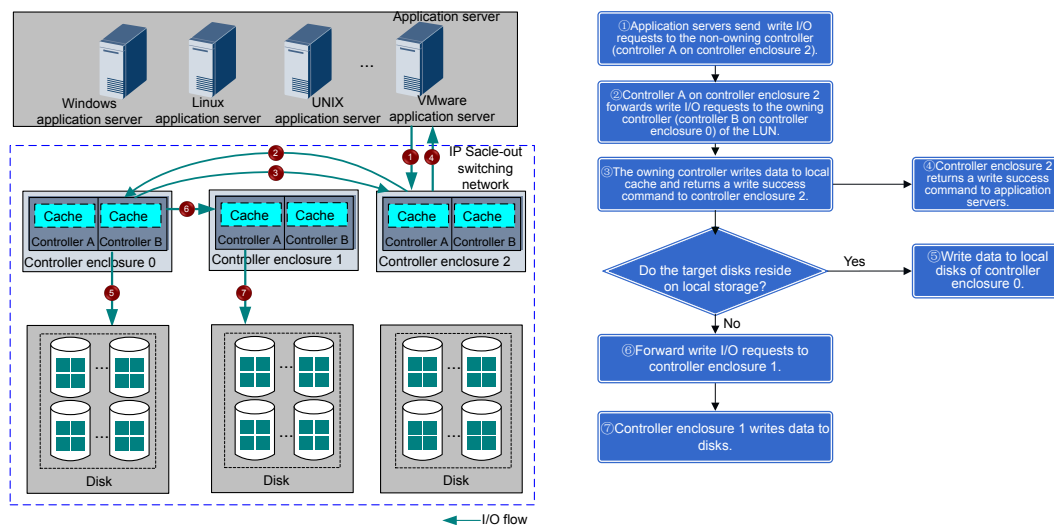
**Figure 1-6** Multiple-controller enclosure scenario where an application server sends a read I/O request to a LUN



### Scenario 5: Write Process in the Multiple-Controller Enclosure Scenario Where the Working and Owing Controllers of a LUN Are Different

When the working and owning controllers of a LUN are different, I/O requests to the LUN are forwarded by the working controller to the owning controller and then processed by the owning controller. **Figure 1-7** shows the scenario where an application server sends a write I/O request to a LUN. The figure on the left shows the principles of delivering a write I/O request from an application server to a LUN in the scenario of multiple controller enclosures. The figure on the right shows the principles in a flowchart.

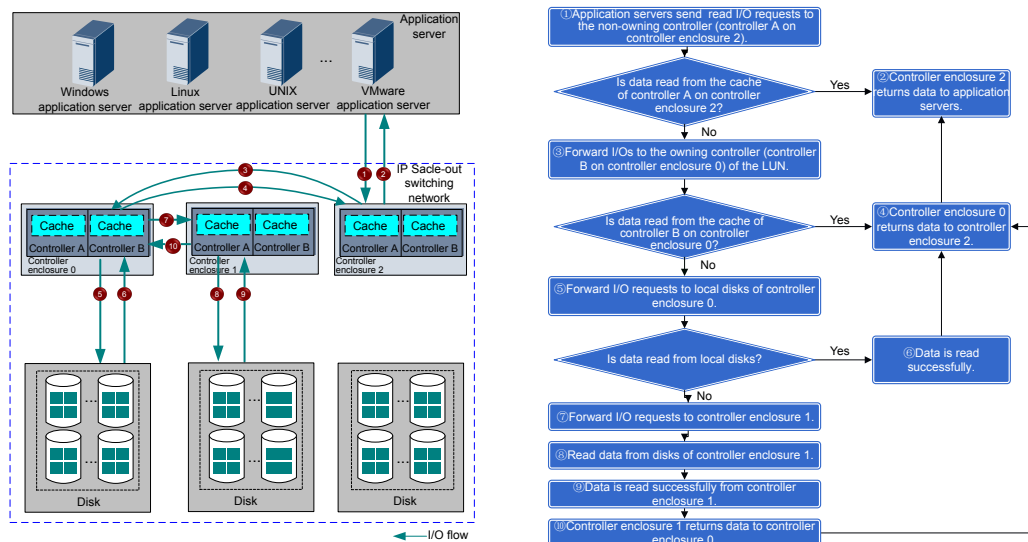
**Figure 1-7** Write process in the multiple-controller enclosure scenario where the working and owning controllers of a LUN are different



## Scenario 6: Read Process in the Multiple-Controller Enclosure Scenario Where the Working and Owning Controllers of a LUN Are Different

When the working and owning controllers of a LUN are different, I/O requests to the LUN are forwarded by the working controller to the owning controller and then processed by the owning controller. **Figure 1-8** shows the scenario where an application server sends a read I/O request to a LUN. The figure on the left shows the principles of delivering a read I/O request from an application server to a LUN in the scenario of multiple controller enclosures. The figure on the right shows the principles in a flowchart.

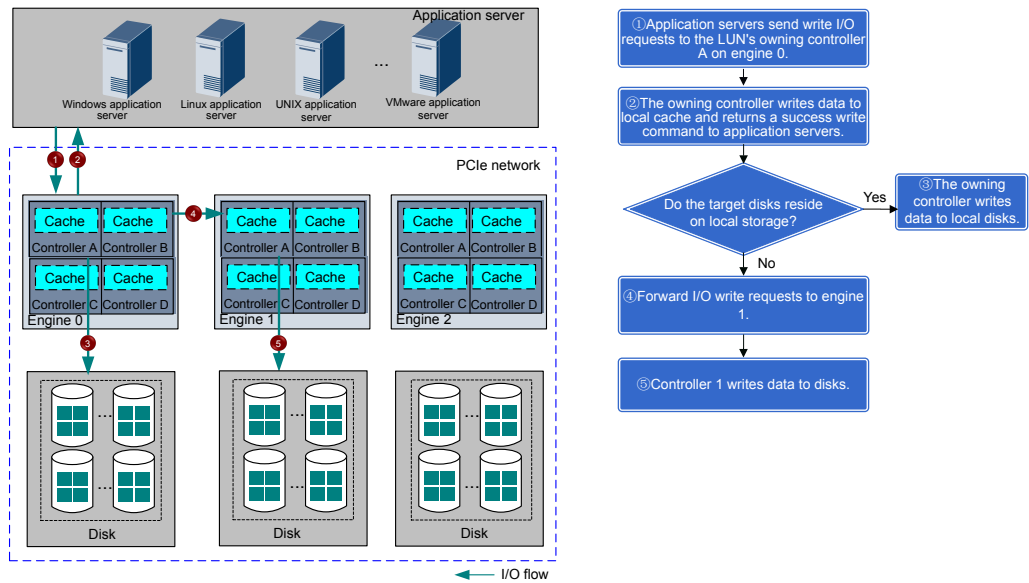
**Figure 1-8** Read process in the multiple-controller enclosure scenario where the working and owning controllers of a LUN are different



## Scenario 7: Multiple-Engine Scenario Where an Application Server Sends a Write I/O Request to a LUN (18000 and 18000F Series Storage Systems)

**Figure 1-9** shows the multiple-engine scenario where an application server sends a write I/O request to a LUN whose working and owning controllers are the same.

**Figure 1-9** Scenario where an application server sends a write I/O request to a LUN



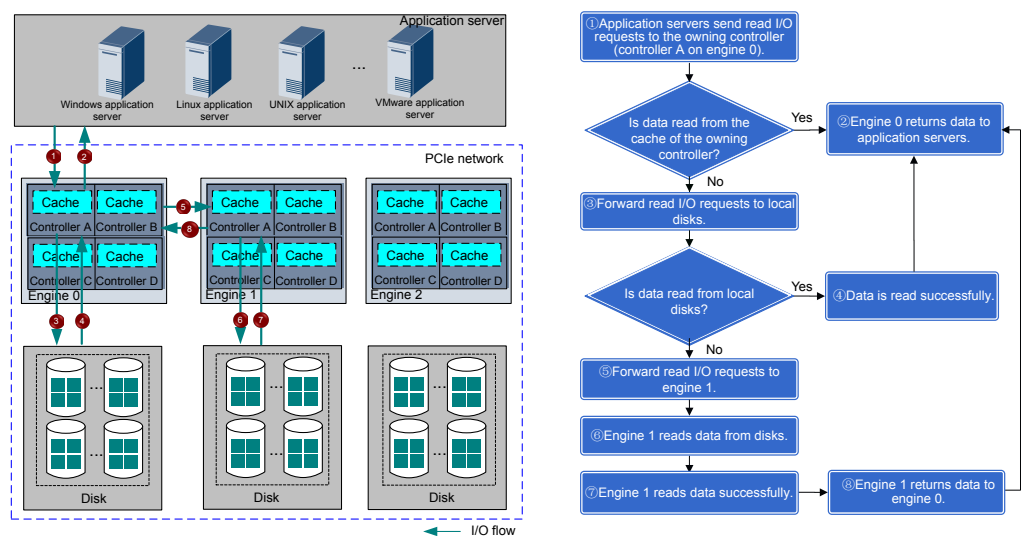
**NOTE**

The figure on the left shows the write principle when the working controller is an owning one and the figure on the right shows the principles in a flowchart.

**Scenario 8: Multiple-Engine Scenario Where an Application Server Sends a Read I/O Request to a LUN (18000 and 18000F Series Storage Systems)**

**Figure 1-10** shows the multiple-engine scenario where an application server sends a read I/O request to a LUN whose working and owning controllers are the same.

**Figure 1-10** Scenario where an application server sends a read I/O request to a LUN



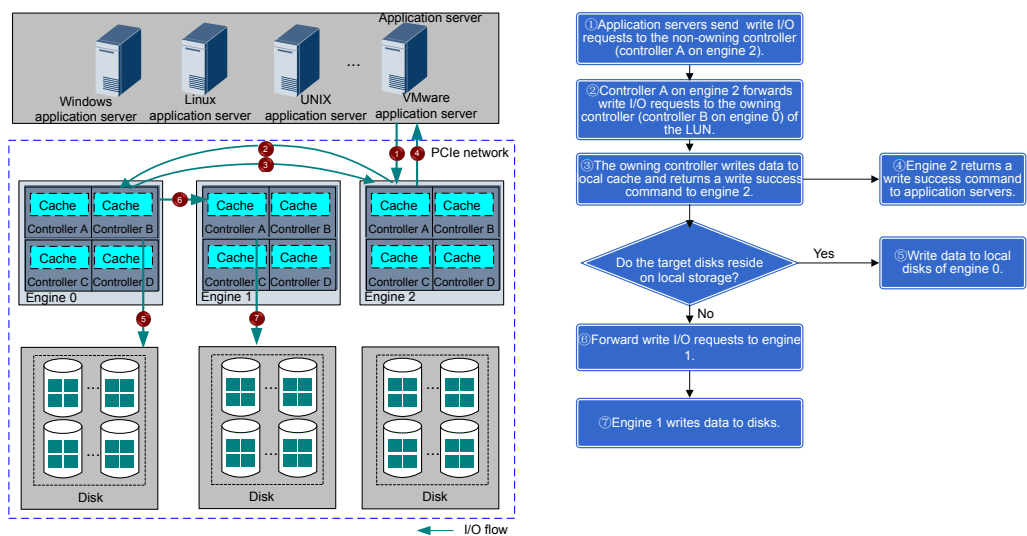
**NOTE**

The figure on the left shows the read principle when the working controller is an owning one and the figure on the right shows the principles in a flowchart.

### Scenario 9: Write Process in the Multiple-Engine Scenario Where the Working and Owning Controllers of a LUN Are Different (18000 and 18000F Series Storage Systems)

When the working and owning controllers of a LUN are different, I/O requests are forwarded by the working controller to the owning controller and then processed by the owning controller. **Figure 1-11** shows the multiple-engine scenario where an application server sends a write I/O request to a LUN.

**Figure 1-11** Write process where the working and owning controllers of a LUN are different



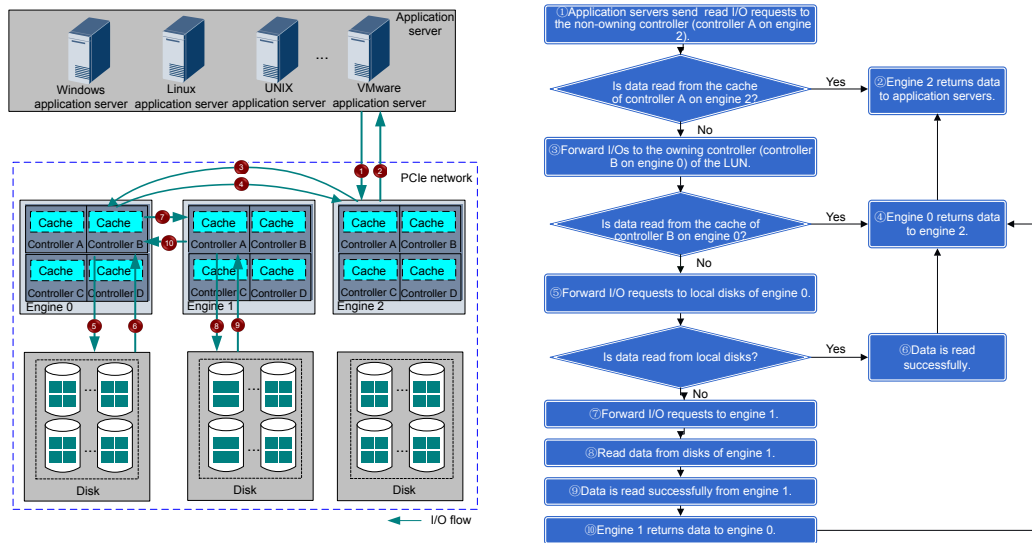
**NOTE**

The figure on the left shows the write principle when the working controller is a non-owning one and the figure on the right shows the principles in a flowchart.

### Scenario 10: Read Process in the Multiple-Engine Scenario Where the Working and Owning Controllers of a LUN Are Different (18000 and 18000F Series Storage Systems)

When the working and owning controllers of a LUN are different, I/O requests are forwarded by the working controller to the owning controller and then processed by the owning controller. **Figure 1-12** shows the multiple-engine scenario where an application server sends a read I/O request to a LUN.

**Figure 1-12** Read process where the working and owning controllers of a LUN are different



**NOTE**

The figure on the left shows the read principle when the working controller is a non-owning one and the figure on the right shows the principles in a flowchart.

### Scenarios Where the LUN Write Mode Becomes Write Through

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



**Table 1-1** Scenarios where the write mode of LUNs shifts from write back to write through and recommended actions

Symptom	Scenario	Impact and Recommended Action
<p>The temperature of a controller exceeds the upper limit.</p>	<ul style="list-style-type: none"> <li>● If the <b>Controller Enclosure Temperature Exceeds The Upper Limit</b> alarm is generated due to an exception in the equipment room temperature or the internal components of a storage system, LUNs continue the write back mode within a specified period of time (192 hours). If the alarm persists after the specified period of time, LUNs change the write mode to write through.</li> <li>● If the <b>Controller Enclosure Temperature Exceeds The Upper Limit</b> alarm is generated due to a fault on a single controller of a controller enclosure, LUNs continue the write back mode within a specified period of time (1 hour). If the alarm persists after the specified period of time, LUNs change the write mode to write through.</li> </ul> <p><b>NOTE</b>                      If the <b>Controller Enclosure Temperature Is Far Beyond The Upper Limit</b> alarm is generated in a storage system, the storage system will automatically power off.</p>	<ul style="list-style-type: none"> <li>● <b>Impact</b>                              The write mode of service objects on the entire controller becomes write through.</li> <li>● <b>Recommended action</b>                              Check the external refrigerating system, fan modules, and air channels to locate the overtemperature causes and rectify faults.</li> </ul>

Symptom	Scenario	Impact and Recommended Action
<p>Backup battery units (BBUs) on a controller enclosure malfunction.</p>	<ul style="list-style-type: none"> <li>● Dual-controller storage device: If two BBUs malfunction and an alarm is generated, the write mode of LUNs shifts from write back to write through.</li> <li>● Four-controller storage device: If two or more BBUs malfunction and an alarm is generated, the write mode of LUNs shifts from write back to write through.</li> </ul>	<ul style="list-style-type: none"> <li>● Impact The write mode of service objects on the entire controller enclosure becomes write through.</li> <li>● Recommended action <ul style="list-style-type: none"> <li>- Check whether BBUs are properly inserted.</li> <li>- Check whether the BBUs break down. If the BBUs break down, replace them with spare parts.</li> <li>- Check whether the power of the BBUs is insufficient. If the power of the BBUs is insufficient, wait until the BBUs are fully charged.</li> </ul> </li> </ul>
<p>The coffer disks of a controller enclosure malfunction.</p>	<ul style="list-style-type: none"> <li>● Dual-controller storage device: If two coffer disks break down, the write mode of LUNs shifts from write back to write through.</li> <li>● Four-controller storage device: If all coffer disks of controllers A and B or controllers C and D break down (the controllers in the first row are controllers A and B and the controllers in the second row are controllers C and D), the write mode of LUNs shifts from write back to write through.</li> </ul>	<ul style="list-style-type: none"> <li>● Impact The write mode of service objects on the entire controller enclosure becomes write through.</li> <li>● Recommended action Check whether the coffer disks are faulty. If the coffer disks are faulty, replace them with spare parts.</li> </ul>

Symptom	Scenario	Impact and Recommended Action
A controller malfunctions.	By default, the write mode of LUNs remains write back within a certain period (192 hours) after a single controller malfunctions. If the fault is not rectified within this period, the write mode of LUNs shifts from write back to write through.	<ul style="list-style-type: none"> <li>● Impact The write mode of service objects on the entire controller enclosure becomes write through if the fault persists after 192 hours.</li> <li>● Recommended action                             <ul style="list-style-type: none"> <li>- Replace the faulty controller at the off-peak point within the write back protection period.</li> <li>- If a spare part is unavailable during the write back protection period, prolong the protection period properly after assessing risks to prevent write through from adversely affecting service performance.</li> </ul> </li> </ul>
The remaining capacity of a storage pool is smaller than the reserved capacity.	An alarm is generated, indicating that the capacity usage of a storage pool exceeds the threshold and reminding you to expand the capacity.	<ul style="list-style-type: none"> <li>● Impact The write mode of thin LUNs and thick LUNs with value-added features shifts from write back to write through.</li> <li>● Recommended action Expand the capacity of the storage pool.</li> </ul>

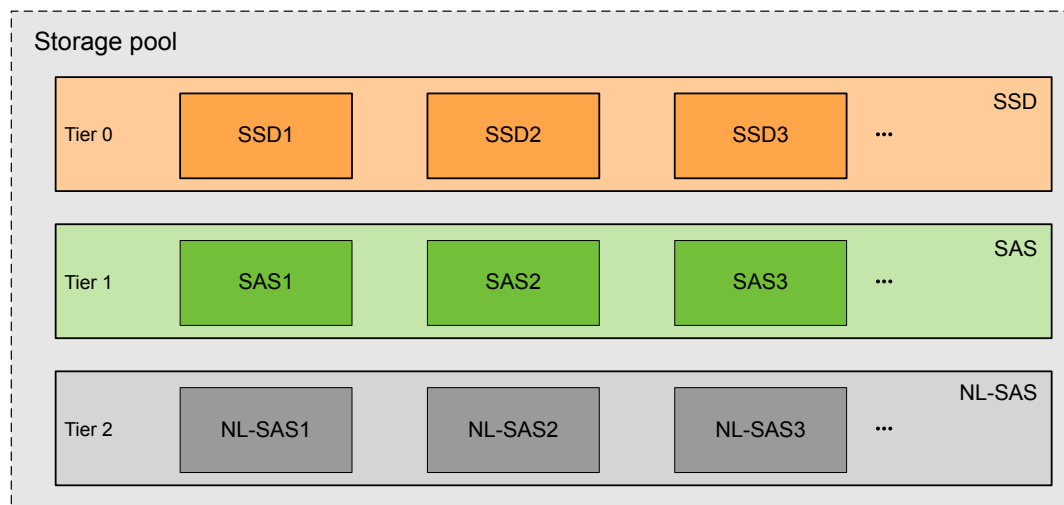
## 1.4.2 Operating Principles in a Storage System

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

### Storage Pool Structure

**Figure 1-13** shows the structure of a storage pool.

**Figure 1-13** Structure of a storage pool



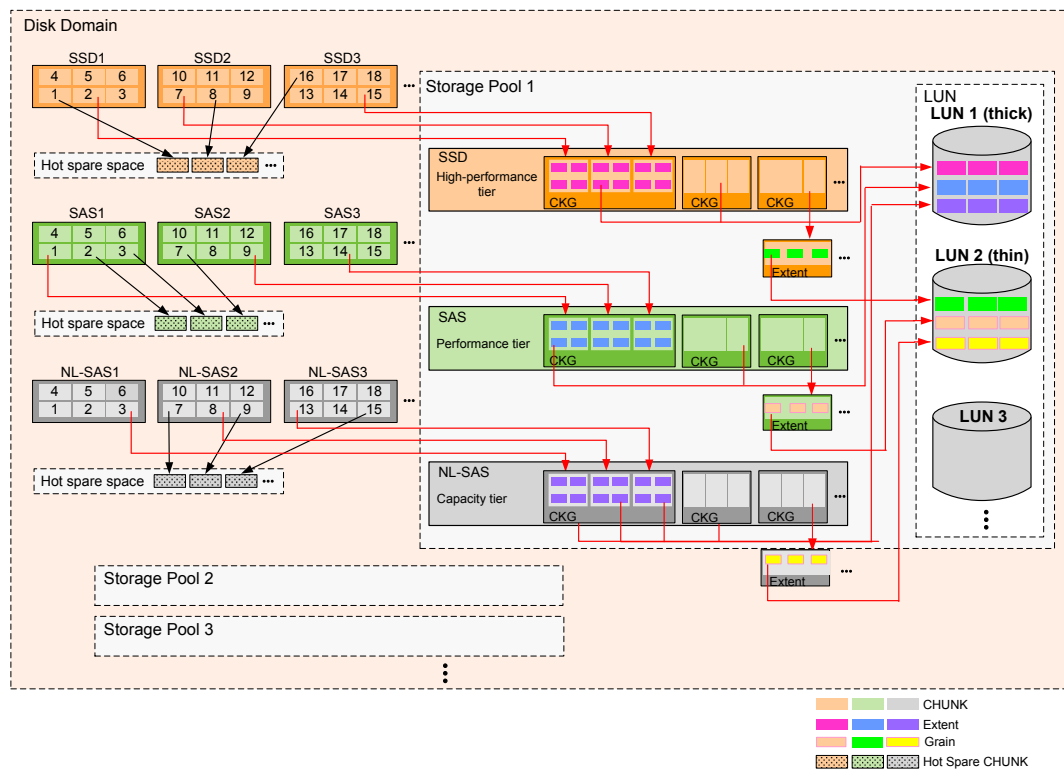
A storage pool consists of three storage tiers at most. Each storage tier is constructed by the same type of storage media.

- Tier 0 is the high performance tier, which is composed of SSDs. Tier 0 provides the highest performance at a high cost. It is used to store frequently accessed data.
- Tier 1 is the performance tier, which is composed of serial attached SCSI (SAS) disks. Tier 1 provides high performance at a moderate cost. It is used to store less frequently accessed data.
- Tier 2 is the capacity tier, which is composed of near line serial attached SCSI (NL-SAS) disks. Tier 2 provides moderate performance and a large capacity per disk at a low cost. It is used to store a large amount of seldom-accessed data.

## Block Virtualization Process

[Figure 1-14](#) shows the block virtualization process.

**Figure 1-14** Block virtualization process



The process of creating storage through block virtualization is as follows:

1. The disks on a storage system can be divided into multiple disk domains. A disk domain consists of the same type or different types of disks. Disk types of a disk domain determine the storage tiers of storage pools. The number of storage pools that can be created in a disk domain depends on the capacity of the disk domain.
2. The storage system divides the storage media in disk domains into CKs. Each CK has a fixed size, which cannot be changed.
3. When creating a disk domain, the storage system assigns it the default hot spare policy. When a disk is faulty, the storage system allocates free CKs in real time as hot spare space based on the disk usage.
4. A storage pool in a disk domain supports a maximum of three storage tiers. Each storage tier consists of the same type of CKGs.
  - The high performance tier consists of CKGs provided by SSDs and delivers the highest performance among the three tiers. As SSDs have a high cost and low capacity, the high performance tier is suitable for storing frequently accessed data.
  - The performance tier consists of CKGs provided by SAS disks and delivers high performance. As SAS disks have a moderate cost and large capacity, the performance tier is suitable for storing less frequently accessed data.
  - The capacity tier consists of CKGs provided by NL-SAS disks and delivers the lowest performance among the three tiers. As NL-SAS disks have the lowest cost and largest capacity, the capacity tier is suitable for storing a large amount of seldom-accessed data.
5. A CKG is formed by CKs in a storage tier based on the RAID policy configured on the DeviceManager. CKs of each CKG come from different disks. You can set the RAID

policy for each storage tier. The RAID policy specifies the RAID level of a storage tier and the number of data blocks and parity blocks for this RAID level.

6. The storage system divides CKGs into extents based on the data migration granularity configured on the DeviceManager. The extent is the smallest unit of a thick LUN. The extents may vary according to storage pools but must be the same in one storage pool.
7. The LUNs used by application servers are composed of extents. Space application, space release, and data relocation of LUNs are based on extents. When creating a LUN, you can specify that the capacity of the LUN comes from a storage tier. In this case, the LUN is composed of the extents in the storage tier. When the services are running, the storage system relocates data among the storage tiers based on the data activity level and data relocation policy (this function requires a license). After that, data on the LUN is distributed by extent to the storage tiers in the storage pool.

When a user creates a thin LUN, the storage system divides extents into grains and maps the grains to the thin LUN. In this way, fine-grained management of storage capacity is accomplished.

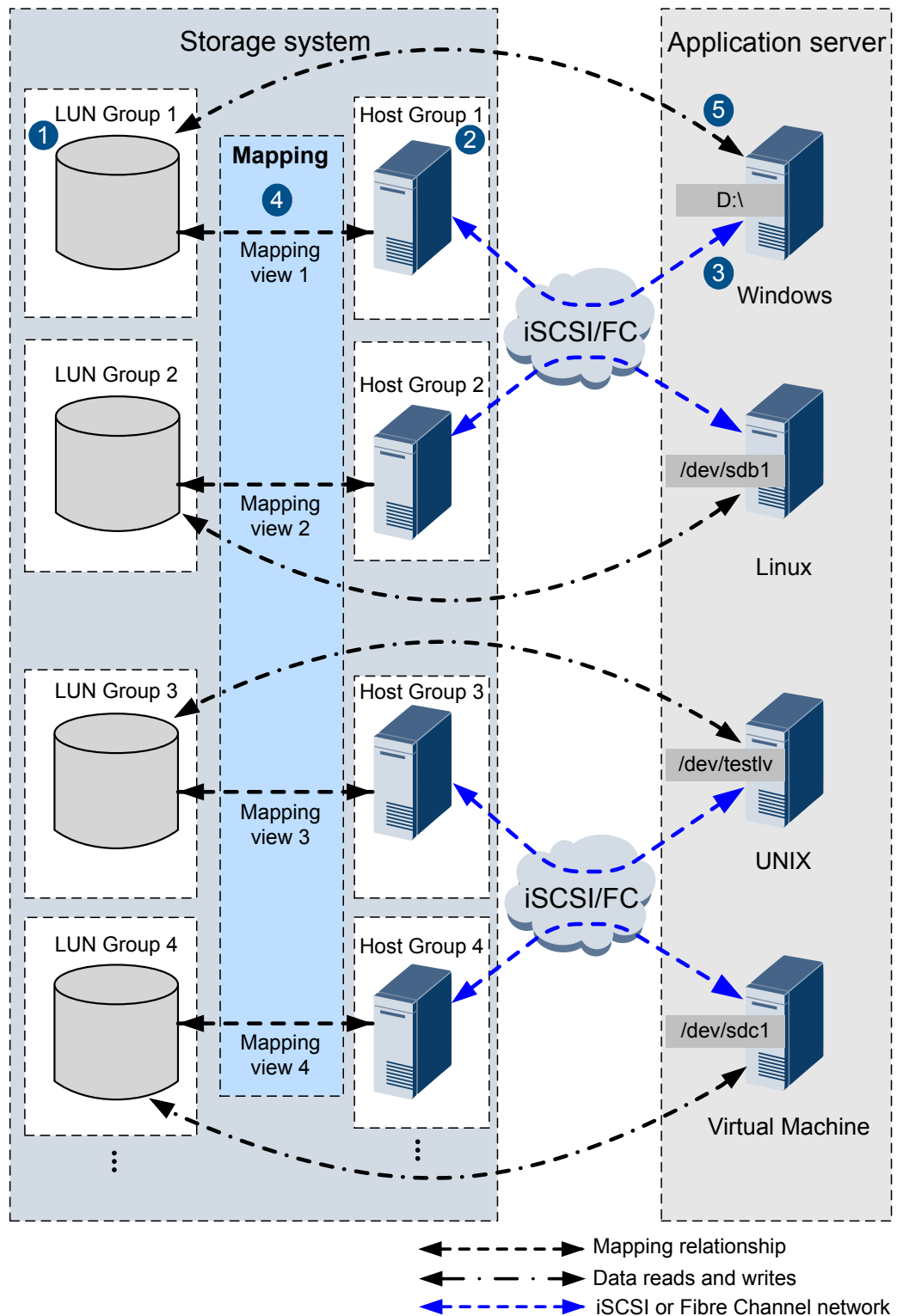
 **NOTE**

Multiple extents form a LUN. When creating a LUN, you are advised to specify the LUN capacity to a value that is an integer multiple of extents. Otherwise, when the LUN applies for space in the unit of extent, the storage system allocates space that is an integer multiple of extents and larger than the specified capacity to the LUN, wasting certain capacity. For example, the capacity of a storage pool is 1 GB and an extent contains 4 MB. If the capacity of a thick LUN is set to 1 MB, the thick LUN capacity is displayed as 1 MB but actually the thick LUN occupies 4 MB. The remaining capacity that can be allocated is 1020 MB only. If you want to expand the thick LUN, the thick LUN can be expanded to 1021 MB at most. The thick LUN cannot be expanded to 1 GB.

## Process for Making Storage Space Available

[Figure 1-15](#) shows the process for making storage space available.

**Figure 1-15** Process for making storage space available



1. Create LUNs based on the specific names, capacity, and number of LUNs. To facilitate LUN management, the storage system directly manages LUN groups instead of

individual LUNs. After LUNs are created, you need to create a LUN group for those LUNs so that they can be added to a mapping view.

2. A host represents an application server on a storage system. Following **Create Host Wizard** on the DeviceManager, link hosts with application servers. To facilitate host management, the storage system directly manages host groups instead of individual hosts. After hosts are created, you need to create a host group for those hosts so that they can be added to a mapping view.
3. **Optional:** On an Internet Small Computer Systems Interface (iSCSI) network, you must configure iSCSI initiators on application servers for the application servers to properly communicate with the storage system. When using a Fibre Channel network, you do not need to perform this operation.
4. After a mapping view is created, and a host group and a LUN group are added to the mapping view, the application servers, host group, and LUN group are logically associated. Then the application servers can detect LUNs in the LUN group.
5. Scan for LUNs on the application servers. The allocated storage space will be discovered. The application servers can use the storage space as local disks.



# 2 Planning Basic Storage Services

---

## About This Chapter

To achieve a balance among the security, performance, and cost, make appropriate plans to facilitate subsequent configuration and maintenance before configuring basic storage services.

### [2.1 Planning Process](#)

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

### [2.2 Planning Applications](#)

The storage system provides application-based wizards to create storage resources. The applications include Microsoft Exchange, VMware, Hyper-V, Oracle, and SQL Server. Therefore, you can use the corresponding wizard to create storage resources for the preceding five applications. To create storage resources for other applications, follow the configuration procedure for basic storage services.

### [2.3 Planning the Capacity](#)

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

### [2.4 Planning Ports and Service Data](#)

To smoothly configure basic storage services, you must prepare or plan the required data based on your site requirements.

### [2.5 Planning Disk Domains](#)

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

### [2.6 Planning Storage Pools](#)

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

### [2.7 Planning LUNs](#)

Select appropriate LUN types, read/write policies, and prefetch policies for LUNs based on the data storage requirements to achieve the optimal performance of the storage system.

### [2.8 \(Optional\) Planning iSCSI CHAP](#)

To ensure the storage system access security, plan iSCSI CHAP to control the access to the storage system.

### 2.9 Planning Management User Accounts

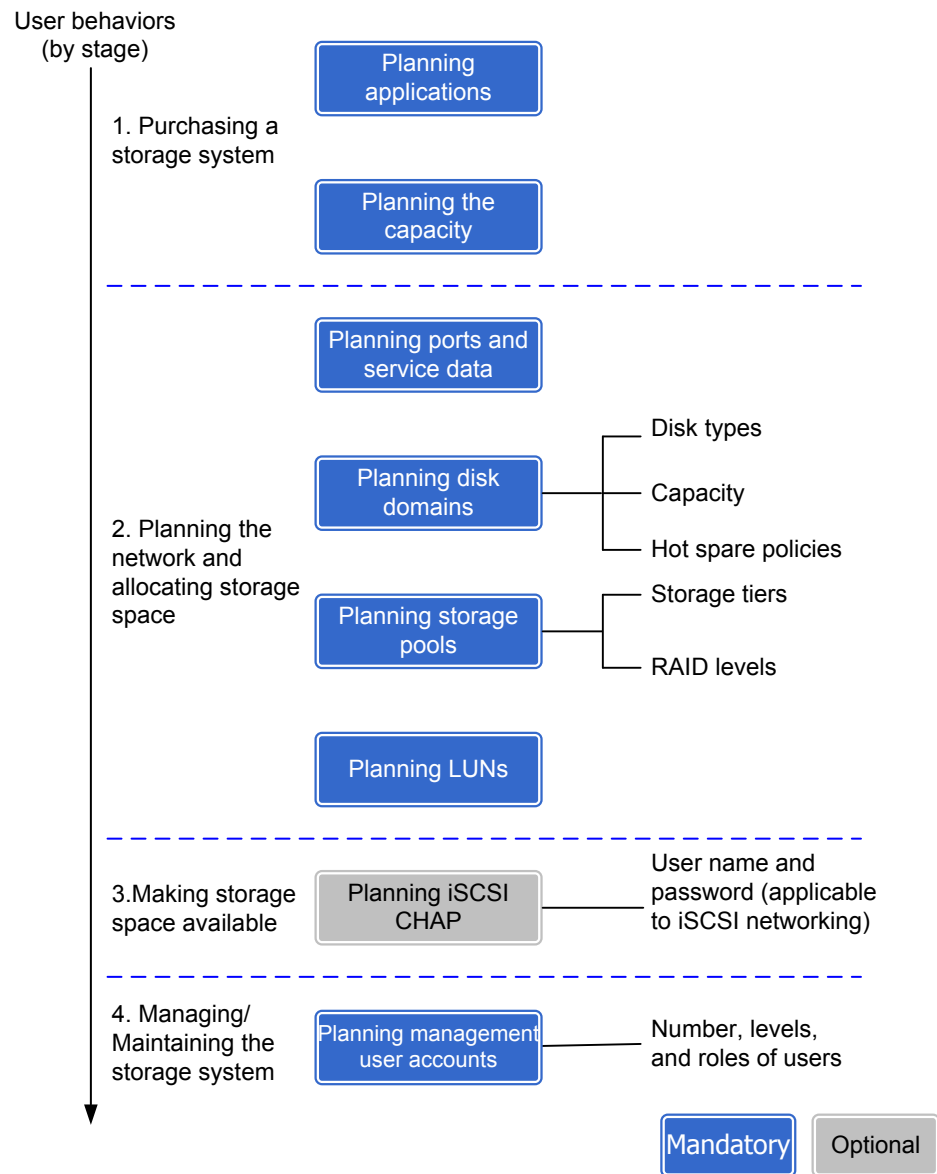
Any user that has logged in to a storage system can operate the storage system. Misoperations by a user can impair the storage system reliability and data integrity. To prevent misoperations, the storage system defines types of users and assigns specific roles to them based on different service scenarios.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

## 2.1 Planning Process

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

**Figure 2-1** shows the recommended planning process, which is based on user behavior in different stages.

**Figure 2-1** Planning process



**Table 2-1** describes the planning items.

**Table 2-1** Planning items

User Behavior	Item	Description	Reference
1. Purchasing a storage system	Planning applications	The 2000, 5000 and 6000 series storage systems provide application-based wizards to create storage resources. The applications include Microsoft Exchange, VMware, Hyper-V, Oracle, and SQL Server. Therefore, you can use the corresponding wizard to create storage resources for the preceding five applications. To create storage resources for other applications, follow the configuration procedure for basic storage services.	<a href="#">2.2 Planning Applications</a>
	Planning the capacity	Storage capacity is users' basic requirement and must be planned first of all.	<a href="#">2.3 Planning the Capacity</a>
2. Planning the network and allocating storage space	Planning ports and service data	To smoothly configure basic storage services, you must prepare or plan the required data based on your site requirements.	<a href="#">2.4 Planning Ports and Service Data</a>
	Planning disk domains	<p>A disk domain provides storage space for storage pools, whose storage tiers and available capacities depend on the disk types, capacity, and hot spare policy of the disk domain. Therefore, the disk types, capacity, and hot spare policy must be properly planned for a disk domain.</p> <ul style="list-style-type: none"> <li>● Disk type: Disk types of a disk domain determine the storage tiers of storage pools. Plan disk types based on your requirements.</li> <li>● Capacity: The capacity of a disk domain determines the available capacities of storage pools.</li> <li>● Hot spare policy: Plan hot spare policies and hot spare space so that the hot spare space can take over data from failed member disks.</li> </ul>	<a href="#">2.5 Planning Disk Domains</a>

User Behavior	Item	Description	Reference
	Planning storage pools	<p>A storage system provides storage space for application servers in the form of storage pools.</p> <p>The storage tiers and RAID levels of the storage pools must be properly planned in advance for better storage utilization.</p> <ul style="list-style-type: none"> <li>● Storage tier: Plan storage tiers to meet the need for optimal distribution of hot data and cold data.</li> <li>● RAID level: Plan RAID levels based on actual needs because RAID levels vary in performance, cost, and reliability.</li> </ul>	<a href="#">2.6 Planning Storage Pools</a>
	Planning LUNs	<p>Different read/write policies configured for LUNs affect the response time of the storage system. Properly planned write policies and prefetch policies can help improve the response speed of the storage system.</p>	<a href="#">2.7 Planning LUNs</a>
3. Making storage space available	(Optional) Planning iSCSI CHAP	<p>Considering the storage system access security when application servers connect to the storage system through iSCSI and use the storage space provided by the storage system, plan the CHAP user name and password to control the access to the storage system.</p>	<a href="#">2.8 (Optional) Planning iSCSI CHAP</a>
4. Managing/Maintaining the storage system	Planning management user accounts	<p>Plan the number of users and their privileges carefully for subsequent management and maintenance. Users with different responsibilities should have different permissions.</p>	<a href="#">2.9 Planning Management User Accounts</a>

## Compatibility

When configuring storage services, ensure that the host operating system, multipathing software, and switches are compatible with each other. You can query the compatibility using the [OceanStor Interoperability Navigator](#).

## 2.2 Planning Applications

The storage system provides application-based wizards to create storage resources. The applications include Microsoft Exchange, VMware, Hyper-V, Oracle, and SQL Server.

Therefore, you can use the corresponding wizard to create storage resources for the preceding five applications. To create storage resources for other applications, follow the configuration procedure for basic storage services.

The storage system provides two storage resource creation methods: one based on applications and one based on the configuration procedure of basic storage services. Normally, all storage resources are created following the configuration procedure of basic storage services. However, if Microsoft Exchange, VMware, Hyper-V, Oracle, and SQL Server are involved, you can use the corresponding storage resource wizard provided by the storage system to create storage resources. Therefore, before you configure services, check whether the previous five applications are involved. [Table 2-2](#) shows the details of the two configuration methods.

**Table 2-2** Two methods of creating storage resources

Application Type	Method of Creating Storage Resources	Reference
Microsoft Exchange, VMware, Hyper-V, Oracle, and SQL Server	Create storage resources using the corresponding wizard provided by the storage system.	<a href="#">5 Creating Storage Resources Based on Applications</a>
Other applications	Create storage resources by following the configuration procedure for basic storage services.	<a href="#">3 Configuring Basic Storage Services</a>

Before you use the application-based method to create storage resources, ensure that a storage pool for the specific application exists in the storage system. All required LUNs, LUN groups, and host groups are automatically configured, which significantly reduces planning and configuration time and improves configuration efficiency.

Since the five applications have different requirements on storage media and RAID policies in the storage pool, the configuration procedures for the five applications may be different:

- If there is no storage pool in the storage system or none of the existing storage pools meet the application's requirements, create a new storage pool following instructions displayed on the wizard. For details, see [3.5 Creating a Storage Pool](#).
- If any of the existing storage pools meets the application's requirements and the capacity in the pool is sufficient, the storage system automatically matches with the pool. You can use the storage resource creation wizard to configure services to enable the application server to use the storage resources of the application.

## 2.3 Planning the Capacity

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

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

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

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

**Table 2-3** lists the disk utilization of different RAID levels.

**Table 2-3** Disk utilization of different RAID levels

RAID Level	Disk Utilization
RAID 0	The disk utilization is 100%.
RAID 1	<ul style="list-style-type: none"> <li>● 2D<sup>a</sup>: The disk utilization is about 50%.</li> <li>● 4D: The disk utilization is about 25%.</li> </ul>
RAID 3	<p>RAID 3 supports flexible configurations. Specifically, a RAID 3 policy allows data block and parity block policies ranging from 2D+1P to 13D+1P. The following examples show disk utilization rates of several configurations commonly used by RAID 3:</p> <ul style="list-style-type: none"> <li>● 4D + 1P<sup>b</sup>: The disk utilization is about 80%.</li> <li>● 2D + 1P: The disk utilization is about 66.67%.</li> <li>● 8D + 1P: The disk utilization is about 88.89%.</li> </ul> <p><b>NOTE</b> For a flexibly configured RAID policy <math>x\mathbf{D}+y\mathbf{P}</math>, the disk utilization is <math>[x/(x + y)] \times 100\%</math>.</p>
RAID 5	<p>RAID 5 supports flexible configurations. Specifically, a RAID 5 policy allows data block and parity block policies ranging from 2D+1P to 13D+1P. The following examples show disk utilization rates of several configurations commonly used by RAID 5:</p> <ul style="list-style-type: none"> <li>● 2D + 1P: The disk utilization is about 66.67%.</li> <li>● 4D + 1P: The disk utilization is about 80%.</li> <li>● 8D + 1P: The disk utilization is about 88.89%.</li> </ul> <p><b>NOTE</b> For a flexibly configured RAID policy <math>x\mathbf{D}+y\mathbf{P}</math>, the disk utilization is <math>[x/(x + y)] \times 100\%</math>.</p>
RAID 6	<p>RAID 6 supports flexible configurations. Specifically, a RAID 6 policy allows data block and parity block policies ranging from 2D+2P to 26D+2P. The following examples show disk utilization rates of several configurations commonly used by RAID 6:</p> <ul style="list-style-type: none"> <li>● 2D + 2P: The disk utilization is about 50%.</li> <li>● 4D + 2P: The disk utilization is about 66.67%.</li> <li>● 8D + 2P: The disk utilization is about 80%.</li> <li>● 16D + 2P: The disk utilization is about 88.89%.</li> </ul> <p><b>NOTE</b> For a flexibly configured RAID policy <math>x\mathbf{D}+y\mathbf{P}</math>, the disk utilization is <math>[x/(x + y)] \times 100\%</math>.</p>

RAID Level	Disk Utilization
RAID 10	The disk utilization is 50%.
RAID 50	<ul style="list-style-type: none"> <li>● (2D + 1P) x 2: The disk utilization is about 66.67%.</li> <li>● (4D + 1P) x 2: The disk utilization is about 80%.</li> <li>● (8D + 1P) x 2: The disk utilization is about 88.89%.</li> </ul>
a: <b>D</b> indicates the data block. b: <b>P</b> indicates the parity block.	

- Capacity used by hot spare space

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

- ■ High

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

- ■ Low

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

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

The system does not provide hot spare space.

**Table 2-4** describes how hot spare space changes with the number of disks. The hot spare space changes at a storage tier are used as an example here. The hot spare space changes at different types of storage tiers are the same.

**Table 2-4** Changes of hot spare space

Number of Disks	Number of Disks of Which Capacity Is Used as Hot Spare Space in High Hot Spare Policy <sup>a</sup>	Number of Disks of Which Capacity Is Used as Hot Spare Space in Low Hot Spare Policy <sup>a</sup>
(1, 12]	1	1
(12, 25]	2	
(25, 50]	3	2
(50, 75]	4	
(75, 125]	5	3



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

 **NOTE**

- For 18000 and 18000F series storage systems, the high hot spare policy is used by default. You can only run the **change disk\_domain general** command on the CLI to modify the hot spare policy.
- When you are creating a disk domain, ensure that the disks used to provide hot spare space are sufficient.
- Hot spare space can be used for the current disk domain only.
- **Table 2-4** lists common capacity changes of the hot spare space. The number of disks supported by a storage system and the capacity of their hot spare space are based on actual specifications.

● Capacity used by coffer disks

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

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

For the 18000 and 18000F series storage systems, the first four disks in the disk enclosure of the storage system are configured as coffer disks. Part of the coffer disk

space (each coffer disk requires 5 GB capacity, and four coffer disks require 20 GB in total) can be used to store critical system data, including configuration data and system logs. The rest of the coffer disk space can be used to store service data.

Capacity partitions of coffer disks are shown in [Table 2-5](#).

**Table 2-5** Description of coffer disk capacity partitions

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

 **NOTE**

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

- Capacity used by file systems and volume management software on the application server  
 File systems and volume management software of multiple types on the application server may occupy a portion of space in the storage system. The actually occupied capacities depend on the deployment of applications on the application server.
- WriteHole capacity  
 WriteHole is used to resolve inconsistent data stripe verification caused by certain operations before I/Os are delivered to disks. Each disk reserves a 256 MB space as WriteHole capacity.
- Capacity used by system information.  
 The system information occupies 577 MB per disk.
- Metadata capacity  
 Each disk reserves 0.6% of its total capacity as metadata capacity, and reserves 2% as metadata backup capacity.
- Reserved space for improving system performance and disk balance

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

- Integrated capacity

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

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

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

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

 **NOTE**

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

## Available Capacity Calculation Method

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

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

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

$$600 \text{ GB} \times (1000/1024) \times (1000/1024) \times (1000/1024) = 572204.590 \text{ MB}$$

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

$$572204.590 \text{ MB} \times (1 - 2\%) = 560760.500 \text{ MB}$$

2. Minus the WriteHole capacity:

$$560760.500 \text{ MB} - 256 \text{ MB} = 560504.500 \text{ MB}$$

3. Minus the reserved production space:

$$560504.500 \text{ MB} - 577 \text{ MB} = 559927.500 \text{ MB}$$

4. Minus the metadata capacity:

$$559927.500 \text{ MB} \times (1 - 0.6\%) = 556567.935 \text{ MB}$$

 **NOTE**

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

5. Minus the metadata backup capacity:  
 $556567.935 \text{ MB} \times (1 - 2\%) = 545436.576 \text{ MB}$
6. Minus the reserved space for improving system performance and disk balance:  
 $545436.576 \text{ MB} \times (1 - 1\%) = 539982.210 \text{ MB}$
7. Minus the integrated capacity:  $539982.210 \text{ MB} \times 98.46\% = 531666.484 \text{ MB}$
8. Because the hot spare policy of the storage system is set to **Low**, capacity of two disks is used as hot spare space capacity. Therefore, the remaining capacity is as follows after the hot space capacity is deducted:  
 $531666.484 \text{ MB} \times (48 - 2) = 24456658.264 \text{ MB}$   
Equals to  $24456658.264 \text{ MB} / 1024 / 1024 = 23.324 \text{ TB}$
9. Minus the coffer data capacity:  
 $23.324 \text{ TB} - 4 \times 5 \text{ GB} = 23.304 \text{ TB}$
10. Because the RAID policy of the storage system is RAID 6 (8D + 2P), the disk utilization is 80%. Therefore, the allowed expansion capacity is:  
 $23.304 \text{ TB} \times 80\% = 18.643 \text{ TB}$

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

 **NOTE**

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

## 2.4 Planning Ports and Service Data

To smoothly configure basic storage services, you must prepare or plan the required data based on your site requirements.

### Planning Ports in an iSCSI Networking Scenario

For an iSCSI networking scenario, you must plan the IP addresses of service ports and VLAN information. Using a 2 U controller enclosure as an example, [Table 2-6](#) lists the parameters that you must configure in an iSCSI networking scenario.

**Table 2-6** Parameters you must configure in an iSCSI networking scenario

Controller, Slot, and Port	IP Address	Switch Port	Application Server IP Address	VLAN
Controller A, ___ Slot, ___ Port	IP address: _____ Subnet mask (prefix): _____ Gateway: _____	Port that connects to the storage system: _____ Port that connects to the server: _____	IP address: _____ Subnet mask (prefix): _____ Gateway: _____	_____

Controller, Slot, and Port	IP Address	Switch Port	Application Server IP Address	VLAN
Controller A, __ Slot, __ Port	IP address: _____ Subnet mask (prefix): _____ Gateway: _____	Port that connects to the storage system: _____ Port that connects to the server: _____	IP address: _____ Subnet mask (prefix): _____ Gateway: _____	_____
Controller A, __ Slot, __ Port	IP address: _____ Subnet mask (prefix): _____ Gateway: _____	Port that connects to the storage system: _____ Port that connects to the server: _____	IP address: _____ Subnet mask (prefix): _____ Gateway: _____	_____
Controller A, __ Slot, __ Port	IP address: _____ Subnet mask (prefix): _____ Gateway: _____	Port that connects to the storage system: _____ Port that connects to the server: _____	IP address: _____ Subnet mask (prefix): _____ Gateway: _____	_____
Controller B, __ Slot, __ Port	IP address: _____ Subnet mask (prefix): _____ Gateway: _____	Port that connects to the storage system: _____ Port that connects to the server: _____	IP address: _____ Subnet mask (prefix): _____ Gateway: _____	_____
Controller B, __ Slot, __ Port	IP address: _____ Subnet mask (prefix): _____ Gateway: _____	Port that connects to the storage system: _____ Port that connects to the server: _____	IP address: _____ Subnet mask (prefix): _____ Gateway: _____	_____

Controller, Slot, and Port	IP Address	Switch Port	Application Server IP Address	VLAN
Controller B, ___ Slot, ___ Port	IP address: _____ Subnet mask (prefix): _____ Gateway: _____	Port that connects to the storage system: _____ Port that connects to the server: _____	IP address: _____ Subnet mask (prefix): _____ Gateway: _____	_____
Controller B, ___ Slot, ___ Port	IP address: _____ Subnet mask (prefix): _____ Gateway: _____	Port that connects to the storage system: _____ Port that connects to the server: _____	IP address: _____ Subnet mask (prefix): _____ Gateway: _____	_____

 **NOTE**

- For details about the ports in the table, see the information recorded in the "typical network solution" of the *Installation Guide* of the corresponding product model.
- If a service requires multiple specified ports to transfer data, you are advised to add the ports to the same port group.
- If the service requires multiple ports to increase the link redundancy, you are advised to bond the ports.

## Planning Ports in an FC Networking Scenario

For an FC networking scenario, you must prepare zones and the required ports. Using a 2 U controller enclosure as an example, [Table 2-7](#) lists the parameters that you must configure in an FC networking scenario.

**Table 2-7** Parameters you must configure in an FC networking scenario

Controller, Slot, and Port	Switch Port	Application Server WWN	Zone
Controller A, ___ Slot, ___ Port	Port that connects to the storage system: _____ Port that connects to the server: _____	_____	_____

Controller, Slot, and Port	Switch Port	Application Server WWN	Zone
Controller A, ___ Slot, ___ Port	Port that connects to the storage system: _____ Port that connects to the server: _____	_____	_____
Controller A, ___ Slot, ___ Port	Port that connects to the storage system: _____ Port that connects to the server: _____	_____	_____
Controller A, ___ Slot, ___ Port	Port that connects to the storage system: _____ Port that connects to the server: _____	_____	_____
Controller B, ___ Slot, ___ Port	Port that connects to the storage system: _____ Port that connects to the server: _____	_____	_____
Controller B, ___ Slot, ___ Port	Port that connects to the storage system: _____ Port that connects to the server: _____	_____	_____
Controller B, ___ Slot, ___ Port	Port that connects to the storage system: _____ Port that connects to the server: _____	_____	_____
Controller B, ___ Slot, ___ Port	Port that connects to the storage system: _____ Port that connects to the server: _____	_____	_____

 **NOTE**

- For details about the ports in the table, see **Typical Networks** in the *Installation Guide* of the corresponding product model.
- If a service requires specific ports to transfer data, you are advised to add the ports to a port group for use.

## Planning Service Data

Some ports on the storage device are reserved for internal communication. Do not disable these ports. For details about the ports, see the *Communication Matrix*. You can obtain the *Communication Matrix* from the Support website.

**Table 2-8** describes the data to be obtained before storage space configuration.

**Table 2-8** Planning service data

Operation	Item	Default/Actual Value
Creating a disk domain	<b>Disk domain name</b> Name of the disk domain to be created.	_____
	<b>Disk type</b> Disk types in the disk domain, which determine the storage tiers that can be created. SSDs correspond to the high performance tier, SAS disks correspond to the performance tier, and NL-SAS disks correspond to the capacity tier.	High performance Tier (SSD) _____ Performance Tier (SAS) _____ Capacity Tier (NL-SAS) _____
	<b>Hot Spare Policies</b> To prevent data loss or performance deterioration caused by a member disk failure, the storage system employs hot spare space to take over data from a failed member disk.	High _____ Low _____ None _____
Creating a storage pool	<b>Storage pool name</b> Name of the storage pool to be created.	_____
	<b>Storage tier</b> The storage pool can have the high performance tier, performance tier, and capacity tier. Each tier uses different types of disks. If you plan to apply SmartTier, the storage pool must have at least two storage tiers.	High performance Tier (SSD) _____ Performance Tier (SAS) _____ Capacity Tier (NL-SAS) _____



Operation	Item	Default/Actual Value
	<p><b>RAID policy</b></p> <p>Each tier is configured with a specific RAID policy. The default RAID policy on the DeviceManager is recommended. For example, the default RAID policy of the performance tier on the DeviceManager is <b>RAID5 4D+1P</b>, where D indicates the data block and P indicates the parity block.</p>	<p>High performance Tier _____</p> <p>Performance Tier _____</p> <p>Capacity Tier _____</p>
	<p><b>Capacity</b></p> <p>Capacity of each storage tier. The value must be an integer on the DeviceManager.</p>	<p>High performance Tier _____</p> <p>Performance Tier _____</p> <p>Capacity Tier _____</p>
Creating a LUN	<p><b>LUN name</b></p> <p>If a LUN is created in a batch, four digits are automatically added after the LUN name.</p>	<p>_____</p>
	<p><b>Enable SmartThin or not</b></p> <p>If you enable the SmartThin when creating a LUN, a thin LUN will be created. The storage system first allocates an initial capacity to a thin LUN and then increases the LUN capacity in real time and on demand based on the required storage capacity. You are advised not to enable this function during the initial configuration.</p>	<p>Yes ____</p> <p>No ____</p>
	<p><b>Capacity</b></p> <p>Capacity of the LUN to be created. For a thin LUN, the capacity is the maximum capacity to which the LUN can be expanded.</p>	<p>_____</p>

Operation	Item	Default/Actual Value	
	<b>Quantity</b> Number of LUNs created in a batch.	_____	
	<b>Read policy</b> Cache read policy refers to the residence policy of data in the cache after the application server delivers the read I/O request.	Resident _____	_____
		Default _____	_____
		Recycle _____	_____
	<b>Write policy</b> Cache write policy refers to the residence policy of data in the cache after the application server delivers the write I/O request.	Resident _____	_____
		Default _____	_____
		Recycle _____	_____
		_____	_____
	<b>Prefetch Policy</b> Applications have different size requirements for data reads. The prefetch policies of LUNs can improve the read performance.	Intelligent prefetch _____	_____
		Constant prefetch _____	_____
		Variable prefetch _____	_____
		Non-prefetch _____	_____
Creating a LUN group	<b>LUN group name</b> Name of the LUN group to be created.	_____	
	<b>LUNs in the LUN group</b> LUNs in the LUN group. LUNs in a LUN group can be used by application servers only after the LUN group is added to the mapping view.	LUN group _____ _____	LUN _____ _____
Configuring an initiator (applicable to iSCSI connection)	<b>iSCSI host port</b> IP address of the iSCSI host port connected to the application server.	IP address _____	_____
		Subnet mask/IPv6 prefix _____	_____
		Gateway _____	_____

Operation	Item	Default/Actual Value	
	<p><b>IQNs and IP addresses of the host ports</b></p> <p>The initiator qualified name (IQN) is used by a storage system to identify application servers and can be changed on application servers.</p>	IQNs _____ _____	Host port IP addresses _____ _____
Creating a host	<p><b>Host name</b></p> <p>The host is a concept used in the storage system environment. A host corresponds to an application server.</p>	_____	
	<p><b>WWPN of the Fibre Channel port on the application server (applicable to Fibre Channel connection)</b></p> <p>World Wide Port Name (WWPN) of the Fibre Channel port on the application server.</p>	_____	
Creating a host group	<p><b>Host group name</b></p> <p>Name of the host group to be created.</p>	_____	
	<p><b>Hosts in the host group</b></p> <p>Hosts in the host group.</p>	Host group _____ _____	Host _____ _____
Creating a port group	<p><b>Port group name</b></p> <p>Name of the port group to be created.</p>	_____	
	<p><b>Host ports in the port group</b></p> <p>Host ports in the port group.</p>	Port group _____ _____	Port _____ _____
Creating a mapping view	<p><b>Mapping view name</b></p> <p>Name of the mapping view to be created.</p>	_____	

Operation	Item	Default/Actual Value	
	<b>Mapping</b> Mapping between host groups and LUN groups.	Host group _____ _____	LUN group _____ _____

## 2.5 Planning Disk Domains

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

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

Disks can be divided based on the following two factors:

- Encryption: Disks can be divided into self-encrypting and non-encrypting disks. Self-encrypting and non-encrypting disks cannot exist in the same disk domain. Encrypted disks are not sold in mainland China.
  - Self-encrypting disk: When data is written into or read from a disk, the data is encrypted or decrypted using the hardware circuit and internal encryption key of the disk. The self-encrypting disk is a special type of disk.  
Before using self-encrypting disks to create an encrypted disk domain, install and configure key management servers, and complete their interconnections with the storage system. For details, see *OceanStor V3 Series V300R006 Disk Encryption User Guide*.
  - Non-encrypting disk: Non-encrypting disks are common disks that do not support the encryption function.
- Medium: Disks can be divided into SSDs, SAS disks, and NL-SAS disks.  
A disk type in a disk domain corresponds to a storage tier of a storage pool. If the disk domain does not have a specific disk type, the corresponding storage tier cannot be created for a storage pool.

**Table 2-9** describes the mapping between disk types and storage tiers.

**Table 2-9** Mapping between disk types and storage tiers

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

### Planning Hot Spare Policies for a Disk Domain

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

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

- - High
 

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

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

The system does not provide hot spare space.

**Table 2-10** describes how hot spare space changes with the number of disks. The hot spare space changes at a storage tier are used as an example here. The hot spare space changes at different types of storage tiers are the same.

**Table 2-10** Changes of hot spare space

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

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

 **NOTE**

- For 18000 and 18000F series storage systems, the high hot spare policy is used by default. You can only run the **change disk\_domain general** command on the CLI to modify the hot spare policy.
- When you are creating a disk domain, ensure that the disks used to provide hot spare space are sufficient.
- Hot spare space can be used for the current disk domain only.
- **Table 2-10** lists common capacity changes of the hot spare space. The number of disks supported by a storage system and the capacity of their hot spare space are based on actual specifications.

## Recommended Configurations for Disks in the Disk Domain

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

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

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

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

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

 **NOTE**

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

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

The space of a storage pool originates from a disk domain. Therefore, the capacity of the disk domain determines the available capacity of the storage pool. The capacity of the disk domain must be properly planned to make full utilization of storage space. When planning the minimum capacity for a disk domain, you must set related parameters including the hot spare policy, RAID policy, and storage media to ensure that the disk domain can meet capacity requirements of storage pools and hot spare space. [Table 2-11](#) describes the minimum number of disks required for planning a disk domain (for a single engine).

**Table 2-11** Planning a disk domain (for a single engine)

RAID Policy	Minimum Number of Disks in a Disk Domain
RAID 0	4
RAID 1 (2D)	4 <b>NOTE</b> For the 5000 and 6000 series storage systems, if the number of SSDs in a disk domain is two or three, you are advised to configure the corresponding high-performance tier to RAID 1 (2D).
RAID 1 (4D)	4
RAID 10	4
RAID 3 (2D+1P)	4
RAID 3 (4D+1P)	6
RAID 3 (8D+1P)	10
RAID 5 (2D+1P)	4
RAID 5 (4D+1P)	6
RAID 5 (8D+1P)	10
RAID 6 (2D+2P)	5
RAID 6 (4D+2P)	7
RAID 6 (8D+2P)	11
RAID 6 (16D+2P)	19

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

 **NOTE**

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

Refer to the following suggestions to plan disk domains:

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

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

The space of a storage pool originates from a disk domain. Therefore, the capacity of the disk domain determines the available capacity of the storage pool. The capacity of the disk domain must be properly planned to make full utilization of storage space. When planning the minimum capacity for a disk domain, you must set related parameters including the hot spare policy, RAID policy, and storage media to ensure that the disk domain can meet capacity requirements of storage pools and hot spare space. [Table 2-12](#) describes the minimum number of disks required for planning a disk domain (for a single engine).



**Table 2-12** Planning a disk domain (for a single engine)

RAID Policy	Minimum Number of Disks in a Disk Domain (SSD)	Minimum Number of Disks in a Disk Domain (SAS) <sup>a</sup>	Minimum Number of Disks in a Disk Domain (NL-SAS) <sup>a</sup>
RAID 0	6	8	8
RAID 1 (2D)	6	8	8
RAID 1 (4D)	6	8	8
RAID 10	6	8	8
RAID 3 (2D+1P)	6	8	8
RAID 3 (4D+1P)	6	8	8
RAID 3 (8D+1P)	10	10	10
RAID 5 (2D+1P)	6	8	8
RAID 5 (4D+1P)	6	8	8
RAID 5 (8D+1P)	10	10	10
RAID 6 (2D+2P)	6	8	8
RAID 6 (4D+2P)	7	8	8
RAID 6 (8D+2P)	11	11	11
RAID 6 (16D+2P)	19	19	19
RAID 50 (2D+1P)x2	7	8	8
RAID 50 (4D+1P)x2	11	11	11
RAID 50 (8D+1P)x2	19	19	19
a: only applies to the 18000 series storage systems.			

 **NOTE**

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

Refer to the following suggestions to plan disk domains:

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

## 2.6 Planning Storage Pools

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

### Usage

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

### Storage Tiers (2000, 5000, 6000, 18000 Series Storage Systems)

A storage pool is a logical combination of one or more storage tiers. The storage pool of the storage system supports a maximum of three storage tiers. A storage tier is a set of storage

media that has the same performance and uses the same RAID level. Each storage tier provides different performance at different costs. You can configure storage tiers based on your requirements.

**Table 2-13** lists the specifications of each storage tier.

**Table 2-13** Specifications of each storage tier

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

Functions of different storage tiers are as follows:

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

## RAID Levels

Consider the following when selecting RAID levels:

- Reliability
- Read/Write performance
- Disk utilization

Different RAID levels provide different reliability, read/write performance, and disk utilization, as described in **Table 2-14**.

**Table 2-14** RAID levels

RAID Level	Redundancy and Data Recovery Capability	Read Performance	Write Performance	Disk Utilization	Maximum Number of Allowed Faulty Disks
RAID 0	No data redundancy is provided and damaged data can not be recovered.	High	High	The disk utilization is 100%.	0
RAID 1	High. RAID 1 provides completely redundancy. When a CK fails, the mirror CK can be used for data recovery.	Relatively high	Relatively low	<ul style="list-style-type: none"> <li>● 2D<sup>a</sup>: The disk utilization is about 50%.</li> <li>● 4D: The disk utilization is about 25%.</li> </ul>	A maximum of N-1 disks can fail at the same time (in a RAID 1 disk array with N disks).

RAID Level	Redundancy and Data Recovery Capability	Read Performance	Write Performance	Disk Utilization	Maximum Number of Allowed Faulty Disks
RAID 3	Relatively high. Each CKG has one CK as the parity CK. Data on any data CK can be recovered using the parity CK. If two or more CKs fail, the RAID level fails.	High	Low	RAID 3 supports flexible configurations. Specifically, a RAID 3 policy allows data block and parity block policies ranging from 2D+1P to 13D+1P. The following examples show disk utilization rates of several configurations commonly used by RAID 3: <ul style="list-style-type: none"> <li>● 4D + 1P<sup>b</sup>: The disk utilization is about 80%.</li> <li>● 2D + 1P: The disk utilization is about 66.67%.</li> <li>● 8D + 1P: The disk utilization is about 88.89%.</li> </ul> <b>NOTE</b> For a flexibly configured RAID policy $x\text{D}+y\text{P}$ , the disk utilization is $[\frac{x}{x+y}] \times 100\%$ .	1

RAID Level	Redundancy and Data Recovery Capability	Read Performance	Write Performance	Disk Utilization	Maximum Number of Allowed Faulty Disks
RAID 5	Relatively high. The parity data is distributed on different CKs. In each CKG, the parity data occupies space of a CK. RAID 5 allows the failure of only one CK. If two or more CKs fail, the RAID level fails.	Relatively high	Relatively high	RAID 5 supports flexible configurations. Specifically, a RAID 5 policy allows data block and parity block policies ranging from 2D+1P to 13D+1P. The following examples show disk utilization rates of several configurations commonly used by RAID 5: <ul style="list-style-type: none"> <li>● 2D + 1P: The disk utilization is about 66.67%.</li> <li>● 4D + 1P: The disk utilization is about 80%.</li> <li>● 8D + 1P: The disk utilization is about 88.89%.</li> </ul> <b>NOTE</b> For a flexibly configured RAID policy $x\text{D}+y\text{P}$ , the disk utilization is $[\frac{x}{x+y}] \times 100\%$ .	1

RAID Level	Redundancy and Data Recovery Capability	Read Performance	Write Performance	Disk Utilization	Maximum Number of Allowed Faulty Disks
RAID 6	Relatively high. Two groups of parity data are distributed on different CKs. In each CKG, the parity data occupies space of two CKs. RAID 6 allows two CKs to fail simultaneously. If three or more CKs fail, the RAID level fails.	Medium	Medium	RAID 6 supports flexible configurations. Specifically, a RAID 6 policy allows data block and parity block policies ranging from 2D+2P to 26D+2P. The following examples show disk utilization rates of several configurations commonly used by RAID 6: <ul style="list-style-type: none"> <li>● 2D + 2P: The disk utilization is about 50%.</li> <li>● 4D + 2P: The disk utilization is about 66.67%.</li> <li>● 8D + 2P: The disk utilization is about 80%.</li> <li>● 16D + 2P: The disk utilization is about 88.89%.</li> </ul> NOTE For a flexibly configured RAID policy $x\text{D}+y\text{P}$ , the disk utilization is $[x/(x + y)] \times 100\%$ .	2

RAID Level	Redundancy and Data Recovery Capability	Read Performance	Write Performance	Disk Utilization	Maximum Number of Allowed Faulty Disks
RAID 10	High. RAID 10 allows multiple CKs to fail simultaneously. When a CK fails, the mirror CK can be used for data recovery. If a CK and its mirror CK fail simultaneously, the RAID level fails.	Relatively high	Relatively high	The disk utilization is 50%.	A maximum of N disks can fail at the same time (in a RAID 10 disk array with 2N disks).
RAID 50	Relatively high. The parity data is distributed on different CKs of each RAID 5 sub-group. In each RAID 5 sub-group, only one CK is allowed to fail. If two or more CKs of a RAID 5 sub-group fail simultaneously, the RAID level fails.	Relatively high	Relatively high	<ul style="list-style-type: none"> <li>● (2D + 1P) x 2: The disk utilization is about 66.67%.</li> <li>● (4D + 1P) x 2: The disk utilization is about 80%.</li> <li>● (8D + 1P) x 2: The disk utilization is about 88.89%.</li> </ul>	1
<p>a: <b>D</b> indicates the data block. b: <b>P</b> indicates the parity block.</p>					

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

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



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

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

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

## 2.7 Planning LUNs

Select appropriate LUN types, read/write policies, and prefetch policies for LUNs based on the data storage requirements to achieve the optimal performance of the storage system.

### Planning the LUN type

Storage systems support two types of LUNs: common LUNs (including thin LUNs and thick LUNs) and Protocol Endpoint (PE) LUNs.

- Common LUN:
  - Thin LUN: A thin LUN is configured with an initial capacity when created and dynamically allocated required storage resources when its available capacity is insufficient.
  - Thick LUN: When a thick LUN is created, the system uses the auto provisioning technology to allocate the fixed capacity of storage resources to the thick LUN.

#### NOTE

When a host initially reads data from and writes data to a storage system, thick LUNs deliver better performance and thin LUNs boasts higher space utilization.

- PE LUN: PE LUNs are applied only for VMware Virtual Volume (VVOL) LUNs in VMware ESXi 6.0 software defined storage.

### Planning a Cache Policy (Applicable to Common LUNs)

Cache policies are divided into read policies and write policies. Improper setting of read and write policies will deteriorate the read and write performance and reduce the reliability of a storage system. A storage system supports two cache policies: read policy and write policy.

[Table 2-15](#) describes the two cache policies and optional policies.

**Table 2-15** Description and optional policies of the cache policy

Policy	Description	Optional Policy
Read policy	Cache read policy refers to the residence policy of data in the cache after the application server delivers the read I/O request.	The following cache policies are available on the storage system: <ul style="list-style-type: none"> <li>● <b>Resident:</b> Applies to randomly accessed services, ensuring that data can be cached as long as possible to improve the read hit ratio.</li> <li>● <b>Default:</b> Applies to regular services, striking a balance between the hit ratio and disk access performance.</li> <li>● <b>Recycle:</b> Applies to sequentially accessed services, releasing cache resources for other services as soon as possible.</li> </ul>
Write policy	Cache write policy refers to the residence policy of data in the cache after the application server delivers the write I/O request.	

## Planning Prefetch Policies (Applicable to Common LUNs)

Applications have different size requirements for data reads. The prefetch policies of LUNs can improve the read performance.

Storage system supports four prefetch policies: intelligent prefetch, constant prefetch, variable prefetch, and non-prefetch. [Table 2-16](#) describes the principles and application scenarios of the four prefetch policies.

**Table 2-16** Principles and application scenarios of prefetch policies

Prefetch Policy	Principle	Application Scenario
Intelligent prefetch	Intelligent prefetch analyzes whether the requested data is sequential. If it is, the data following the currently requested data is prefetched from disks to the cache to improve the cache hit ratio. The length of intelligent prefetch ranges from the start address of the currently requested data to the end address of the CK.	Suitable for single-stream read applications or for the read applications that cannot be determined sequential or random, for example, file read/write.

Prefetch Policy	Principle	Application Scenario
Constant prefetch	After receiving a data read request, the storage system prefetches the data to the cache based on the preset prefetch length, regardless of the read length specified in the I/O request.	Suitable for the sequential read applications that have a fixed size, for example, requests initiated by multiple users for playing streaming media on demand at the same bit rate.
Variable prefetch	After receiving a data read request, the storage system prefetches the data to the cache based on a multiple of the read length specified in the I/O request.	Suitable for the sequential read applications that have an unfixed size or for the multi-user concurrent read applications whose prefetch data amount cannot be determined, for example, requests initiated by multiple users for playing multimedia on demand at different bit rates.
Non-prefetch	The host reads data directly from disks based on the read length specified in the I/O request without a prefetch process.	Suitable for small-block random read applications, for example, databases.

 **NOTE**

Cache prefetch may deteriorate the system performance when random read services are running on the storage system. You are advised to use the non-prefetch policy.

## Planning Value-Added Features (Applicable to Common LUNs)

After a LUN is mapped to a host, the LUN supports the following features or functions:

- HyperMetro (Works as a local or remote LUN)
- Snapshot (Works as a source LUN)
- Clone (Works as a primary LUN)
- LUN Copy (Works as a source LUN)
- Remote Replication (Works as a primary LUN)
- SmartMigration (Works as a source LUN)
- HyperMirror (Works as a Mirror LUN)
- SmartDedupe&SmartCompression
- SmartQoS
- SmartPartition
- SmartTier
- SmartCache
- SmartMulti-Tenant



OceanStor 2200 V3 storage system does not support SmartDedupe&SmartCompression.

## Planning Value-Added Features (Applicable to VVol LUNs)

After configuring VVol LUNs, you can configure the following value-added features:

- Source LUN in the snapshot feature
- Snapshot LUN
- Source LUN in a LUN copy
- Target LUN in a LUN copy
- SmartThin
- SmartQoS

## 2.8 (Optional) Planning iSCSI CHAP

To ensure the storage system access security, plan iSCSI CHAP to control the access to the storage system.

The CHAP is a method of verifying the identity of the peer using a 3-way handshake. This verification is based on a ciphertext or cipher key.

1. During the establishment of a link, the authenticator sends a challenge message to the peer.
2. The peer encrypts the random packet using the password and algorithm and responds with the ciphertext.
3. The authenticator checks the response by encrypting the random packet using the peer's password and algorithm that have been saved. If the two ciphertexts match, the authentication is acknowledged. If the two ciphertexts do not match, the authentication is not acknowledged.

After CHAP authentication is enabled on the storage system, you must enter the CHAP user name and password when accessing the storage system from an application server.

When planning CHAP, note the following:

- User name for CHAP authentication
  - The name contains 4 to 223 characters.
  - The name only contains letters, digits or special characters. Special characters are:  
!"#\$%&'()\*+,-./:;<=>?@[\\]^\_`{|}~
  - The first character must be letter or digit.
- Password for CHAP authentication
  - The password contains 12 to 16 characters.
  - The password must contain three of the following four types of characters:
    - Uppercase letters
    - Lowercase letters
    - Digits
    - Special characters (including space)  
!"#\$%&'()\*+,-./:;<=>?@[\\]^\_`{|}~

- The password cannot be the same as the account or mirror writing of the account.
- Mapping between CHAP user accounts and initiators  
Create CHAP user accounts and assign them to corresponding initiators.

## 2.9 Planning Management User Accounts

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

The storage system defines the following three user roles:

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

[Table 2-17](#) and [Table 2-18](#) show the roles preset by the storage system and their permissions.

**Table 2-17** System roles

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

Preset Role	Function Group	Permissions
Backup administrator	System group	Permission of managing data backup, remote data protection, including local data and mapping views

**Table 2-18** Tenant roles

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

Besides preset roles, the storage system also supports self-defined roles. For details about the permissions of self-defined roles, see [B Permission Matrix for Self-defined Roles](#).

# 3 Configuring Basic Storage Services

---

## About This Chapter

Configure the basic storage services to divide the storage space into LUNs and map the LUNs to application servers so that the application servers can read and write the storage space provided by the storage system.

### [3.1 Configuration Process](#)

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

### [3.2 Checking Before Configuration](#)

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

### [3.3 Logging In to the DeviceManager](#)

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

### [3.4 Creating a Disk Domain](#)

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

### [3.5 Creating a Storage Pool](#)

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

### [3.6 Creating a LUN](#)

The storage space of a newly created storage pool cannot be identified by the host. The host can use the storage space only after the storage space of the storage pool is divided into LUNs and the LUNs are mapped to the host.

### [3.7 Creating a LUN Group](#)

To allow hosts to use LUNs, you must add LUNs into LUN groups. Then, establish mapping views between the LUN groups and host groups. By doing so, the hosts in the host groups can use the LUNs in the LUN groups. A LUN group can contain 1 to 4096 LUNs. A LUN can be added to a maximum of 8 LUN groups.

### 3.8 Configuring Connectivity between Host and Storage System

This section describes how to configure the connectivity between a host and a storage system to enable the host to use storage resources.

#### 3.9 Creating a Host

Create a host to establish a connection between a storage system and an application server, and add an initiator for the host to establish a mapping relationship between the host and application server.

#### 3.10 Creating a Host Group

To allow hosts to use LUNs, you must add hosts into host groups. Then, establish mapping views between the LUN groups and host groups. By doing so, the hosts in the host groups can use the LUNs in the LUN groups. A host group can contain one or multiple hosts.

#### 3.11 (Optional) Creating a Port Group

A port group is a logical combination of multiple physical ports. The storage system specifies ports to set up mappings between storage resources (LUNs) and servers. This operation enables you to create a port group and add it to a mapping view. After that, LUNs of a specified LUN group use the ports of the port group to communicate with the corresponding hosts of the host group. If no port group is added to the mapping view, available ports are randomly used. A port group can be added to a maximum of 64 mapping views. A port can be added to a maximum of 64 port groups.

#### 3.12 Creating a Mapping View

This operation enables you to create a mapping view and manage the mapping relationship between multiple host groups and LUN groups by adding them to the mapping view.

#### 3.13 Configuring LUN Mapping Using a Cipher Machine

Use a cipher machine to configure mapping relationships between application servers and LUNs to keep critical services running in an encrypted environment. If no cipher machine is available, skip this section.

#### 3.14 Making Storage Space Available

After a connection is established between a storage system and an application server, the application server must discover the newly-added logical disk (that is, the storage space specified by a mapped LUN) to use it as a common disk for data reads and writes.

#### 3.15 Performing an Emergency Rollback

If a newly created storage resource does not meet service requirements, you must roll it back.

## 3.1 Configuration Process

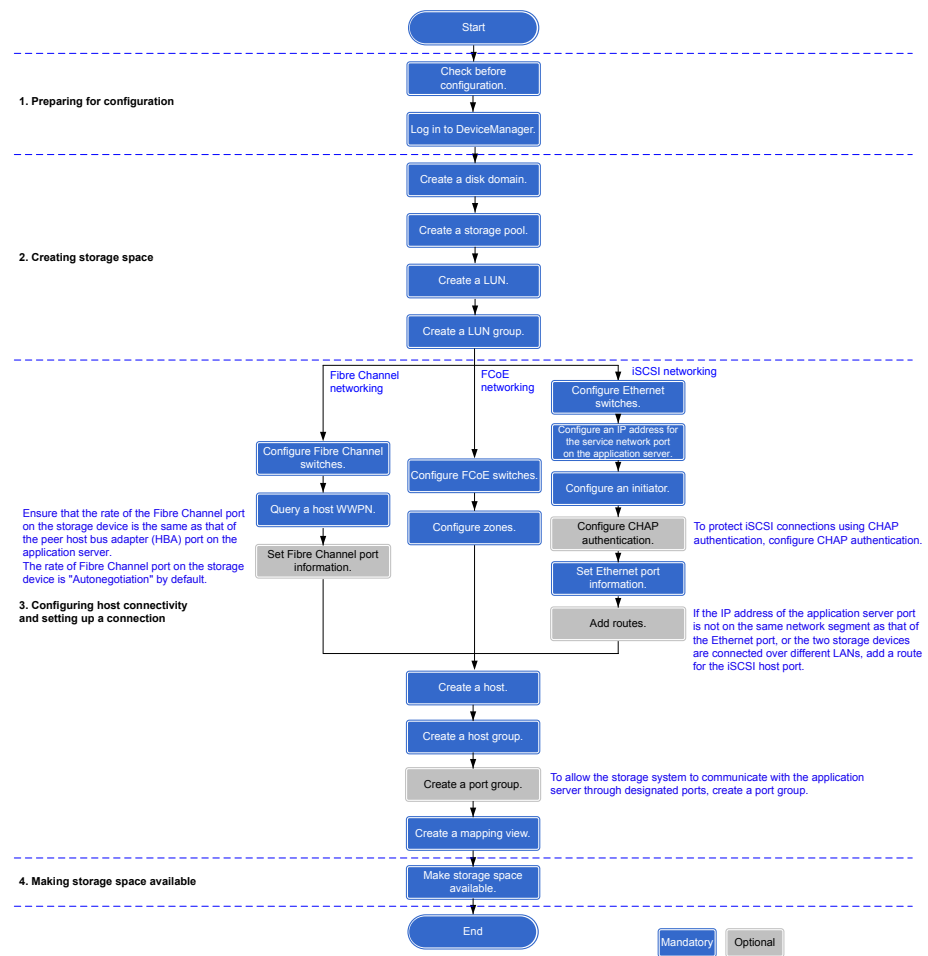
The configuration process includes the overall procedures for configuring the storage space. You can learn about the storage space configuration logic.

If critical data must be encrypted, you are advised to deploy a cipher machine. The process for configuring storage space differs between a storage system configured with a cipher machine and that without a cipher machine without one. The processes are described as follows:

- When a storage system is not configured with a cipher machine, the flowchart for configuring storage space is shown in **Figure 3-1**.

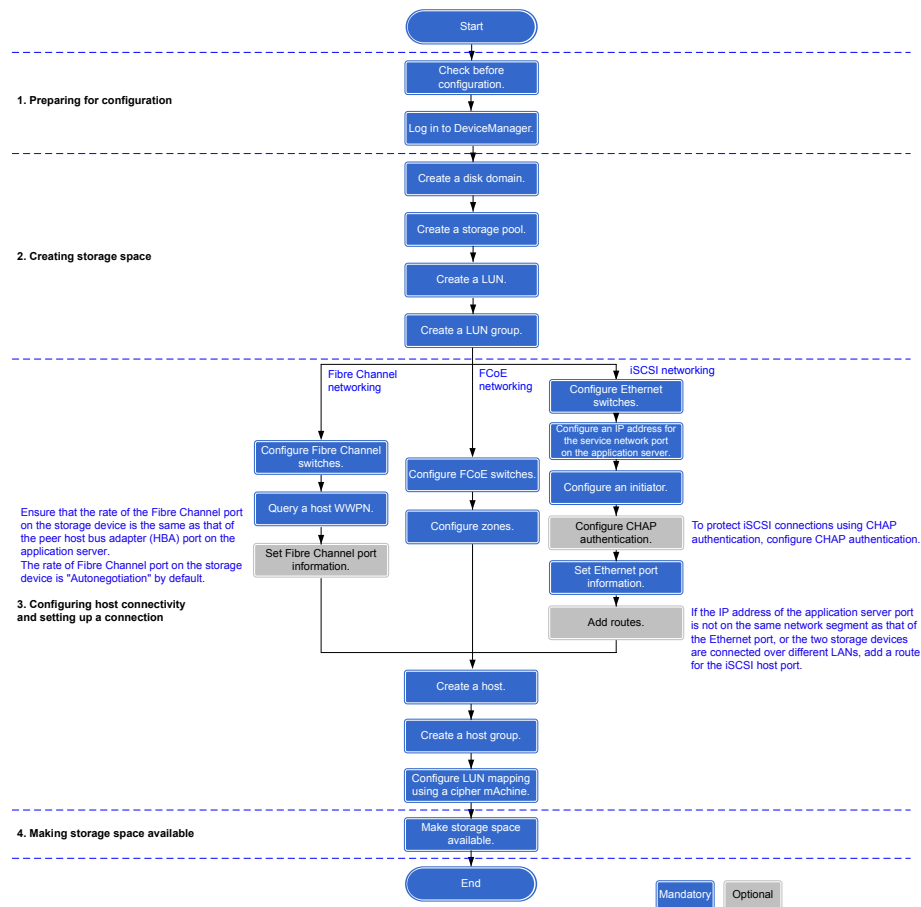


**Figure 3-1** Configuring storage space (without a cipher machine)



- When a storage system is configured with a cipher machine, the flowchart for configuring storage space is shown in **Figure 3-2**.

**Figure 3-2** Configuring storage space (with a cipher machine)



**NOTE**

Certain versions of storage systems do not support iSCSI connection of cipher machines. In these cases, use Fibre Channel connection. For details, contact Huawei technical support engineers.

Table 3-1 describes the procedures for configuring storage space in the previous two scenarios.

**Table 3-1** Procedures for configuring storage space

Procedure	Operation	Description	Reference
1. Preparing for configuration	Checking before configuration	Check whether the software installation and initial configuration meet the requirements for storage space configuration.	<a href="#">3.2 Checking Before Configuration</a>
	Logging in to the DeviceManager	The is a device management platform program developed by Huawei. You can log in to the DeviceManager to manage and maintain the storage system.	<a href="#">3.3 Logging In to the DeviceManager</a>

Procedure	Operation	Description	Reference
2. Creating storage space	Creating a disk domain	A disk domain provides storage space for storage pools, whose storage tiers and available capacities depend on the disk types, capacity, and hot spare policy of the disk domain. The storage system automatically allocates hot spare space with different capacities based on hot spare policies to take over data from failed member disks.	<a href="#">3.4 Creating a Disk Domain</a>
	Creating a storage pool	The storage space used by application servers is provided by the storage pools on the storage system.	<a href="#">3.5 Creating a Storage Pool</a>
	Creating a LUN	A LUN indicates a logical unit in storage space.	<a href="#">3.6 Creating a LUN</a>
	Creating a LUN group	A LUN group is a set of LUNs. Only LUN groups can be added to a mapping view.	<a href="#">3.7 Creating a LUN Group</a>
3. Configuring host connectivity and setting up a connection	Configuring connectivity between host and storage system	The connectivity between a host and a storage system is configured to enable the host to use storage resources. <ul style="list-style-type: none"> <li>● iSCSI networking</li> <li>● Fibre Channel networking</li> <li>● FCoE networking</li> </ul>	<a href="#">3.8 Configuring Connectivity between Host and Storage System</a>
	Creating a host	A host is a virtual concept of an application server. An initiator is added for a host to establish a connection with the application server.	<a href="#">3.9 Creating a Host</a>
	Creating a host group	A host group is a set of hosts. Only host groups can be added to a mapping view.	<a href="#">3.10 Creating a Host Group</a>
	(Optional) Creating a port group	Multiple ports can be logically added to a port group to facilitate port management.	<a href="#">3.11 (Optional) Creating a Port Group</a>
	Creating a mapping view	The application server corresponding to a host in a host group can use the storage space designated by a LUN in a LUN group only after the host group and LUN group are added to the same mapping view.	<a href="#">3.12 Creating a Mapping View</a>

Procedure	Operation	Description	Reference
	Configuring LUN mapping using a cipher machine	Use a cipher machine to configure mapping relationships between application servers and LUNs to keep critical services running in an encrypted environment.  <b>NOTE</b> If no cipher machine is available, skip this procedure.	<a href="#">3.13 Configuring LUN Mapping Using a Cipher Machine</a>
4. Making storage space available	Making storage space available	Application servers must scan for disks to detect the LUNs mapped by the storage system and use the storage space.	<a href="#">3.14 Making Storage Space Available</a>

## Configuring Storage Resources Using SmartConfig (2000 and 2000F Series Storage Systems)

If a service host and a storage system meet the following conditions, you can install SmartConfig on the host to divide disk resources into LUNs and mount the LUNs to the host in a more efficient and easy manner:

- The service host can access the management IP address of the storage system.
- The service host connects to the service port of the storage system through iSCSI or Fibre Channel links (directly or over switches).
- Users do not have service planning requirements on disk domains and storage pools. For example, a service requires that a LUN be created on a certain storage pool.
- [Table 3-2](#) shows supported product models and host operating systems.

**Table 3-2** Supported products

Storage Device Model	Host Operating System
OceanStor 2200 V3&2600 V3	<ul style="list-style-type: none"> <li>● Windows                             <ul style="list-style-type: none"> <li>- Windows Server 2008 R2 Enterprise Edition SP1 (32-bit or 64-bit)</li> <li>- Windows Server 2012(32-bit or 64-bit)</li> </ul> </li> <li>● Linux                             <ul style="list-style-type: none"> <li>- RedHat Enterprise Linux 5 to 7</li> <li>- SUSE Enterprise Linux 10 to 11</li> </ul> </li> </ul>

For details, see *SmartConfig User Guide* of corresponding versions. To obtain the documents, log in to Huawei support website at <http://enterprise.huawei.com/>. In the search box, enter the product model or document name and search for the desired document.

## 3.2 Checking Before Configuration

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

### Checking Software Installation

Check whether required software is properly installed on the storage system and application server. [Table 3-3](#) lists the check items and provides the check methods.

**Table 3-3** Software installation checklist

Check Item	Operating System	Check Method	How to Obtain
iSCSI initiator (required only for iSCSI connection)	Windows	On the Windows task bar, check whether <b>Microsoft iSCSI Initiator</b> exists in the <b>All programs</b> list.	<ul style="list-style-type: none"> <li>● For Windows Server 2003 and earlier versions, you can download iSCSI initiator from Microsoft website.</li> <li>● For Windows Server 2008 and later versions, iSCSI initiator is delivered with the system.</li> </ul>
	SUSE	On the SUSE-based application server, run the <b>rpm -qa   grep open-iscsi</b> command. If the iSCSI initiator information is displayed, the iSCSI initiator is installed on the application server.	Operating system installation CD-ROM
	Red Hat	On the Red Hat-based application server, run the <b>rpm -qa   grep iscsi</b> command. If the iSCSI initiator information is displayed, the iSCSI initiator is installed on the application server.	Operating system installation CD-ROM

Check Item	Operating System	Check Method	How to Obtain
	Solaris	On the Solaris-based application server, run the <b>pkginfo   grep iscsi</b> command. If the iSCSI initiator information is displayed, the iSCSI initiator is installed on the application server.	Operating system installation CD-ROM
	AIX	On the AIX-based application server, run the <b>lspp -l   grep -i iscsi</b> command. If the iSCSI initiator information is displayed, the iSCSI initiator is installed on the application server.	Operating system installation CD-ROM
	HP-UX	On the HP-UX-based application server, run the <b>swlist iSCSI-00</b> command. If the iSCSI initiator information is displayed, the iSCSI initiator is installed on the application server.	You can download iSCSI initiator from HPE website.
	VMware	For VMware ESXi 4.1 and earlier versions, an iSCSI adapter already exists in a storage adapter. You can directly enable the iSCSI adapter. For VMware ESXi 5.0 and later versions, you must add an iSCSI adapter on the <b>Storage Adapters</b> page and then perform the follow-up configuration.	You can visit the VMware website to view how to install the iSCSI adapter.
UltraPath (optional and required only when redundant paths exist between the storage system and application server)	Windows	On the Windows task bar, choose <b>Start &gt; Control Panel</b> . Click <b>Add or Remove Programs</b> . Check whether UltraPath exists in the <b>Currently installed programs</b> list.	Go to <a href="http://support.huawei.com/enterprise/">http://support.huawei.com/enterprise/</a> and register for an account with the website. Log in with the applied user name and password. In the search field, enter <b>UltraPath</b> , and select a path from the paths that are

Check Item	Operating System	Check Method	How to Obtain
<b>NOTE</b> Install UltraPath V100R008C50SP C500 or later.	SUSE	On the SUSE-based application server, run the <b>rpm -ql UltraPath</b> command. If the UltraPath information is displayed, UltraPath is installed.	automatically displayed to go to the document page. Then click the <b>Downloads</b> tab, and search for and download your desired software files.
	Red Hat	On the Red Hat-based application server, run the <b>rpm -ql UltraPath</b> command. If the UltraPath information is displayed, UltraPath is installed.	
	Solaris	On the Solaris-based application server, run the <b>pkginfo   grep UltraPath</b> command. If the UltraPath information is displayed, UltraPath is installed.	
	AIX	On the AIX-based application server, run the <b>lspp -l   grep -i UltraPath</b> command. If the UltraPath information is displayed, UltraPath is installed.	
	VMware	On the vCenter management page, select a host and check whether the <b>UltraPath</b> tab is displayed in the right pane. If the tab page is displayed, UltraPath is installed on the host.	

 **NOTICE**

For Linux systems whose kernel is 3.8 or later (Oracle Linux 6.5 or later, Red Hat 7.0, CentOS 7.0 or later, SUSE 12 or later), if you want to create and use a LUN with a capacity over 2 TB and select OceanStor UltraPath as multipathing software, use UltraPath V100R008C50SPC500 or later.

## Checking Initial Configuration

- Network connection status

[Table 3-4](#) lists the check items and provides the check methods.

**Table 3-4** Network connection status checklist

Category	Check Item	Check Method
Connection between the maintenance terminal and storage system	Check whether the management network port on the storage system communicates with the maintenance terminal properly.	<p>In the command-line interface (CLI) mode on the maintenance terminal, run the following command:</p> <ul style="list-style-type: none"> <li>● For IPv4, <b>ping ip</b> (where <i>ip</i> indicates the IP address of the management network port).</li> <li>● For IPv6, <b>ping -6 ip</b> (where <i>ip</i> indicates the IP address of the management network port).</li> </ul> <p>If the maintenance terminal receives data packets from the management network port, the communication between the storage system and maintenance terminal is normal. If the maintenance terminal receives no data packets from the management network port, change the IP address of the management network port and try again.</p>
Connection between the storage system and application server (using the Windows-based application server as an example)	When an iSCSI host port on the storage system is used for connection, check whether the iSCSI host port communicates with the service network port on the application server properly.	<p>On the CLI of the application server, run the following command:</p> <ul style="list-style-type: none"> <li>● For IPv4, <b>ping ip</b> (where <i>ip</i> indicates the IP address of the iSCSI host port).</li> <li>● For IPv6, <b>ping -6 ip</b> (where <i>ip</i> indicates the IP address of the iSCSI host port).</li> </ul> <p>If the application server receives data packets from the iSCSI host port, the communication between the storage system and application server is normal. If the application server receives no data packets from the iSCSI host port, replace the network cable, change the IP address of the iSCSI host port, or add a route between the iSCSI host port and service network port, and try again. For details about how to change the IP address of an iSCSI host port or add a route between an iSCSI host port and a service network port, see the DeviceManager online help.</p>



Category	Check Item	Check Method
	When a Fibre Channel host port on the storage system is used for connection, check whether the rate of the Fibre Channel host port is the same as that of the Fibre Channel host bus adapter (HBA) on the application server.	If the rates are different, change the rate of the Fibre Channel host port. For details about how to change the rate of a Fibre Channel host port, see the DeviceManager online help.
	When a Fibre Channel host port on the storage system is used for connection, check whether the mode of the Fibre Channel host port is the same as that of the Fibre Channel HBA on the application server.	If the modes are different, change the mode of the Fibre Channel host port. For details about how to change the mode of a Fibre Channel host port, see the DeviceManager online help.

- Licenses

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

### 3.3 Logging In to the DeviceManager

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

#### 3.3.1 Logging In to the DeviceManager Through Web

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

#### Prerequisites

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

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

## Context

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

## Procedure

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

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

### NOTE

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

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

1. Click **Advanced**.
2. From the **Authentication Mode** list, select an authentication mode.
  - Local user: You will log in to the storage system in local authentication mode. The super administrator can log in to the storage system using the local user authentication mode only.
  - LDAP user: You will log in to the storage system in LDAP domain authentication mode. You can log in to the storage system in LDAP domain authentication mode only after the LDAP server is properly configured.
3. Choose a language from the **Language** list.

 **NOTE**

DeviceManager supports two languages: simplified Chinese and English.

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

 **NOTE**

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

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

The DeviceManager home page is displayed.

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

Figure 3-3 Home page of the DeviceManager

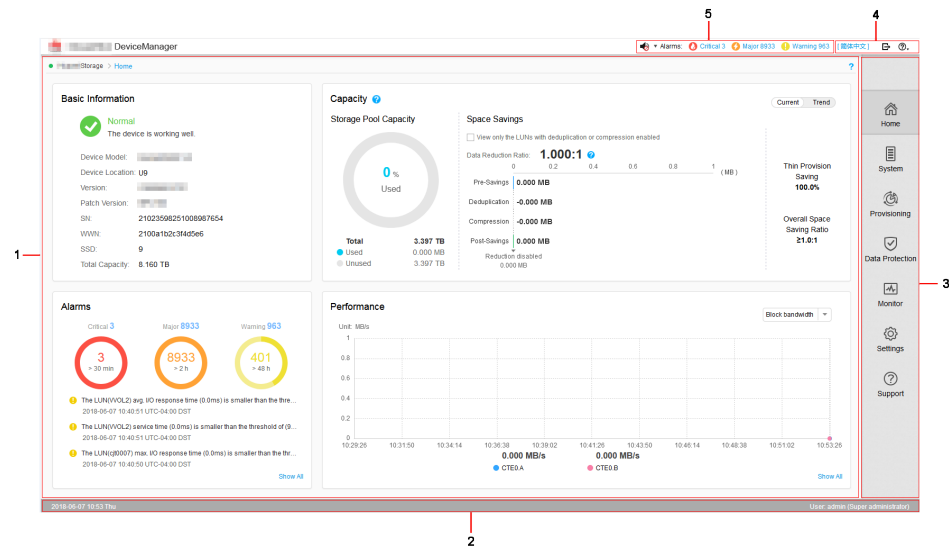


Table 3-5 describes DeviceManager components.


Table 3-5 DeviceManager components

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

----End

## Follow-up Procedure

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

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

- The **Confirm** dialog box is displayed.
2. Click **OK**. You have logged out of the DeviceManager.

### 3.3.2 Logging In to the DeviceManager Using a Tablet

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

#### Prerequisites

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

#### Context

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

#### Procedure

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

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

4. Click **Join**.

The iPad is connected to the Wi-Fi network.

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

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

The login page of the management software is displayed.

For 2000, 5000 and 6000 series storage systems, **xxx.xxx.xxx.xxx** indicates the IP address of the management network port on the storage system. For 18000 series storage systems, **xxx.xxx.xxx.xxx** indicates the IP address of the SVP management network port.

3. **Optional:** In **Language**, select a language.

 **NOTE**

DeviceManager supports two languages: simplified Chinese and English.

4. Set **User Name** and **Password** to the user name and password for logging in to the management software. Set **Verification Code** to a four-digit verification code.

 **NOTE**

- The default user name and password are **admin** and **Admin@storage** respectively.
- You are advised to change the default login password immediately after you have logged in to the storage system for the first time. In addition, periodically change your login password to reduce password leakage risks. For details about how to change a password, see the *Administrator Guide* of the corresponding product model.

5. Click **Login**.

The home page of the management software is displayed.

---End

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

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

#### Prerequisites

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

#### Context

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

## Procedure

### Step 1 Log in to the SVP server.

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

#### NOTE

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

- a. Choose **Start > All Programs > Accessories > Remote Desktop Connection**. The **Remote Desktop Connection** dialog box is displayed.
- b. Type the IP address of the management network port in the **Computer** text box and press **Enter** (the default IP address is **192.168.0.136**).
- c. Type the correct user name and password to log in.

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

#### NOTE

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

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

#### NOTE

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

The DeviceManager login page is displayed.

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

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

#### NOTE

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

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



DeviceManager supports two languages: simplified Chinese and English.

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



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

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

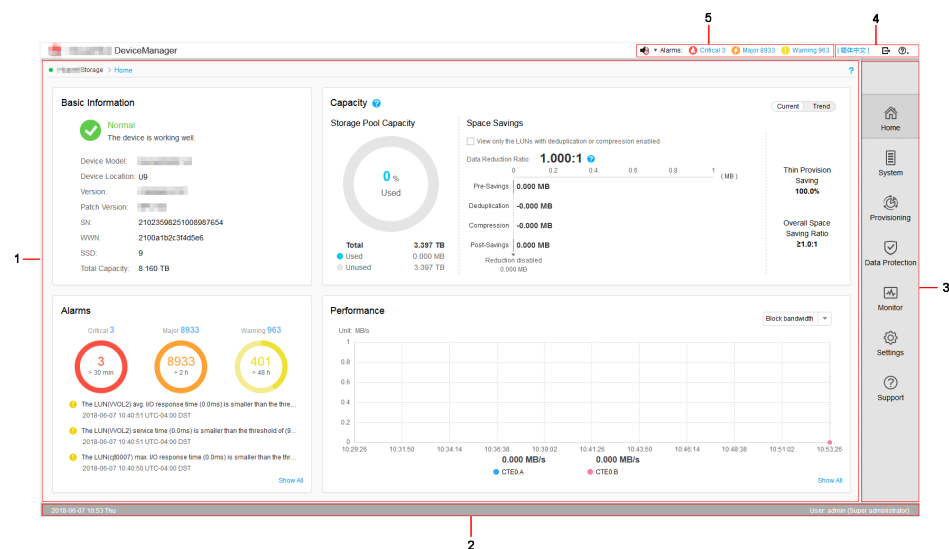


- To log out of the DeviceManager, click in the upper right corner.
- To view online help, click in the upper right corner. The online help provides details about each step and operation.

The DeviceManager main window is displayed.

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

**Figure 3-4** Main window of the DeviceManager





**Table 3-6** describes DeviceManager components.

**Table 3-6** DeviceManager components

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

---End

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

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

#### Prerequisites

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

#### Context

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

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

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

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

## Procedure

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

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

The DeviceManager login page is displayed.

### NOTE

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

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

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

### NOTE

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

- **LDAP user:** Logs in to the storage system using LDAP domain authentication.
3. Choose a language from the **Language** list.

### NOTE

DeviceManager supports two languages: simplified Chinese and English.



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

**NOTE**

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

**Step 5 Click Log In.**

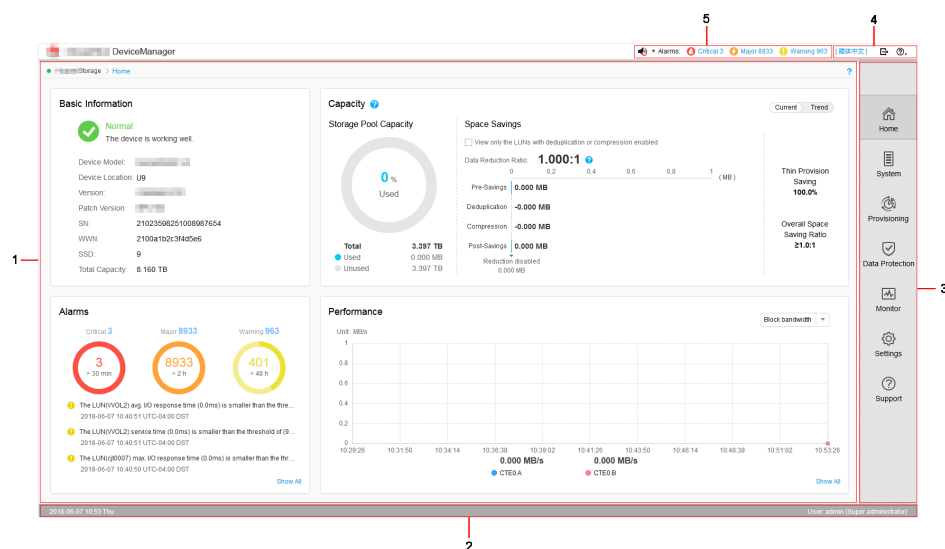
**NOTE**

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

The DeviceManager main window is displayed.

**Figure 3-5** shows the main window of the DeviceManager.

**Figure 3-5** Main window of the DeviceManager



**Table 3-7** describes DeviceManager components.

**Table 3-7** DeviceManager components

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

---End

## 3.4 Creating a Disk Domain

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

### Context

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

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

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

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

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

- - High  
The capacity of one disk is used as hot spare space if the number of disks at a storage tier equals to or fewer than 12. The hot spare space non-linearly increases as the number of disks increases. When the number of disks at a storage tier reaches 175, the storage tier uses the capacity of one disk in every 100 disks as the hot spare space.
- Low  
The capacity of one disk is used as hot spare space if the number of disks at a storage tier equals to or fewer than 25. The hot spare space non-linearly increases as the number of disks increases. When the number of disks at a storage tier reaches 175, the storage tier uses the capacity of one disk in every 200 disks as the hot spare space.
- None (not supported by 18000, 18000F series storage systems)  
The system does not provide hot spare space.

**Table 3-8** describes how hot spare space changes with the number of disks. The hot spare space changes at a storage tier are used as an example here. The hot spare space changes at different types of storage tiers are the same.

**Table 3-8** Changes of hot spare space

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

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

 **NOTE**

- For 18000 and 18000F series storage systems, the high hot spare policy is used by default. You can only run the **change disk\_domain general** command on the CLI to modify the hot spare policy.
- When you are creating a disk domain, ensure that the disks used to provide hot spare space are sufficient.
- Hot spare space can be used for the current disk domain only.
- [Table 3-8](#) lists common capacity changes of the hot spare space. The number of disks supported by a storage system and the capacity of their hot spare space are based on actual specifications.

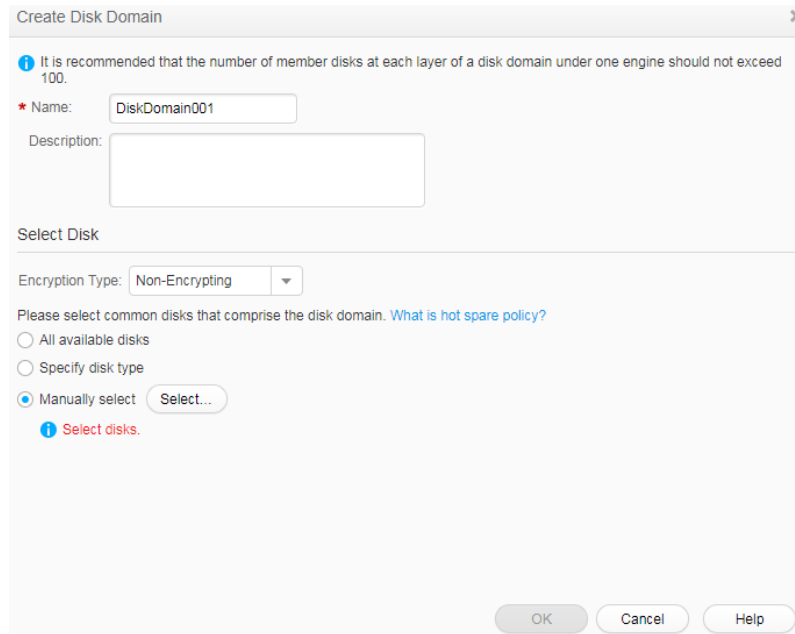
## Procedure

**Step 1** Log in to DeviceManager.

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

**Step 3** Click **Create**.

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



**Step 4** Name and describe the disk domain.

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

**NOTE**

- The name must be unique.
- The name can contain only letters, digits, periods (.), underscores (\_), and hyphens (-).
- The value contains 1 to 31 characters.

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

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

Encryption types include:

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

**NOTE**

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

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

- Select **All available disks**.

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

 **NOTE**

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


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

 **NOTE**

For 18000 series storage systems, the high hot spare policy is used by default. You can only run the **change disk\_domain general** command on the CLI to modify the hot spare policy.

- Select **Specify the number of disks** (2000F, 5000F, 6000F, 18000F series storage systems).

The number of disks composing the storage tier will be configured.

- Select **Manually select**.
  - a. Click **Select**.
  - b. In the **Select Disk** dialog box, select the disks you need and click .
  - c. Click **OK** to finish selecting disks.
  - d. Configure the hot spare policy for each storage tier.

 **NOTE**

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

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

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

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

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

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


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

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



**Step 7** Click **OK**.

A message is displayed, indicating that the operation succeeded.

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

----End

## 3.5 Creating a Storage Pool

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

### Context

- You are advised to use different disk domains to create storage pools for the block storage service and file storage service.
- For 2000, 5000, 6000, 18000 series storage systems, a storage pool is a logical combination of one or multiple storage tiers in a disk domain. Different storage tiers may have different RAID policies.
- A RAID policy includes a RAID level and the number of disk blocks and parity blocks and parity blocks of this RAID level.
- The RAID level is classified into typical configuration and flexible configuration based on the number of data blocks and parity blocks. The detailed configuration is shown in [Table 3-9](#).

**Table 3-9** RAID level configuration

RAID Level	Typical Configuration	Flexible Configuration
RAID 0	-	-
RAID 1	<ul style="list-style-type: none"> <li>● 2D<sup>a</sup></li> <li>● 4D</li> </ul>	-
RAID 10	-	-
RAID 3	<ul style="list-style-type: none"> <li>● 2D+1P<sup>b</sup></li> <li>● 4D+1P</li> <li>● 8D+1P</li> </ul>	2D+1P to 13D+1P
RAID 5	<ul style="list-style-type: none"> <li>● 2D+1P</li> <li>● 4D+1P</li> <li>● 8D+1P</li> </ul>	2D+1P to 13D+1P
RAID 50	<ul style="list-style-type: none"> <li>● (2D+1P)x2</li> <li>● (4D+1P)x2</li> <li>● (8D+1P)x2</li> </ul>	-

RAID Level	Typical Configuration	Flexible Configuration
RAID 6	<ul style="list-style-type: none"> <li>● 2D+2P</li> <li>● 4D+2P</li> <li>● 8D+2P</li> <li>● 16D+2P</li> </ul>	2D+2P to 26D+2P
<p>a: <b>D</b> indicates the data block.</p> <p>b: <b>P</b> indicates the parity block.</p> <p><b>NOTE</b></p> <p>For 2000, 5000, 6000, 18000 series storage systems, if the RAID level of one storage tier is configured with flexible configuration first, this tier is the primary control tier that controls other tiers' RAID policies. The number of RAID data disks of the primary control tier and the number of RAID data disks of other tiers must be a multiple of 1, 2, 4, or 8. For example, if the performance tier is the primary control tier and its RAID policy is 3D+1P, the RAID policy of other tiers must be 3D+1P, 6D+2P, or so on, and cannot be 4D+1P. If you want to change the current primary control tier, deselect this tier and select it again.</p>		

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

## Procedure

**Step 1** Log in to DeviceManager.

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

**Step 3** Click **Create**.

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

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

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

**NOTE**

- The name must be unique.
- The name can contain only letters, digits, periods (.), underscores (\_), and hyphens (-).
- The value contains 1 to 31 characters.

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

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

**NOTE**

**Usage** is unchangeable after it is configured.

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

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

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

1. Select storage tiers that meet service requirements.
2. Set basic properties for the storage tiers. **Table 3-10** describes related parameters.

**Table 3-10** Storage tier parameters

Parameter	Description	Setting
RAID Policy	<p>RAID level. The system supports RAID 0, RAID 1, RAID 10, RAID 3, RAID 5, RAID 50, and RAID 6.</p> <p><b>NOTE</b>                      RAID 0 only supports configuration in CLI mode. For details, see the <i>Command Reference</i> of the corresponding product model.</p>	<p>Select a RAID policy based on the planned solution.</p> <p>The default RAID policy of a storage tier varies with the number of disks allocated to the storage tier.</p> <ul style="list-style-type: none"> <li>- If the number of disks allocated to a storage tier is smaller than 10:                             <ul style="list-style-type: none"> <li>■ Default RAID policy of the high performance tier: RAID 10</li> <li>■ Default RAID policy of the performance tier: RAID 5 (4D+1P)</li> <li>■ Default RAID policy of the capacity tier: RAID 6 (4D+2P)</li> </ul> </li> <li>- If the number of disks allocated to a storage tier is equal to 10:                             <ul style="list-style-type: none"> <li>■ Default RAID policy of the high performance tier: RAID 10</li> <li>■ Default RAID policy of the performance tier: RAID 5 (8D+1P)</li> <li>■ Default RAID policy of the capacity tier: RAID 6 (4D+2P)</li> </ul> </li> <li>- If the number of disks allocated to a storage tier is greater than 10:                             <ul style="list-style-type: none"> <li>■ Default RAID policy of the high performance tier: RAID 10</li> </ul> </li> </ul>

Parameter	Description	Setting
		<ul style="list-style-type: none"> <li>■ Default RAID policy of the performance tier: RAID 5 (8D+1P)</li> <li>■ Default RAID policy of the capacity tier: RAID 6 (8D+2P)</li> </ul> <p><b>NOTE</b>                      If the number of SSDs in a disk domain is two or three, you are advised to configure the corresponding high-performance tier to RAID 1 (2D).</p>
Capacity	The capacity that the storage tier provides for the storage pool. Three capacity levels are provided: TB, GB, and PB. <b>NOTE</b> Select <b>Use all available capacity</b> , and then you can allocate all available capacity in this storage layer to the new storage pool.	The capacity must be not larger than the available capacity of the storage tier.

 **NOTE**

- If the storage pool consists of multiple storage tiers, you are advised to set a SmartTier policy. The policy enables data to migrate among different types of storage tiers, optimizing storage performance distribution.
- You are advised to create RAID 6 groups on the capacity tier to ensure data security.

**Step 8** Configure SmartTier policy for the storage pool being created.

1. Click **Set SmartTier Policy**.

The **Set SmartTier Policy** dialog box is displayed. [Table 3-11](#) lists related parameters.

**Table 3-11** SmartTier policy of the storage pool

Parameter	Description	Setting
Service Monitoring Period	<p>Period of time during which the service is monitored and hotspot statistics is collected after you select <b>Enable I/O monitoring</b>. The statistics serves as guidance for data to migrate among different storage tiers.</p> <p>You can specify the period by setting days, <b>Start Time</b>, and <b>Duration</b>.</p>	<p>[Default value]                      I/O monitoring disabled</p>
Data Migration Plan	<p>The trigger policy of data relocation between the storage layers in a storage pool. The policies include:</p> <ul style="list-style-type: none"> <li>- Manual: You must manually trigger the data relocation among storage tiers. The data relocation process is transparent to application servers. Manual data relocation can be performed anytime.</li> <li>- Periodical: You must specify the start time and duration of data relocation for the storage system to perform data relocation automatically at the specified time. This reduces the management cost and complexity. The data relocation process is transparent to application servers. Automatic data relocation is performed only at the specified time.</li> </ul>	<p>[Default value]                      Manual</p>

 **NOTE**

- SmartTier policy is only applicable when **Usage** of a storage pool is configured as **Block Storage Service**.
- SmartTier is not supported by 2000F, 5000F, 6000F, 18000F series storage systems.
- The dynamic storage tier function can be used when multiple tiers are created. This requires an valid SmartTier license.
- If **Data Migration Plan** is set to **Periodical**, I/Os are monitored on a 7 x 24 basis by default. If **Data Migration Plan** is set to **Manual**, select a path to start migration.
- A storage pool configured with SmartTier needs to reserve free space because SmartTier requires extra data exchange space to dynamically migrate data.

2. Click **OK**. The **Create Storage Pool** dialog box is displayed.

**Step 9** Set advanced properties for the storage pool.

1. Click **Advanced**.

The **Advanced Property Settings** dialog box is displayed. [Table 3-12](#) describes the related parameters.

**Table 3-12** Storage pool advanced parameters

Parameter	Description	Setting
Data Protection Capacity Alarm Threshold (%)	When ratio the data protection capacity of the storage pool to the total capacity of the storage pool exceeds the capacity alarm threshold, the system generates an alarm.	[Value range] 1 to 100 [Default value] 100

Parameter	Description	Setting
Used Capacity Alarm Threshold (%)	<p>If a storage pool contains a LUN or a thin LUN and both LUNs are equipped with value-added services, an alarm will be generated when the percentage of the storage pool's used capacity to its total capacity reaches the alarm threshold of the used capacity. The alarm is generated in 3 circumstances:</p> <ul style="list-style-type: none"> <li>- When the used capacity reaches the used capacity alarm threshold, the system generates an alarm informing that the capacity of storage pool is insufficient.</li> <li>- When the used capacity alarm threshold is no greater than 88 and the used capacity reaches 90%, the system generates an alarm informing that the storage pool is running out.</li> <li>- When the used capacity alarm threshold is no greater than 88 and the used capacity reaches (used capacity alarm threshold +2)%, the system generates an alarm informing that the storage pool is running out.</li> </ul> <p><b>NOTE</b>                      If the used capacity alarm threshold is set as 85, when the used capacity reaches 85%, the system generates an alarm informing that the capacity of storage pool is insufficient, and when the used capacity reaches 90%, the system generates an alarm informing that the storage pool is running out. If the used capacity alarm threshold is set as 91, when the used capacity reaches 93%, the system generates an alarm informing that the storage pool is running out.</p> <p>A proper used capacity alarm threshold helps you monitor the capacity usage of a storage pool.</p>	<p>[Value range]                      1 to 95                      [Default value]                      80</p>



Parameter	Description	Setting
Data Migration Granularity	<p>A logical storage space with a fixed size divided from a CKG. It is the smallest unit (granularity) for data migration and hotspot data statistics collection. It is also the smallest unit for space application and release in a storage pool. The default value <b>4 MB</b> is recommended. The value cannot be changed after being set.</p> <p><b>NOTE</b> You can configure this parameter only when RAID levels of storage tiers are typical configuration.</p>	<p>[Value range] 512 KB to 64 MB</p> <p>[Default value] 4 MB</p>

Parameter	Description	Setting
Strip Depth	<p>Strip refers to that continuous data is divided into data blocks of the same size and data blocks are distributed on different disks of storage devices. In this way, I/O loads are balanced among disks, improving read/write performance.</p> <p>Strip depth refers to strip size, indicating the size of data blocks on each disk. Smaller strip size indicates smaller data blocks. These data blocks are distributed on more disks, improving transmission performance. However, more time is required to find different data blocks, decreasing disk locating performance. On the contrary, fewer data blocks indicate lower transmission performance but higher disk locating performance.</p> <p>The value of this parameter can be:</p> <ul style="list-style-type: none"> <li>- System auto select The system selects the optimal strip depth based on the RAID policy of the storage tier and data migration granularity.</li> <li>- 32 KB</li> <li>- 64 KB</li> <li>- 128 KB 128 KB is recommended for random read/write services (such as in database scenarios).</li> <li>- 256 KB</li> <li>- 512KB 512 KB is recommended for sequential read/write services (such as media asset scenarios)</li> </ul> <p><b>NOTE</b> The parameter value cannot be changed after being determined.</p>	<p>[Default value] System auto select</p>

2. Click **OK**.

**Step 10** In the **Create Storage Pool** dialog box, Click **OK**.

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

**Step 11** Click **Close**.

----End

## 3.6 Creating a LUN

The storage space of a newly created storage pool cannot be identified by the host. The host can use the storage space only after the storage space of the storage pool is divided into LUNs and the LUNs are mapped to the host.

### Prerequisites

- At least one storage pool has been created. If the storage system has no storage pool, create one first.
- Only administrators and super administrators are allowed to create LUNs.

### Context

- As a logical disk accessible to hosts, a thin LUN is configured with an initial capacity when created and then dynamically allocated required storage resources when its available capacity is insufficient.
- As a logical disk accessible to hosts, a thick LUN is allocated the specified capacity during the creation based on the automatic provisioning technology.

 **NOTE**

When a host initially reads data from and writes data to a storage system, thick LUNs deliver better performance and thin LUNs boasts higher space utilization.

- A PE LUN does not provide storage space. Therefore, it cannot be allocated any capacity.
- In the advanced properties of a PE LUN, you can only configure its owning controller.

 **NOTE**

If you want to use a thin LUN, you need to import and activate the SmartThin license in the storage device.

### Precautions

- Before creating a LUN, handle alarm **Available Space In The Storage Pool Is Insufficient**.
- If a storage pool has thin LUNs and the capacity of all LUNs exceeds that of the storage pool, you are advised to expand the storage pool when alarm **No Available Space In The Storage Pool** appears.

### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **LUN**.

**Step 3** Click **Create**.

The **Create LUN** dialog box is displayed.

**Create LUN**

\* Name: LUN001

Description:

SmartThin:  Enable  
If SmartThin is enabled, the storage system creates thin LUNs and dynamically allocates storage capacity to thin LUNs based on the actual capacity used by hosts instead of allocating all the preset capacity to thin LUNs, achieving on-demand allocation.

Owning Storage Pool: StoragePool002   
Available Capacity 1.999 TB

\* Capacity: 5 GB   
 Use all of the available capacity of the owning storage pool

\* Quantity: 5  
A maximum of 500 LUNs can be created at one time. When you create multiple LUNs, the system automatically adds a suffix number to each LUN name to distinguish between LUNs. You can also manually specify suffixes.

[All options](#)

**Step 4** Set basic properties for the LUN.  
[Table 3-13](#) describes related parameters.

**Table 3-13** LUN parameters

Parameter	Description	Value
Name	Name of a newly created LUN.	[Value range] <ul style="list-style-type: none"> <li>● The name must be unique.</li> <li>● The name can contain only letters, digits, periods (.), underscores (_), and hyphens (-).</li> <li>● The name contains 1 to 31 characters.</li> </ul> [Example] LUN001
Description	Description of a LUN.	[Example] -
Start ID	ID of a LUN. <b>NOTE</b> <ul style="list-style-type: none"> <li>● The system automatically allocates an ID to a newly created LUN by default.</li> <li>● If you want to manually set a LUN ID, do not select <b>Automatic allocate</b>. Instead, enter an ID manually.</li> <li>● When creating a single LUN, the value you enter is the ID of the LUN.</li> <li>● When creating LUNs in a batch, the system automatically allocates an ID starting from the value you have entered to each LUN.</li> </ul>	[Example] 2
Use Type	Use type of a LUN. <ul style="list-style-type: none"> <li>● Common LUN Including thin LUNs and thick LUNs.</li> <li>● PE LUN PE LUNs are only applied for VVol LUNs in VMware software defined storage. VVol provides storage space for VMs. A PE LUN is used as an I/O demultiplexer to simplify the connection between a VM and a VVol LUN. VM I/Os are sent to the corresponding VVol LUN through a PE LUN.</li> </ul>	[Default value] Common LUN

Parameter	Description	Value
SmartThin	<p>You can enable the SmartThin feature to create thin LUNs.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>To use this feature, you must purchase a SmartThin license.</li> <li>After SmartThin is enabled, the storage system does not allocate the configured capacity to a LUN at a time. Within configured capacity, the storage system allocates the storage resource to the LUN based on the actual capacity used by the host.</li> </ul>	<p>[Example]</p> <p>Disable</p>
Owning Storage Pool	<p>Storage pool to which the LUN you are creating belongs.</p> <p><b>NOTE</b></p> <p>If the storage system has no storage pool, click <b>Create</b> to create one.</p>	<p>[Example]</p> <p>storagepool002</p>
Capacity	<p>Capacity of a LUN. A user specifies the capacity when creating a LUN.</p> <ul style="list-style-type: none"> <li>When SmartThin is enabled, this parameter indicates the maximum capacity that can be allocated to a thin LUN. That is, the total storage resources dynamically allocated by the system to the thin LUN cannot exceed the value of this parameter.</li> <li>When SmartThin is disabled, this parameter indicates the capacity allocated to a thick LUN at a time.</li> </ul>	<p>[Value range]</p> <p>The value must be an integer.</p> <ul style="list-style-type: none"> <li>The maximum capacity of thick LUNs must be less than or equal to the available capacity of the storage pool.</li> <li>The maximum capacity of thin LUNs must be less than or equal to its specifications.</li> <li>The system supports creating block-level LUNs. Select capacity unit <b>Blocks</b> when creating LUNs. One block is 512 bytes.</li> </ul> <p>[Example]</p> <p>2 GB</p>
Use all the available capacity of the owning storage pool	<p>If this option is selected, all free space of the owning storage pool is allocated to this LUN.</p>	<p>[Example]</p> <p>-</p>

Parameter	Description	Value
Quantity	<p>Number of LUNs created in a batch. Set this parameter based on your need.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>LUNs created in a batch have the same capacity.</li> <li>The total capacity of LUNs created in a batch must be less than or equal to the available capacity of the storage pool.</li> </ul>	<p>[Value range]</p> <p>1 to 500</p> <p>[Example]</p> <p>2</p>
Manually specify the suffix	<p>When creating multiple LUNs, the system automatically appends a suffix number to each LUN name for LUN distinction. You can manually set the start suffix number after selecting this option.</p> <p><b>NOTE</b></p> <p>If this option is not selected, the suffix number starts at 0000 by default.</p>	<p>[Example]</p> <p>-</p>
Start Number	<p>This parameter is valid after <b>Manually specify the suffix</b> is selected. From the configured start number, the system incrementally appends a suffix number to the name of each LUN for LUN distinction.</p>	<p>[Value range]</p> <p>0 to (10000 - Number of LUNs to be created)</p> <p><b>NOTE</b></p> <p>If you want to create 300 LUNs, the value range of the start number is 0 to 9700.</p>

 **NOTE**

- **Start ID, Use Type, Manually specify the suffix, and Start Number** are hidden options. If you want to display these options, click **All options**.
- When you configure **Capacity** and **Quantity** for LUNs, consider that the number of LUNs will affect the management complexity and ease-of-use. For example, fifty 1 TB LUNs are easier to manage than a hundred of 500 GB LUNs.

**Step 5 Optional:** Set advanced properties for the LUN.

- If a common LUN is created, perform the following steps.
  - Click **Advanced**. The **Advanced** dialog box is displayed.
  - Set advanced properties for the LUN. Click the **Properties** and **Tuning** tabs to set related parameters, as described in [Table 3-14](#) and [Table 3-15](#) respectively.

Advanced ✕

---

**Properties** Tuning

Owning Controller:  ▼

Initial Capacity Allocation Policy:  ▼

---

Cache Policy

Read Policy:  ▼ ?

Write Policy:  ▼ ?

---

Prefetch Policy ?

No prefetch

Intelligent prefetch

Constant prefetch Prefetch Size (KB)  (0-1024)

Variable prefetch Prefetch Multiple  (0-1024)

---

Masquerading

Inherited masquerading:  Enable ?



**Table 3-14** Properties parameters

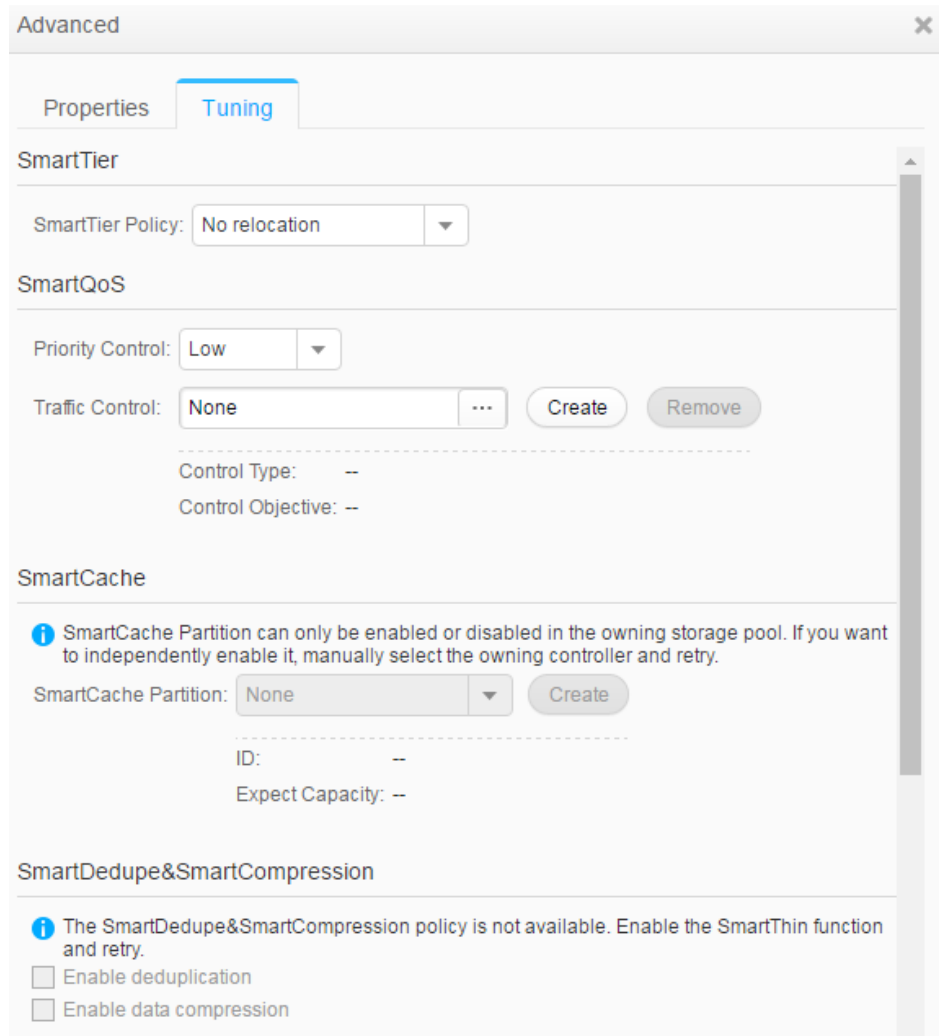
Parameter	Description	Value
Owning Controller	<p>Owning controller of a LUN.</p> <ul style="list-style-type: none"> <li>■ For dual-controller storage device, the system supports the following choices:                             <ul style="list-style-type: none"> <li>○ <b>Auto select</b>: The system automatically specifies the owning controller of LUNs and allocates LUNs evenly to different controllers by default.</li> <li>○ <b>CTEO.A</b>: Allocates LUNs in the storage system to controller A.</li> <li>○ <b>CTEO.B</b>: Allocates LUNs in the storage system to controller B.</li> </ul> </li> <li>■ For four-controller storage device, the system supports the following choices:                             <ul style="list-style-type: none"> <li>○ <b>Auto select</b>: The system automatically specifies the owning controller of LUNs and allocates LUNs evenly to different controllers by default.</li> <li>○ <b>CTEO.A</b>: Allocates LUNs in the storage system to controller A.</li> <li>○ <b>CTEO.B</b>: Allocates LUNs in the storage system to controller B.</li> <li>○ <b>CTEO.C</b>: Allocates LUNs in the storage system to controller C.</li> <li>○ <b>CTEO.D</b>: Allocates LUNs in the storage system to controller D.</li> </ul> </li> </ul> <p><b>NOTE</b>                      To allocate LUNs to controllers for load balancing, you are advised to select <b>Auto select</b>.</p>	<p>[Value range]</p> <ul style="list-style-type: none"> <li>■ For dual-controller storage device, the value can be <b>Auto select</b>, <b>CTEO.A</b>, or <b>CTEO.B</b>.</li> <li>■ For four-controller storage device, the value can be <b>Auto select</b>, <b>CTEO.A</b>, <b>CTEO.B</b>, <b>CTEO.C</b>, or <b>CTEO.D</b>.</li> </ul> <p>[Example]                      Auto select</p> <p>[Default value]                      Auto select</p>

Parameter	Description	Value
Initial Capacity Allocation Policy	<p>Policy for the storage tier to allocate capacity to a LUN.</p> <ul style="list-style-type: none"> <li>■ <b>Automatic allocation:</b> The storage system allocates capacity to a LUN from the performance tier first. If the capacity of the performance tier is insufficient, the storage system allocates capacity from other storage tiers, first from the capacity tier and then from the high performance tier.</li> <li>■ <b>Allocate from the high-performance tier first:</b> The storage system allocates capacity to a LUN from the high performance tier first. If the capacity of the high performance tier is insufficient, the storage system allocates capacity from other storage tiers, first from the performance tier and then from the capacity tier.</li> <li>■ <b>Allocate from the performance tier first:</b> The storage system allocates capacity to a LUN from the performance tier first. If the capacity of the performance tier is insufficient, the storage system allocates capacity from other storage tiers, first from the capacity tier and then from the high performance tier.</li> <li>■ <b>Allocate from the capacity tier first:</b> The storage system allocates capacity to a LUN from the capacity tier first. If the capacity of the capacity tier is insufficient, the storage system allocates capacity from other storage tiers, first from the performance tier and then from the high performance tier.</li> </ul>	<p>[Value range]</p> <p>The value can be <b>Automatic allocation, Allocate from the high performance tier first, Allocate from the performance tier first, or Allocate from the capacity tier first.</b></p> <p>[Example]</p> <p>Automatic allocation</p> <p>[Default value]</p> <p>Automatic allocation</p>

Parameter	Description	Value
Read Policy	<p>Data read policy of a cache.</p> <p>The system supports the following read policies.</p> <ul style="list-style-type: none"> <li>■ <b>Resident:</b> suitable for random access. The policy caches data as long as possible to improve the read hit ratio.</li> <li>■ <b>Default:</b> suitable for common access. The policy strikes a balance between the read hit ratio and disk access performance.</li> <li>■ <b>Recycle:</b> suitable for sequential access. The policy releases idle cache resources as soon as possible for other services to use.</li> </ul>	<p>[Value range]</p> <p>The value can be <b>Resident, Default, or Recycle.</b></p> <p>[Example] Resident</p> <p>[Default value] Default</p>
Write Policy	<p>Data write policy of a cache.</p> <p>The system supports the following write policies.</p> <ul style="list-style-type: none"> <li>■ <b>Resident:</b> suitable for random access. The policy caches data as long as possible to improve the write hit ratio.</li> <li>■ <b>Default:</b> suitable for common access. The policy strikes a balance between the write hit ratio and disk access performance.</li> <li>■ <b>Recycle:</b> suitable for sequential access. The policy releases idle cache resources as soon as possible for other services to use.</li> </ul>	<p>[Value range]</p> <p>The value can be <b>Resident, Default, or Recycle.</b></p> <p>[Example] Resident</p> <p>[Default value] Default</p>

Parameter	Description	Value
Prefetch Policy	<p>Read mode of a LUN. When reading data, the storage system prefetches required data from disks to the cache in advance according to a preset policy. The supported prefetch policies are described as follows:</p> <ul style="list-style-type: none"> <li>■ <b>No prefetch:</b> The storage system reads data based on the read length specified in the I/O request. As a low read hit ratio may lead to performance degradation, <b>No prefetch</b> is recommended for random read services.</li> <li>■ <b>Intelligent prefetch:</b> The intelligent prefetch analyzes the continuity of the read requests from the host. If the read requests are continuous, the data following the current read request is prefetched from disks to the cache. By doing so, the cache hit ratio can be increased. If the requests are random reads, the data is read directly from disks. This policy is applicable to the scenario where sequential reads and random reads coexist or to the read applications that cannot be determined sequential or random.</li> <li>■ <b>Constant prefetch:</b> A constant length of data is read from disks each time when the cache reads data from the disks. The length is user-defined, ranging from 0 to 1024 KB. Constant prefetch is applicable to the sequential read applications with fixed-size data blocks, for example, ring back tone (RBT) and requests initiated by multiple users for playing multimedia on demand at the same bit rate.</li> <li>■ <b>Variable prefetch:</b> The cache reads data from disks based on a multiple of the read length specified in the I/O request. The multiple is user-defined, ranging from 0 to 1024. This policy is applicable to the sequential read applications that</li> </ul>	<p>[Value range]                      The value can be <b>No prefetch</b>, <b>Intelligent prefetch</b>, <b>Constant prefetch</b>, or <b>Variable prefetch</b>.                      [Example]                      Intelligent prefetch                      [Default value]                      Intelligent prefetch</p>

Parameter	Description	Value
	<p>have an unfixed size or for the multi-user concurrent read applications whose prefetch data amount cannot be determined, for example, requests initiated by multiple users for playing multimedia on demand at different bit rates.</p>	
Masquerading	<p>Masquerading replaces the identification information of LUNs on the local device with that on the heterogeneous remote device so that heterogeneous remote LUNs can be taken over online.</p> <p><b>Inherited masquerading</b> can be set for local LUNs. You can enable <b>Inherited masquerading</b> and set <b>Remote Device</b>. After <b>Inherited masquerading</b> is set for a LUN, the LUN can inherit the LUN information on the remote device. The information includes VID, PID, and SCSI protocol version.</p> <p><b>NOTE</b>                      Inherited masquerading enables local LUN masquerading for LUN capacity expansion when the remote device has insufficient LUN space.</p>	[Default] Disabled



**Table 3-15** Tuning parameters

Parameter	Description	Setting
SmartTier Policy	<p>Policy for the storage system to relocate data among storage tiers.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>■ To apply this policy, you must purchase a SmartTier license.</li> <li>■ If LUN formatting is not complete, the data in the extents that are not formatted in the LUN will not be migrated.</li> <li>■ SmartTier is not supported by 2000F, 5000F, 6000F, 18000F series storage systems.</li> <li>■ <b>No relocation:</b> Select this policy when the access frequency of the LUN is stable and the current storage tier is suitable for the services.</li> <li>■ <b>Automatic relocation:</b> Select this policy when you are unclear about the service type and access frequency of the LUN. This policy enables the storage system to collect and analyze performance data and then relocate data among storage tiers based on the activity level of the data.</li> <li>■ <b>Relocation to high-performance tier:</b> Select this policy when data on the LUN is frequently accessed. This policy enables the storage system to promote data to a storage tier with better performance, improving access efficiency.</li> <li>■ <b>Relocation to low-performance tier:</b> Select this policy when data on the LUN will not be accessed after a period of time. This policy enables the storage system to relocate data to a storage tier that provides moderate performance at a low cost, releasing high-performance storage space for hotspot data.</li> </ul>	<p>[Value range]</p> <p>The value can be <b>No relocation</b>, <b>Automatic relocation</b>, <b>Relocation to high-performance tier</b>, or <b>Relocation to low-performance tier</b>.</p> <p>[Example]</p> <p>No relocation</p> <p>[Default value]</p> <p>No relocation</p>

Parameter	Description	Setting
Priority Control	Priority control of SmartQoS. <b>NOTE</b> To apply this policy, you must purchase a SmartQoS license.	[Value range] The value can be <b>Low, Medium, or High</b> . A LUN, snapshot or file system with a high priority can obtain system resources preferentially. You can set different values for specific LUNs or snapshots based on service priorities, ensuring critical service performance. [Example] Low [Default value] Low
Traffic Control	Traffic control policy of SmartQoS. There are two types of traffic control policies: <ul style="list-style-type: none"> <li>■ <b>Upper-limit</b> traffic control policy: controls the upper limits of bandwidth and IOPS.</li> <li>■ <b>Lower-limit</b> traffic control policy: controls the lower limits of bandwidth and IOPS and the upper limit of latency.</li> </ul> <b>NOTE</b> <ul style="list-style-type: none"> <li>■ You can only select LUNs, snapshots and file systems with high I/O priority for a lower-limit traffic control policy, and you must not change the priorities of the LUNs, snapshots and file systems that are working with a lower-limit traffic control policy.</li> <li>■ To apply this policy, you must purchase a SmartQoS license.</li> </ul> If no traffic control policy exists, click <b>Create</b> to create one.	[Value range] The value is user defined. [Example] - [Default value] -



Parameter	Description	Setting
SmartCache Partition	<p>Specifies the SmartCache partition for the LUN. In the scenario that read operations are more than write operations and hot spot data exists, use SSDs as the cache, employing SSD high read performance to improve system read performance.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>■ To apply this policy, you must purchase a SmartCache license.</li> <li>■ Select the owning controller of a LUN manually. The controller must be the same as the owning controller of SmartCache. Otherwise, SmartCache is unavailable.</li> <li>■ SmartCache does not support self-encrypting SSDs.</li> <li>■ SmartCache is not supported by 2000F, 5000F, 6000F, 18000F series storage systems.</li> </ul> <p>If no SmartCache partition exists, click <b>Create</b> to create one.</p>	<p>[Default value]</p> <p>-</p>

Parameter	Description	Setting
SmartDedupe&SmartCompression	<p>SmartDedupe and SmartCompression policies.</p> <p><b>NOTE</b>                      SmartDedupe and SmartCompression are value-added features. To make the policy take effect, you need to purchase the licenses of SmartDedupe&amp;SmartCompression and enable the SmartThin function.</p> <ul style="list-style-type: none"> <li>■ <b>Enable deduplication:</b> After the fingerprints of data blocks being compared, the data blocks with same fingerprints are confirmed as the same data blocks. The duplicated data block is deleted and only the original data block is kept.</li> <li>■ <b>Enable data compression:</b> decreases the storage space occupied by data.</li> </ul> <p><b>NOTE</b>                      If you have not enabled either SmartDedupe or SmartCompression when you create a LUN, you cannot enable them any more after the LUN is created.</p> <p>Virtual Desktop Infrastructure (VDI) is a typical application scenario of SmartDedupe. Databases, file services, engineering data, as well as earthquake and geological exploration data are typical application scenarios of SmartCompression.</p> <p>The efficiency of storage space saving is closely related to the type of data. Observe the following principles when determining whether to use SmartDedupe or SmartCompression:</p> <ul style="list-style-type: none"> <li>■ For non-duplicate archive data such as image files or encrypted data, you are advised not to use SmartDedupe and SmartCompression.</li> <li>■ For data that has been compressed or encrypted by a hardware device or application (backup or archive application), you are advised not to use SmartDedupe and SmartCompression.</li> </ul>	<p>[Value range]</p> <p>The value is user defined.</p> <p>[Example]</p> <p>-</p> <p>[Default value]</p> <p>-</p>

Parameter	Description	Setting
SmartPartition	<p>Specifies SmartPartition for the LUN. SmartPartition allocates cache resources of the storage system to the LUN to meet the cache hit ratio required by different applications.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>■ To apply this policy, you must purchase SmartPartition license.</li> <li>■ Select the owning controller of a LUN manually. The controller must be the same as the owning controller of SmartPartition. Otherwise, SmartPartition is unavailable.</li> </ul> <p>If no SmartPartition exists, click <b>Create</b> to create one.</p>	<p>[Default value]</p> <p>-</p>

- c. Click **OK**. The **Create LUN** dialog box is displayed.
- If a PE LUN is created, perform the following steps.
  - a. Click **Advanced**. The **Advanced** dialog box is displayed.
  - b. Select the owning controller of the PE LUN. **Table 3-16** describes the related parameter.

**Table 3-16** Advanced properties of a PE LUN

Parameter	Description	Setting
Owning Controller	Owning controller of a LUN. You are advised to allocate LUNs to different controllers for load balancing.	<p>If you are not sure about the owning controller, select <b>Auto select</b>. The storage system will automatically select the owning controller for the LUN.</p> <p>[Example]</p> <p>Auto select</p>

- c. Click **OK**. The **Create LUN** dialog box is displayed.

**Step 6** Confirm the creation of the LUN.

1. Click **OK**.  
The **Execution Result** dialog box is displayed, indicating that the operation succeeded.
2. Click **Close**.

----End

## 3.7 Creating a LUN Group

To allow hosts to use LUNs, you must add LUNs into LUN groups. Then, establish mapping views between the LUN groups and host groups. By doing so, the hosts in the host groups can use the LUNs in the LUN groups. A LUN group can contain 1 to 4096 LUNs. A LUN can be added to a maximum of 8 LUN groups.

### Procedure

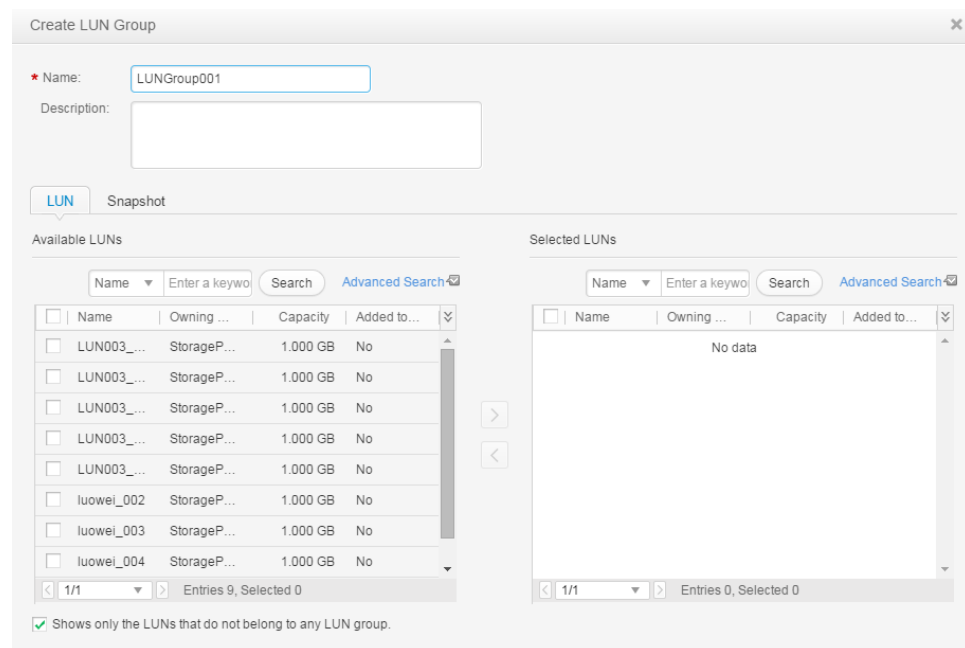
**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **LUN** > **LUN Group**.

**Step 3** Click **Create**.

The **Create LUN Group** dialog box is displayed.

**Step 4** Set basic properties for the LUN group. [Table 3-17](#) describes related parameters.



**Table 3-17** LUN group parameters


Parameter	Description	Setting
Name	Name of a newly created LUN group.	[Value range] <ul style="list-style-type: none"> <li>● The name must be unique.</li> <li>● The name can contain only letters, digits, periods (.), underscores (_), and hyphens (-).</li> <li>● The name contains 1 to 31 characters.</li> </ul> [Example] LUNgroup001
Description	Description of a LUN group.	[Example] -

**Step 5** Select the LUNs or snapshots you want to add to the LUN group.

1. In the **Available LUNs** or **Available Snapshots** area, select one or multiple LUNs or snapshots based on your service need.

 **NOTE**

By default, the **Show only the LUNs that do not belong to any LUN group** checkbox in the bottom left corner of the dialog box is selected to facilitate LUN locating.

2. Click  to add the LUNs or snapshots to the **Selected LUNs** or **Selected Snapshots** area.

**Step 6** Confirm the creation of the LUN group.

1. Click **OK**.  
The **Execution Result** message box is displayed, indicating that the operation succeeded.
2. Click **Close**.

---End

## 3.8 Configuring Connectivity between Host and Storage System

This section describes how to configure the connectivity between a host and a storage system to enable the host to use storage resources.

### 3.8.1 iSCSI Networking

This section describes how to configure the connectivity between host and storage system through iSCSI networking.

### 3.8.1.1 Configuring Ethernet Switches

Configuring VLANs for Ethernet switches can avoid conflicts and improve flexibility of the service systems.

#### Context

On an Ethernet network to which many hosts are connected, a large number of broadcast packets are generated during the host communication. Broadcast packets sent from one host will be received by all other hosts on the network, consuming more bandwidth. Moreover, all hosts on the network can access each other, resulting in data security risks. To save bandwidth and prevent security risks, hosts on an Ethernet network are divided into multiple logical groups. Each logical group is a VLAN.

The following uses HUAWEI Quidway 2700 Ethernet switch as an example to explain how to configure VLANs. In the following example, two VLANs (VLAN 1000 and VLAN 2000) are created. VLAN 1000 contains ports GE 1/0/1 to 1/0/16. VLAN 2000 contains ports GE 1/0/20 to 1/0/24.

#### Procedure

**Step 1** Go to the system view.

```
<Quidway> system-view  
System View: return to User View with Ctrl+Z.
```

**Step 2** Create VLAN 1000 and add ports to it.

```
[Quidway]VLAN 1000  
[Quidway-vlan1000]port GigabitEthernet 1/0/1 to GigabitEthernet 1/0/16
```

**Step 3** Configure the IP address of VLAN 1000.

```
[Quidway-vlan1000]interface VLAN 1000  
[Quidway-Vlan-interface1000]ip address 192.168.1.0 255.255.0.0
```

**Step 4** Create VLAN 2000, add ports, and configure the IP address.

```
[Quidway]VLAN 2000  
[Quidway-vlan2000]port GigabitEthernet 1/0/20 to GigabitEthernet 1/0/24  
[Quidway-vlan2000]interface VLAN 2000  
[Quidway-Vlan-interface2000]ip address 192.168.2.0 255.255.0.0
```

**Step 5** Run the **commit** command to submit the configuration file.

**Step 6** Run the **quit** command to exit the system view.

**Step 7** Run the **save** command to save the configuration file.

----End

### 3.8.1.2 Configuring an IP Address for the Service Network Port on the Application Server

By default, the service network port does not have an IP address. The service network port can receive and send data only after a proper IP address is configured for it.

### 3.8.1.2.1 Configuring an IP Address for the Service Network Port on the Application Server (Windows)

When the storage system uses an iSCSI host port to connect the service network port on the application server, you must configure the IP addresses of the iSCSI host port and service network port on the same network segment to ensure service data transfer.

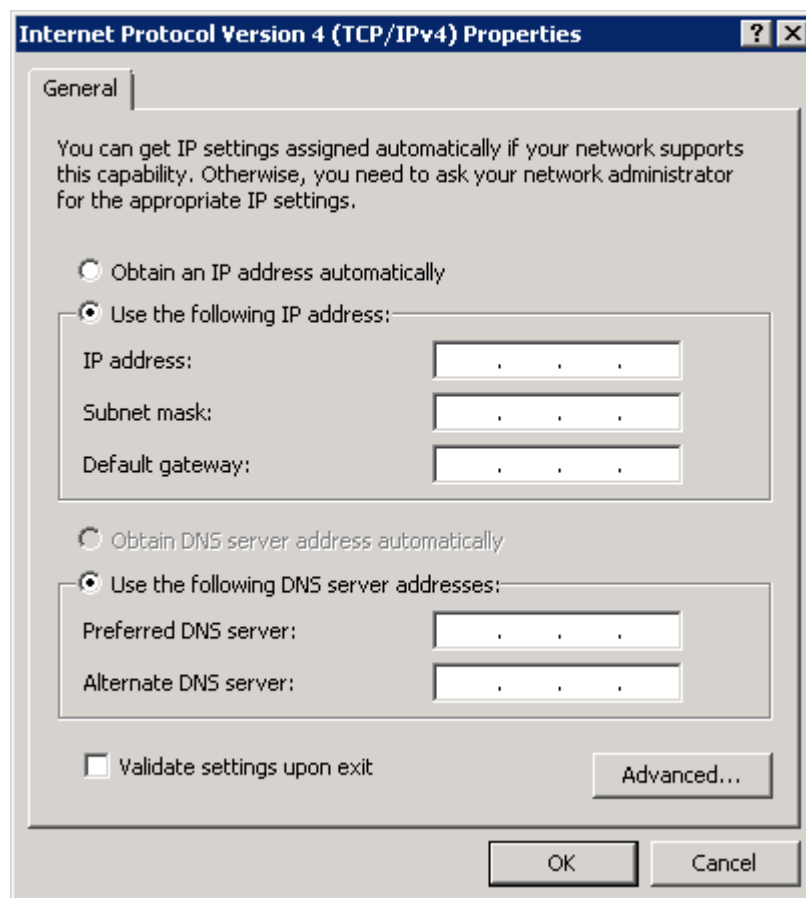
#### Context

This document uses a Windows Server 2008 application server and the network port IP address configured in **Local Area Connection** as an example.

#### Procedure

- Step 1** Log in to the application server and choose **Start > Control Panel > Network and Internet > Network and Sharing Center**.
- Step 2** In the **View your active networks** group box, select **Local Area Connection**.  
The **Local Area Connection Status** dialog box is displayed.
- Step 3** Click **Properties**.  
The **Local Area Connection Properties** dialog box is displayed.
- Step 4** Double-click **Internet Protocol Version 4 (TCP/IPv4)**.  
The **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box is displayed, as shown in [Figure 3-6](#).

**Figure 3-6** Internet Protocol Version 4 (TCP/IPv4) Properties dialog box



- Step 5** In **IP address**, **Subnet mask**, and **Default gateway**, configure the IP addresses of the service network port, subnet mask, and gateway for the application server.
- Step 6** Click **OK**. The **Local Area Connection 4 Properties** dialog box is displayed.
- Step 7** Click **OK**. The **Local Area Connection 4 Status** dialog box is displayed.
- Step 8** Click **Close**. The IP address configuration of the service network port is complete.

 **NOTE**

After completing the configuration, you can run **ipconfig** to check whether the IP address of the application server is correct.

---End

## Follow-up Procedure

After configuring an IP address for the service network port on the application server, run the **ping XXX.XXX.XXX.XXX** command (*XXX.XXX.XXX.XXX* indicates the IP address of the iSCSI host port that connects to the application server). If the command output shows that the application server receives the data packets sent from the iSCSI host port, the communication between the application server and storage system is normal.

### 3.8.1.2.2 Configuring an IP Address for the Service Network Port on the Application Server (SUSE)

The service network port can receive and send data only after a proper IP address is configured for it.

## Context

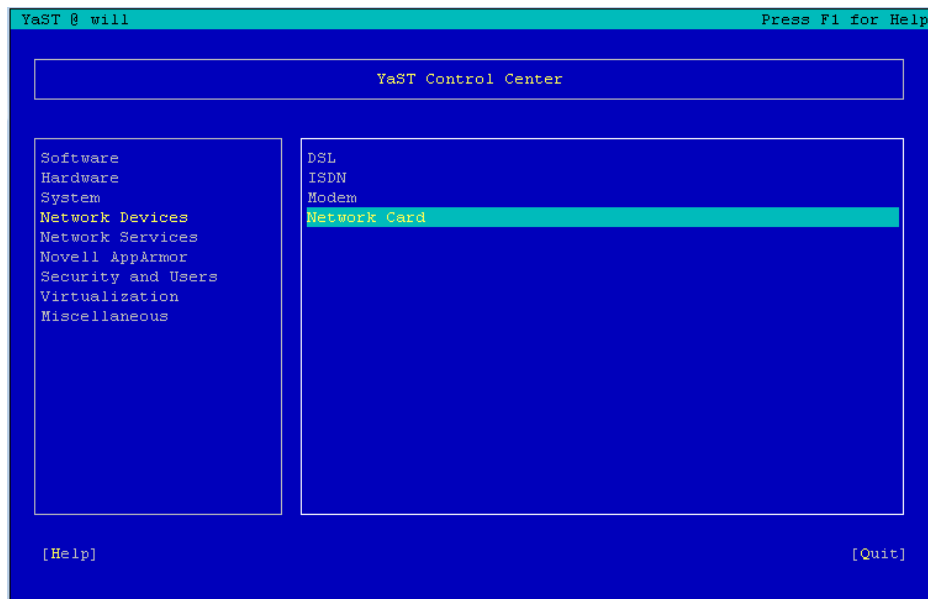
You can use multiple methods to configure an IP address for the service network port of the SUSE-based application server. This section uses the application server running YaST as an example to describe how to configure an IP address for the service network port.

## Procedure

- Step 1** Log in to the SUSE-based application server as user **root**.
- Step 2** Run the **yast** command. The **YaST** screen is displayed.
- Step 3** In the left-hand pane of the **YaST** screen, select **Network Devices**. In the right-hand pane, select **Network Card** and press **Enter**, as shown in [Figure 3-7](#).

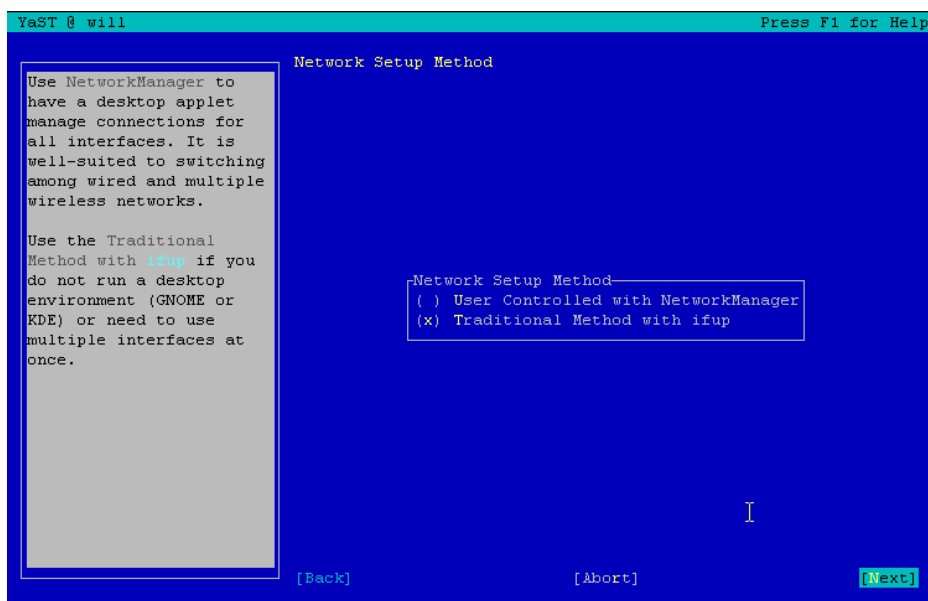


Figure 3-7 YaST Control Center interface



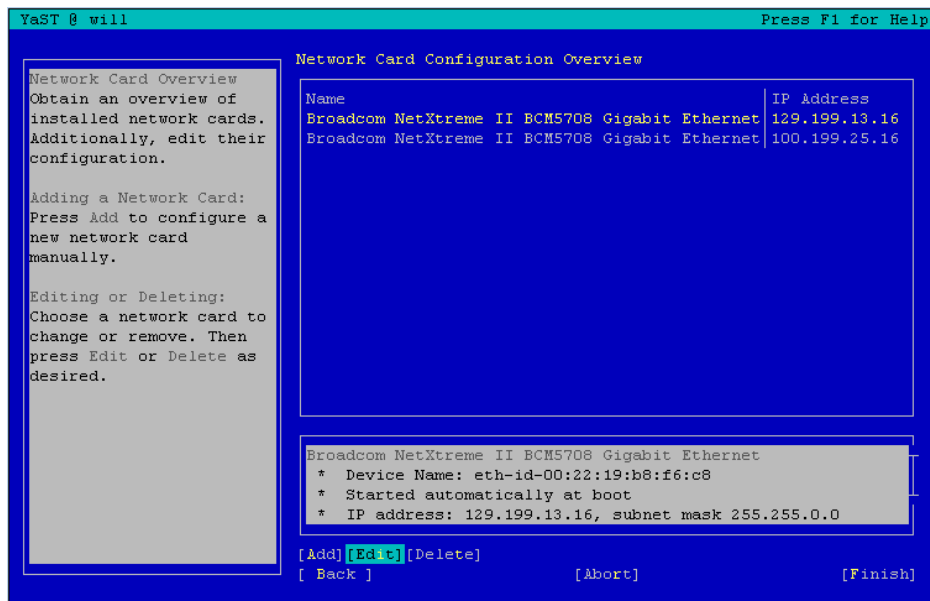
**Step 4** On the **Network Setup Method** interface, select a configuration method (by default, **Traditional Method with ifup** is selected), and press **Enter**. Select **Next**, and press **Enter**, as shown in [Figure 3-8](#).

Figure 3-8 Network Setup Method interface



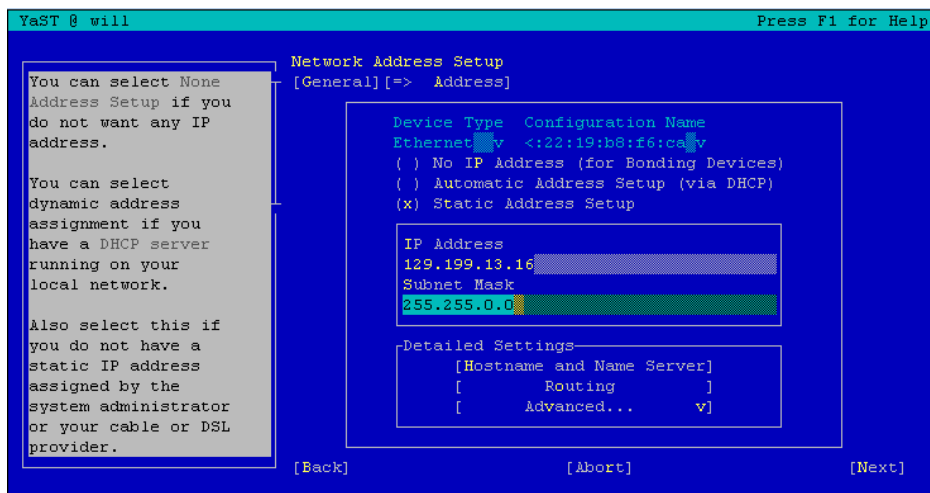
**Step 5** On the **Network Card Configuration Overview** interface, select the network adapter that you want to configure and press **Enter**. Then select **Edit** and press **Enter**, as shown in [Figure 3-9](#).

Figure 3-9 Network Card Configuration Overview interface



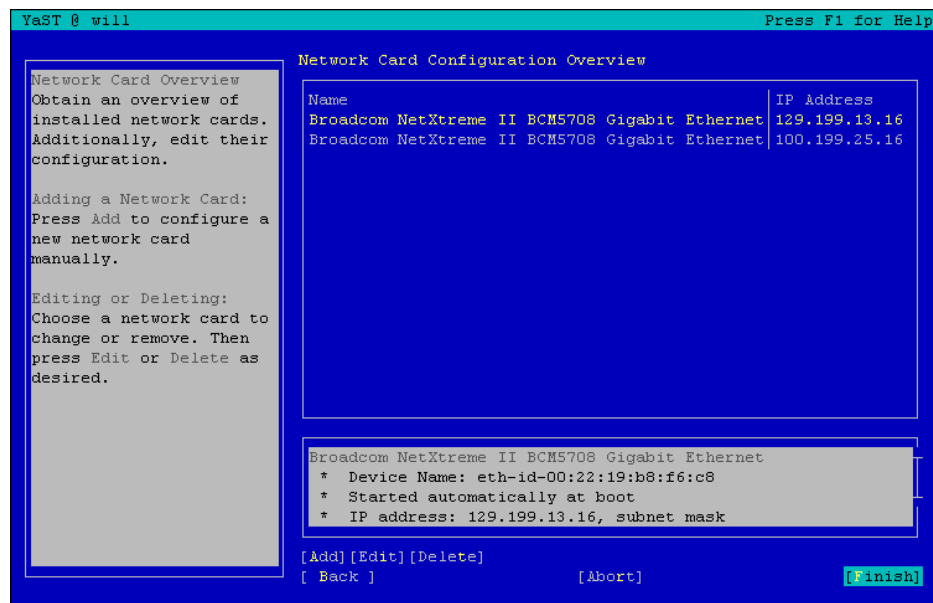
**Step 6** On the **Network Address Setup** interface, set an IP address and subnet mask in **IP Address** and **Subnet Mask**, select **Next**, and press **Enter**, as shown in [Figure 3-10](#).

Figure 3-10 Network Address Setup interface



**Step 7** On the **Network Card Configuration Overview** interface, select **Finish** and press **Enter**, as shown in [Figure 3-11](#).

Figure 3-11 Network Card Configuration Overview interface



----End

## Follow-up Procedure

After completing the configuration:

1. Run the **ifconfig** command to check whether the IP address of the application server is correct.
2. Run the **ping xxx.xxx.xxx.xxx** command (*xxx.xxx.xxx.xxx* indicates the IP address of the iSCSI host port that connects to the application server) to check whether the application server can communicate with the storage system. If the communication between the application server and storage system fails, ensure that the physical link and IP addresses are correct, and perform the following operations:
  - Configure the IP addresses of the iSCSI host port and service network port on the same network segment.
  - If the two IP addresses are on different network segments, add a route to establish a connection between them.

### 3.8.1.2.3 Configuring an IP Address for the Service Network Port on the Application Server (Red Hat)

By default, the service network port does not have an IP address. The service network port can receive and send data only after a proper IP address is configured for it.

## Context

You can use multiple methods to configure an IP address for the service network port of the Red Hat application server. This section uses the script modification method as an example to describe how to configure an IP address for the service network port.

## Procedure

- Step 1** Log in to the Red Hat application server as user **root**.
- Step 2** Run the **ifconfig eth0 up** command to open the service network port (**eth0** is used as an example).
- Step 3** Edit the **ifcfg-eth0** script and configure an IP address.
1. Run the **vi /etc/sysconfig/network-scripts/ifcfg-eth0** command to open the **ifcfg-eth0** file.
  2. Press **i** to enter the editing mode, and edit the **ifcfg-eth0** file.  
  
Add the following field to the **ifcfg-eth0** file. **IPADDR=xxx.xxx.xxx.xxx** and **NETMASK=xxx.xxx.xxx.xxx** indicate the IP address and subnet mask respectively. You need to replace them with the planned IP address and subnet mask.

```
DEVICE=eth0
BOOTPROTO=static
IPADDR=xxx.xxx.xxx.xxx
NETMASK=xxx.xxx.xxx.xxx
TYPE=Ethernet
```
  3. Press **Esc** to exit the editing mode.
  4. Run the **:wq** command to save the changes and exit the **ifcfg-eth0** file.
- Step 4** Run the **/etc/init.d/network restart** command to restart the network service.
- Step 5** Run the **ifconfig eth0** command to check whether the IP address is configured successfully.
- Step 6** Run the **ping XXX.XXX.XXX.XXX** command (**XXX.XXX.XXX.XXX** indicates the IP address of the iSCSI host port connected to the application server) to check whether the application server communicates with the storage system properly. If the communication between the application server and storage system fails, check whether the physical link and IP address are correct.

---



### NOTICE

In some Red Hat versions, the system enables the network and NetworkManager services concurrently by default. Under this condition, a network configuration conflict is easy to occur. You are advised to run **service NetworkManager stop** to disable the NetworkManager service. Then run the **chkconfig NetworkManager off** command to prevent the service from being automatically started after the system is restarted.

---

---End

### 3.8.1.2.4 Configuring an IP Address for the Service Network Port on the Application Server (Solaris)

The service network port can receive and send data only after a proper IP address is configured for it.

## Context

The method used to configure an IP address varies according to different Solaris versions.

- Solaris 10 and earlier versions: Configure an IP address by setting the configuration file of the network port.

- Solaris 11 and later versions: Run the **ipadm** command to configure an IP address for the service network port.

## Solaris 10 and Earlier Versions

**Step 1** Log in to the Solaris-based application server as user **root**.

**Step 2** Run the **dladm show-dev** command to determine the network port for which you want to configure an IP address.

Generally, a Solaris-based server has four network ports of the same model. The four network ports are marked by 0, 1, 2, and 3 respectively. When the system is installed, one network port is selected and a management IP address is configured for it.

```
bash-3.2# dladm show-dev
bge0          link: up      speed: 100   Mbps        duplex: full
bge1          link: unknown speed: 0     Mbps        duplex: unknown
bge2          link: unknown speed: 0     Mbps        duplex: unknown
bge3          link: down    speed: 0     Mbps        duplex: unknown
```

### NOTE

You can run the **ifconfig -a** command to check whether a network adapter is enabled. If the network adapter is not enabled, run the **ifconfig xxx plumb up** command to enable it. In the preceding command, **xxx** indicates the port name such as **bge3**.

**Step 3** Configure an IP address for a port such as **bge3**.

The IP address information is planned as follows: The interface name is **serv01**, the IP address is **192.168.224.100**, the subnet mask is **255.255.255.0**, and the gateway is **192.168.0.1**.

1. Edit the **/etc/hostname.\*** file to configure the network adapter interface name.

```
bash-3.2# vi /etc/hostname.bge3
serv01
```

2. Edit the **/etc/inet/netmasks** file to configure the subnet mask.

```
bash-3.2# vi /etc/inet/netmasks
192.168.224.0 255.255.255.0
```

3. Edit the **/etc/defaultrouter** file to configure the gateway.

```
bash-3.2# vi /etc/defaultrouter
192.168.0.1
```

4. Edit the **/etc/hosts** file to add the IP address and interface name.

```
bash-3.2# vi /etc/hosts
192.168.224.100 serv01
```

**Step 4** Run the **svcs | grep -i physical** command to query the network adapter information.

```
bash-3.00# svcs | grep -i physical
online 14:17:34 svc:/network/physical:default
```

**Step 5** Run the **svcadm restart svc:/network/physical:default** command to restart the network service to enable the configuration to take effect.

 **NOTE**

After the IP address is modified in the `/etc/hosts` file and the system is restarted, the IP address is still the original one. This problem occurs because the original IP address is retained in the `/etc/inet/ipnodes` file. To solve the problem, delete the IP address line from the `/etc/inet/ipnodes` file or change the original IP address to the new one. Then, restart the system.

----End

## Solaris 11 and Later Versions

**Step 1** Log in to the Solaris-based application server as user **root**.

**Step 2** Run the `netadm enable -p ncp DefaultFixed` command to switch the network management mode from automatic to manual.

```
bash-3.2# netadm enable -p ncp DefaultFixed

bash-3.2# netadm list

netadm: DefaultFixed NCP is enabled;

automatic network management is not available.

'netadm list' is only supported when automatic network management is active.
```

**Step 3** Run the `dladm show-phys` command to determine the network port for which you want to configure an IP address.

```
bash-3.2# dladm show-phys

LINK          MEDIA          STATE          SPEED  DUPLEX  DEVICE
net2          Ethernet       up             10000  full   hxge0
net3          Ethernet       up             10000  full   hxge1
net4          Ethernet       up             10     full   usbecm0
net0          Ethernet       up             1000   full   igb0
net1          Ethernet       up             1000   full   igb1
net9          Ethernet       unknown        0      half   e1000g0
net5          Ethernet       unknown        0      half   e1000g1
net10         Ethernet       unknown        0      half   e1000g2
net11         Ethernet       unknown        0      half   e1000g3
```

**Step 4** Configure an IP address for a port such as **net0**.

The IP address information is planned as follows: The IP address is **192.168.224.200**, the subnet mask is **255.255.255.0**, and the gateway is **192.168.0.1**.

1. Run the `ipadm` command to configure the IP address.

```
bash-3.2# ipadm create-ip net0

bash-3.2# ipadm create-addr -T static -a 192.168.224.200/24 net0/v4
```

2. Run the `route` command to configure the gateway.

```
bash-3.2# route -p add default 192.168.0.1

add net default: gateway 192.168.0.1

add persistent net default: gateway 192.168.0.1
```

```
bash-3.2#
```

---End

### 3.8.1.2.5 Configuring an IP Address for the Service Network Port on the Application Server (AIX)

The service network port can receive and send data only after a proper IP address is configured for it.

#### Context

Configure an IP address for a service network port on the application server using the smit method.

#### Procedure

- Step 1** Log in to the AIX-based application server as user **root**.
- Step 2** Run the **smitty tcpip** command to go to the IP address configuration page. Click **Minimum Configuration & Startup**. On the page that is displayed, select the iSCSI service network port you want to set and press **Enter** to go to the network port configuration page.

```
TCP/IP
Move cursor to desired item and press Enter.
Minimum Configuration & Startup
Further Configuration
Use DHCP for TCP/IP Configuration & Startup
IPv6 Configuration
Quality of Service Configuration & Startup
Configure IP Security (IPv4)
Configure IP Security (IPv6)

-----+-----
|                                     |
|                                     |
| Available Network Interfaces       |
|                                     |
| Move cursor to desired item and press Enter. |
|                                     |
| en0 02-00 Standard Ethernet Network Interface |
| en1 02-01 Standard Ethernet Network Interface |
| en2 02-04 Standard Ethernet Network Interface |
| en3 02-05 Standard Ethernet Network Interface |
| et0 02-00 IEEE 802.3 Ethernet Network Interface |
| et1 02-01 IEEE 802.3 Ethernet Network Interface |
| et2 02-04 IEEE 802.3 Ethernet Network Interface |
| et3 02-05 IEEE 802.3 Ethernet Network Interface |
|                                     |
| F1=Help           F2=Refresh       F3=Cancel |
| F8=Image          F10=Exit         Enter=Do  |
| /=Find            n=Find Next      |
| F9=Shell          |                                     |
+-----+-----
```

- Step 3** Configure an IP address.  
In **Internet ADDRESS (dotted decimal)**, enter the IP address. In **Network MASK (dotted decimal)**, enter the subnet mask. In **Address (dotted decimal or symbolic name)**, enter the gateway.

```
Minimum Configuration & Startup

To Delete existing configuration data, please use Further Configuration menus

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

[Entry Fields]
* HOSTNAME [3750blpar02]
* Internet ADDRESS (dotted decimal) []
* Network MASK (dotted decimal) []
* Network INTERFACE en3
  NAMESERVER
    Internet ADDRESS (dotted decimal) []
    DOMAIN Name []
  Default Gateway
    Address (dotted decimal or symbolic name) []
    Cost [0] #
    Do Active Dead Gateway Detection? yes +
  Your CABLE Type N/A +
  START Now no +

F1=Help      F2=Refresh   F3=Cancel    F4=List
F5=Reset     F6=Command   F7=Edit      F8=Image
F9=Shell     F10=Exit     Enter=Do
```

**Step 4** After configuring the IP address, press **Enter**. The configuration is complete.

----End

### 3.8.1.2.6 Configuring an IP Address for the Service Network Port on the Application Server (HP-UX)

The service network port can receive and send data only after a proper IP address is configured for it.

#### Context

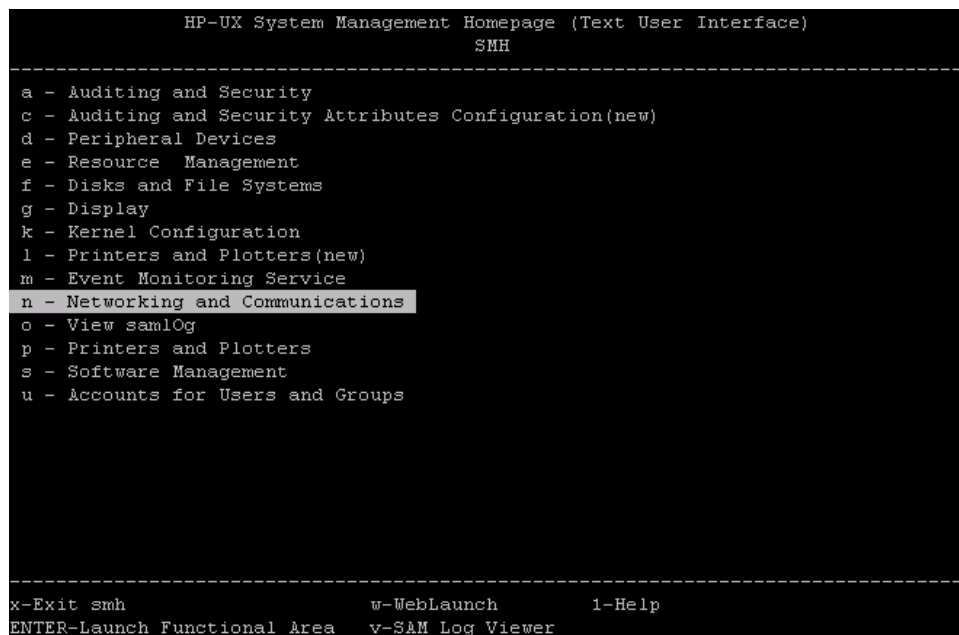
Configure an IP address for a service network port on the application server using the SAM method.

#### Procedure

- Step 1** Log in to the HP-UX-based application server as user **root**.
- Step 2** Run the **sam** command to go to the SAM configuration page. Click **Networking and Communications** to go to the network configuration page, as shown in [Figure 3-12](#).

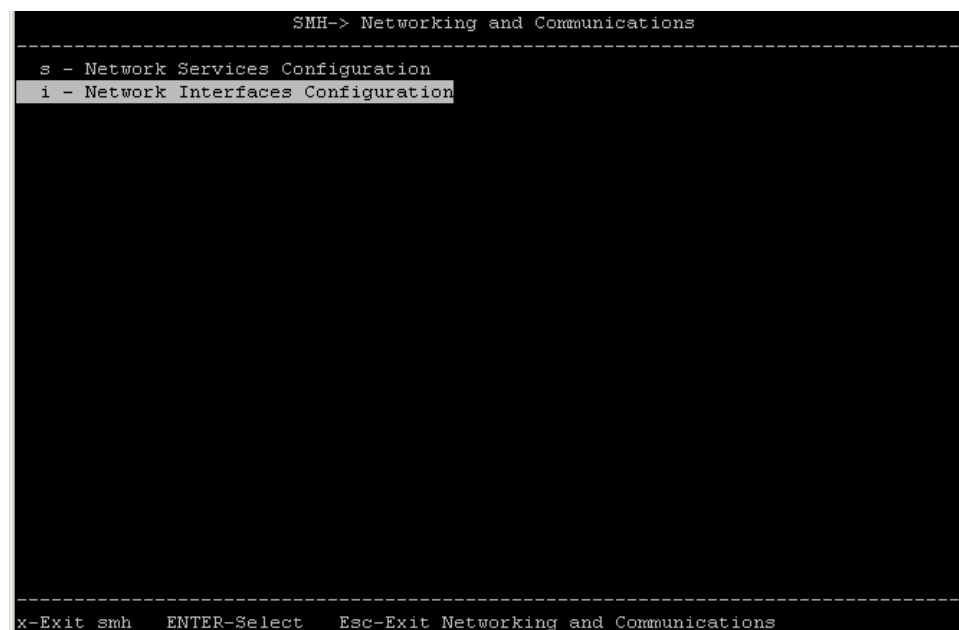


Figure 3-12 Page for selecting SAM functions



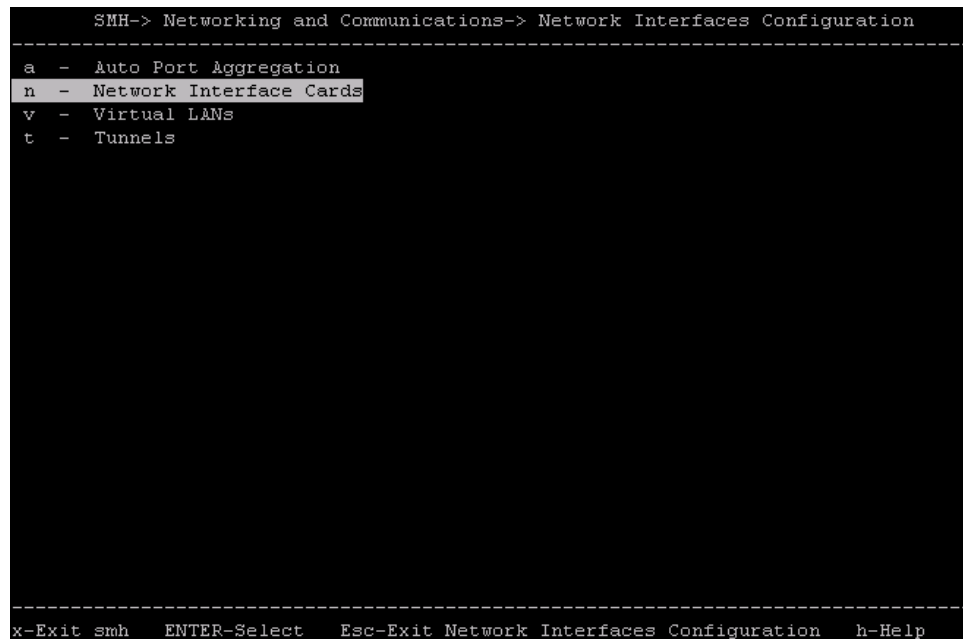
Step 3 Select Network Interfaces Configuration, as shown in Figure 3-13.

Figure 3-13 Network communication menu



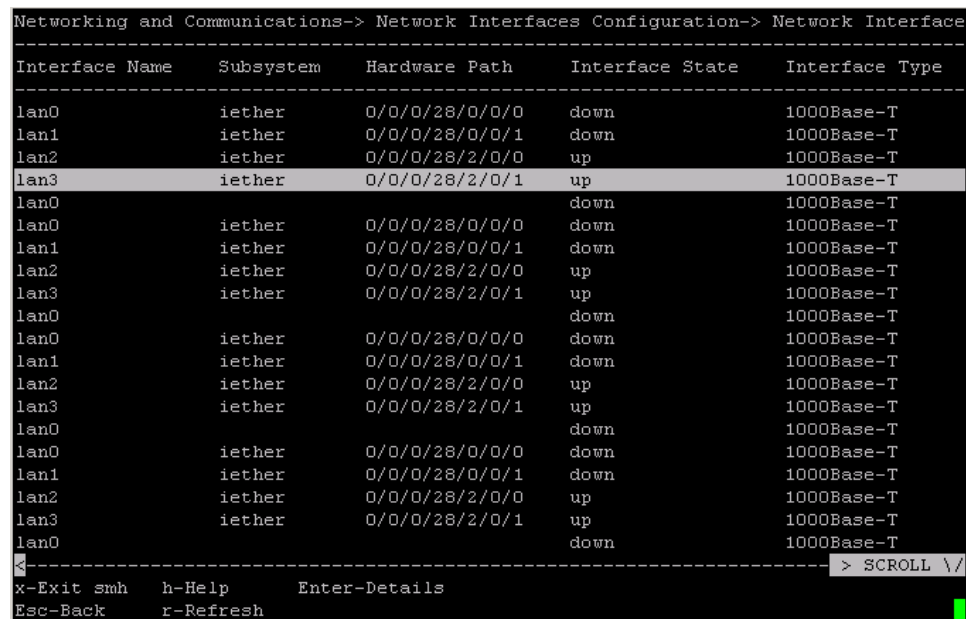
Step 4 Select Network Interface Cards, as shown in Figure 3-14.

**Figure 3-14** Network interface configuration menu



**Step 5** Select a desired port, as shown in [Figure 3-15](#).

**Figure 3-15** Network interface card configuration menu



**Step 6** The configuration page shown in [Figure 3-16](#) is displayed. Enter **p** to go to the network port configuration editing page, as shown in [Figure 3-17](#).

Figure 3-16 Network port configuration details

```
orking and Communications-> Network Interfaces Configuration-> Network Interface Card
-----
Details of Interface: lan3
-----
Group Name          NIC Attributes
MAC Address         0x9C8E9936B61F
MTU                 1500

Link Information
-----
Link State          Up
Speed              1 Gbps Full Duplex (Autonegotiation : On)

IPv4 Attributes
-----
IPv4 Address        -
IPv4 Status         Not Configured
Subnet Mask         -
Broadcast Address   -
Alias               -
Comments           -

-----SCROLL \ /
x-Exit smh    h-Help          p-View/Modify IP Attributes
Esc-Back     v-Add VLAN    a-View/Modify NIC Attributes
```

Figure 3-17 Network port configuration page

```
SMH-> Networking and Communications-> Network Interface Cards-> Modify IP Attributes
-----
* Required field

Interface Name      : lan3
Hardware Path       : 0/0/0/28/2/0/1

Encapsulation Type  : Ethernet ->

[ ] IPv4 Attributes (Select to enable)

IPv4                : (X) Enable IPv4
                   : ( ) Disable IPv4

* IPv4 Address      : _____
Subnet Mask         : _____
Broadcast Address   : _____
[X] Add entry to /etc/hosts file
* Hostname          : root_____
Comments           : _____
Enable DHCP client  : [ ]

-----SCROLL \ /
```

**Step 7** Enter an IP address.

In **IPv4 Address**, enter the IP address. In **Subnet Mask**, enter the subnet mask. In **Broadcast Address**, enter the broadcast address.

 **NOTE**

- The broadcast address is an address used to concurrently send broadcast messages to all workstations on a network. On a network that uses the TCP or IP protocol, the IP addresses with host IDs all being binary 1s are broadcast addresses. For example, on the 192.168.1.0/24 network segment, the broadcast address is 192.168.1.255 (11111111 in binary). When a message (packet encapsulated) whose target address is 192.168.1.255 is sent, the message will be sent to all computers on the network segment.
- If you want to configure a gateway, choose **Network Services Configuration > Router** in [Step 3](#) and configure the gateway information as prompted.

----End

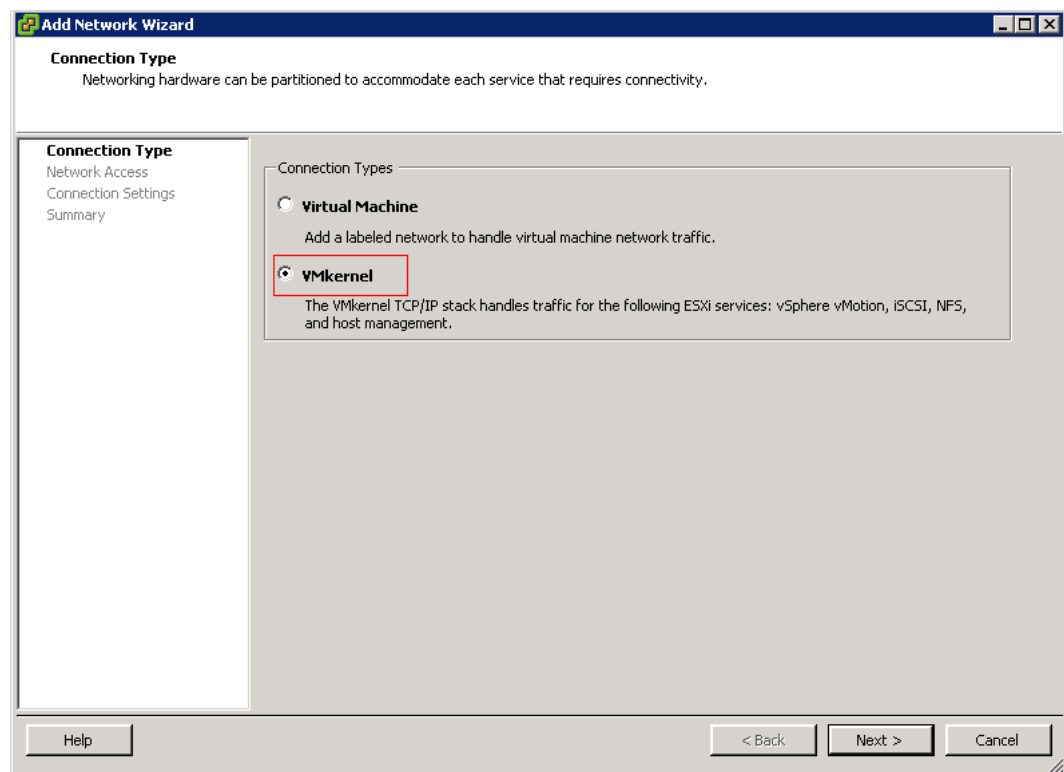
### 3.8.1.2.7 Configuring an IP Address for the Service Network Port on the Application Server (VMware)

When the application server connects to a storage system through iSCSI, you must configure the IP address of the service network port on the application server and the IP address of the iSCSI host port on the storage system on the same network segment. You can add a virtual network to the VMware host system to configure the service IP address. This section describes how to configure the IP address for a VMware service network port.

#### Procedure

- Step 1** Log in to the vSphere client as user **administrator**.
- Step 2** On the vSphere client, click the **Configuration** tab and choose **Networking > Add Networking...** The **Add Network Wizard** dialog box is displayed.
- Step 3** Select **VMkernel**, as shown in [Figure 3-18](#).

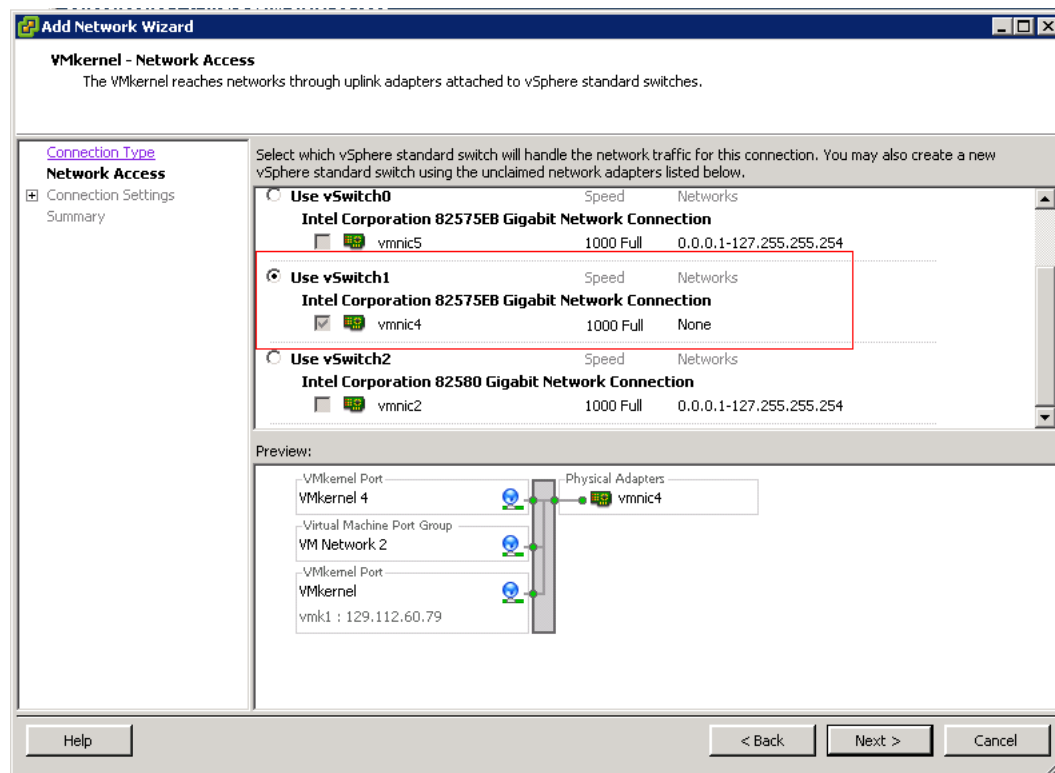
**Figure 3-18** Selecting VMkernel



**Step 4** Click **Next**. The page for selecting a vSphere standard switch is displayed.

**Step 5** Select a standard switch that you want to connect to the storage system, as shown in **Figure 3-19**.

**Figure 3-19** Selecting a vSphere standard switch



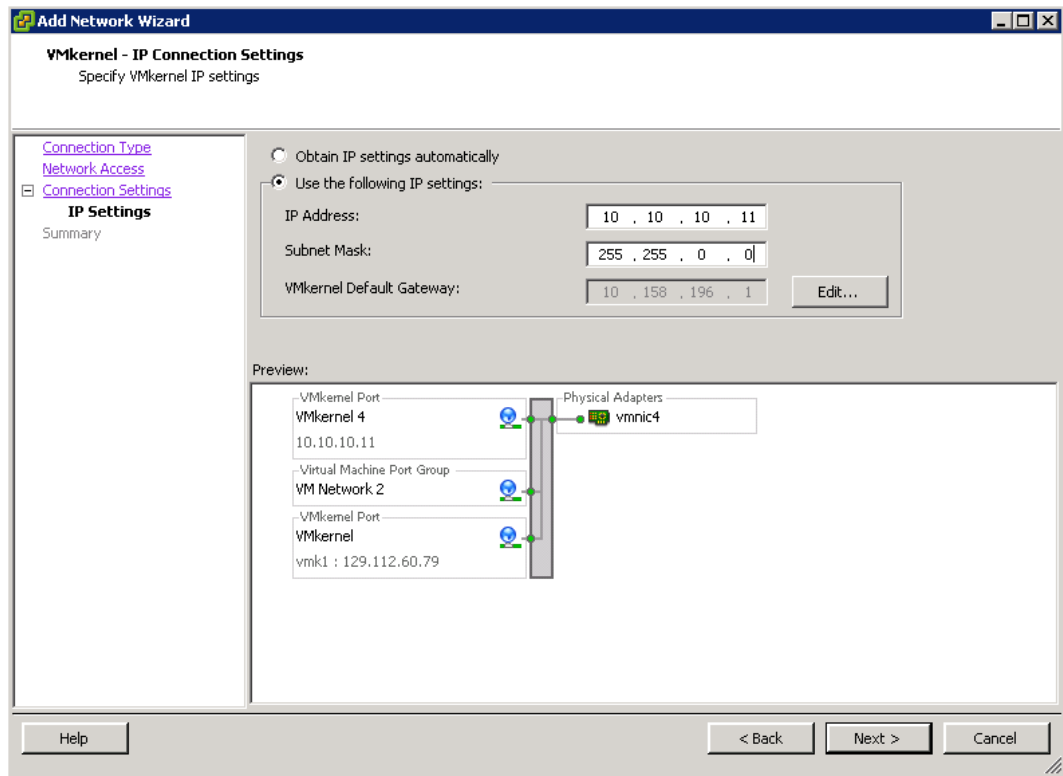
**Step 6** Click **Next** and configure a network label.

**Step 7** Click **Next**. The page for setting an IP address is displayed.

**Step 8** Configure an IP address for the service network port, as shown in **Figure 3-20**.

You must configure the service network port IP address and the iSCSI host port IP address on the same network segment. By doing so, the storage system can properly communicate with the application server.

**Figure 3-20** Configuring an IP address for the service network port



**Step 9** Click **Next** to confirm the configuration.

**Step 10** Click **Finish**.

**NOTE**

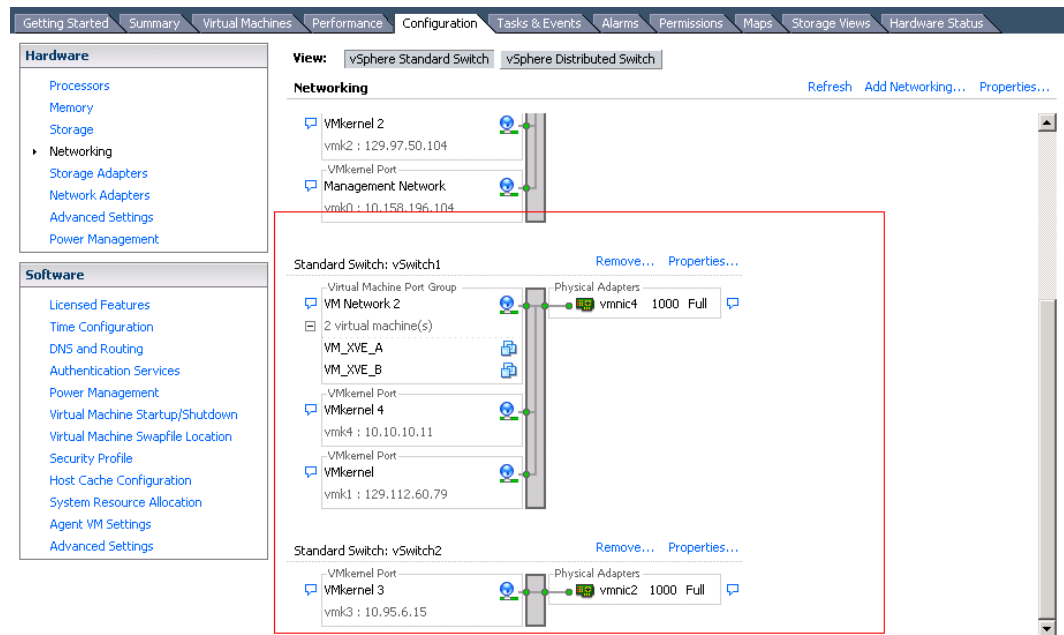
- After completing the configuration, you can run **ifconfig** to check whether the IP address of the application server is correct.
- If you want to create multiple virtual networks, repeat the preceding operations.

----End

## Follow-up Procedure

Choose **Configuration > Networking**. In the **Networking** area, check the virtual network that has been configured, as shown in **Figure 3-21**.

**Figure 3-21** Checking the virtual network configuration



### 3.8.1.3 Configuring an Initiator

A storage system cannot communicate with an application server if you only physically connect one of its Ethernet ports to a service network port on the application server using a network cable. You must configure an initiator on the application server to establish a logical connection between the application server and storage system.

#### Prerequisites

- The IP address of the Ethernet port connected to the application server is obtained.

**NOTE**

For details about how to query the IP address of an Ethernet port, see the *Administrator Guide* of the corresponding product model.

- Port 3260 is enabled.

Before connecting an application server to a storage system, enable port 3260 used by the TCP/IP network on which the iSCSI protocol is transported.

- When a firewall device is working between the storage system and the application server, ensure that port 3260 is enabled on the firewall device.
- When firewall software is running on the application server, ensure that port 3260 is enabled by the firewall software.

#### Context

You can configure iSCSI connections in either of the following modes:

- Direct connection

The Ethernet port on the storage system is directly connected to the service network port on the application server. This is the basic connection mode.

- Network connection

The Ethernet port on the storage system is connected to the service network port on the application server through an IP network (LAN or routed network).

For an iSCSI connection, the application server functions as an initiator that sends iSCSI program requests from the application server to the storage system. The storage system functions as a target that receives and responds to the iSCSI program requests from the application server. The IP addresses of an initiator and a target are unique. The two IP addresses are used to set up a communication channel between the storage system and application server.

### 3.8.1.3.1 Configuring an Initiator (Windows)

This section describes how to configure an initiator on an application server running Windows.

#### Prerequisite

- iSCSI software

- For Windows Server 2008 and later versions, iSCSI initiator is delivered with the system. You can open the iSCSI software in **Administrative Tools**.

 **NOTE**

- If you use the multipathing software delivered with Windows, you must add the **Multipath I/O** function to **Server Manager**.
- If you use UltraPath, see your UltraPath document.
- For Windows Server 2003 and earlier versions, the installation package specific to your operating system version is downloaded.

You can download the **Microsoft iSCSI Initiator** installation package from Microsoft website.

The version of **Microsoft iSCSI Initiator** must be 2.01 or later. If the UltraPath software is used, **Microsoft iSCSI Initiator** 2.08 is recommended.

 **NOTE**

- If you use the multipathing software delivered with Windows, select **Microsoft MPIO Multipathing Support for iSCSI** when installing the iSCSI software.
- If you use UltraPath, see your UltraPath document.
- The service network port on the application server is communicating properly with the iSCSI host port on the storage system. You can perform the following operation to check whether the communication is normal:

On the application server, run the **ping ip** command, where *ip* indicates the IP address of the iSCSI host port connected to the application server. If the application server receives the data packets sent from the iSCSI host port, the communication between the application server and storage system is normal. If the application server fails to receive the data packets, use either of the following methods to ensure normal communication:

- Configure the IP addresses of the iSCSI host port and service network port onto the same network segment.
- If the two IP addresses are on different network segments, add a route to establish a connection between them.



## Windows Server 2003 and Earlier Versions

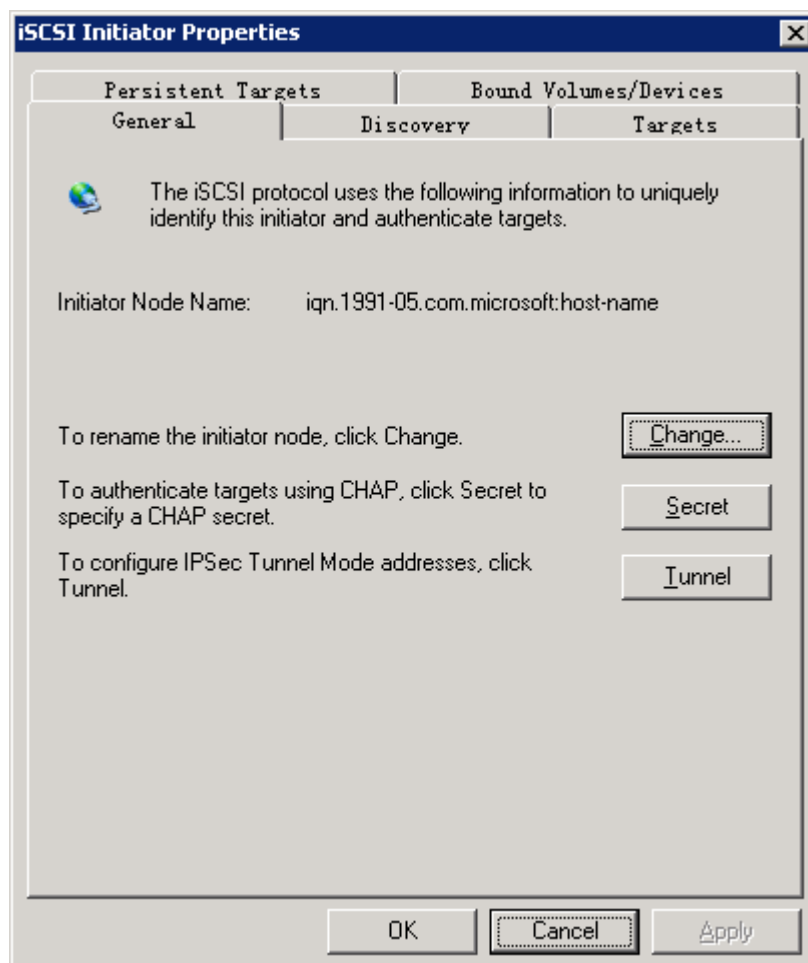
Windows Server 2003 and earlier versions use the same method to configure an iSCSI initiator. This section uses Windows Server 2003 as an example to describe how to configure an iSCSI initiator.

**Step 1** Log in to the Windows-based application server as **administrator**.

**Step 2** Double-click the shortcut icon of Microsoft iSCSI Initiator on the desktop of the application server.

The **iSCSI Initiator Properties** dialog box is displayed, as shown in [Figure 3-22](#).

**Figure 3-22** iSCSI Initiator Properties dialog box



### NOTE

If a target has been logged in to, log out of the target as follows:

1. Click the **Targets** tab. In the **Targets** area, select the target that has been logged in to and click **Details**. The **Target Properties** dialog box is displayed.
2. On the **Sessions** tab page, select the target in the **Identifier** area and click **Log off**.

**Step 3 Optional:** Change the name of the initiator.

When multiple application servers are connected to the storage system, you are advised to change the names of initiators to quickly locate the desired initiator. The name of an initiator

must be unique. Otherwise, the connection between the storage system and the application server fails.

1. On the **General** tab page of the **iSCSI Initiator Properties** dialog box, click **Change**. The **Initiator Node Name Change** dialog box is displayed.
2. In the **Initiator node name**, enter a new name for the initiator.

 **NOTE**

The name can contain only letters, digits, periods (.), hyphens (-), and colons (:) and must not start with a hyphen (-). If an initiator name contains illegal characters, the application server cannot connect to the storage system.

3. Click **OK**.  
The **Initiator Node Name Change** dialog box is closed.

**Step 4** Configure the IP address of the target.

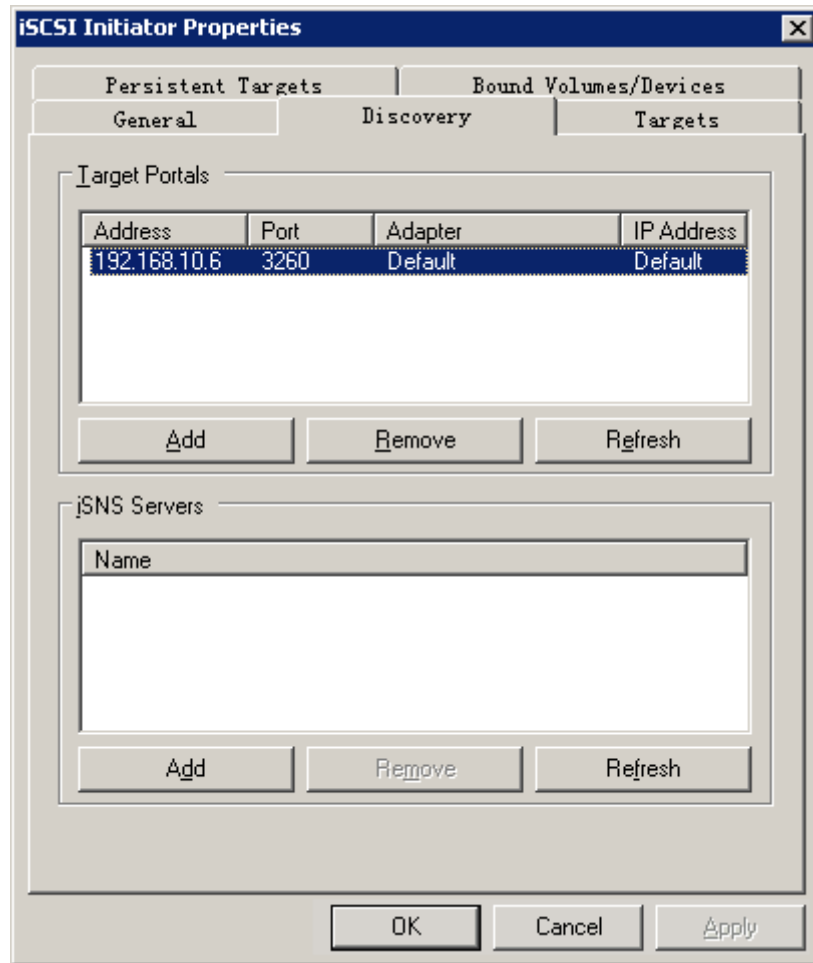
1. In the **iSCSI Initiator Properties** dialog box, click the **Discovery** tab.
2. In the **Target Portals** area, click **Add**. The **Add Target Portal** dialog box is displayed.
3. In **IP address or DNS name**, enter the IP address of the iSCSI host port connected to the application server.
4. In **Port**, enter an available port number for iSCSI connection.

The default port number is **3260**.

5. Click **OK**.

You have finished configuring the IP address of the target. The newly added target port is displayed in the **Target Portals** area, as shown in [Figure 3-23](#).

**Figure 3-23** Viewing the discovered target port

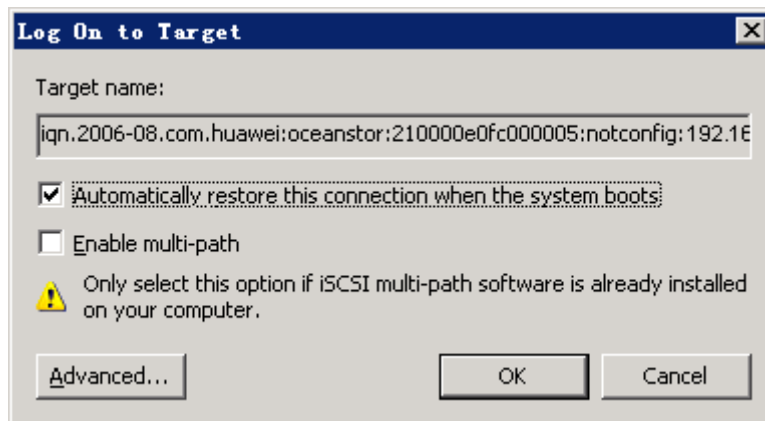


**Step 5** Log in to the target.

1. In the **iSCSI Initiator Properties** dialog box, click the **Targets** tab.
2. In the **Targets** area, select the target to be connected to (**Status** is **Inactive**) and click **Log On**.

The **Log On to Target** dialog box is displayed, as shown in [Figure 3-24](#).

**Figure 3-24** Log On to Target dialog box



3. In the **Log On to Target** dialog box, select **Automatically restore this connection when the system boots**.
  - If this check box is selected, the application server can constantly access the storage system through the target port.
  - If this check box is not selected, you must establish the iSCSI connection again using this target port after the application server restarts.
4. Configure the multipathing policy.
  - Do not select **Enable multi-path** if UltraPath is installed on the application server because UltraPath will conflict with the multipathing software provided by Microsoft iSCSI Initiator.
  - If no multipathing software is installed on the application server, select **Enable multi-path** and perform the following steps:
    - i. Click **Advanced...**. The **Advanced Settings** dialog box is displayed.
    - ii. From the **Local adapter** list, select **Microsoft iSCSI Initiator**.
    - iii. From the **Source IP** list, select the IP address of the application server.
    - iv. From the **Target Portal** list, select the IP address of the iSCSI host port connected to the application server.
    - v. Click **OK** to return to the **Log On to Target** dialog box.
    - vi. Click **OK** to return to the **iSCSI Initiator Properties** dialog box.

**Step 6** Click **OK**.

You have finished configuring the initiator.

 **NOTE**

If the login fails, CHAP authentication may be enabled on the storage system for the initiator. Set a CHAP user name and password on the application server.

---End

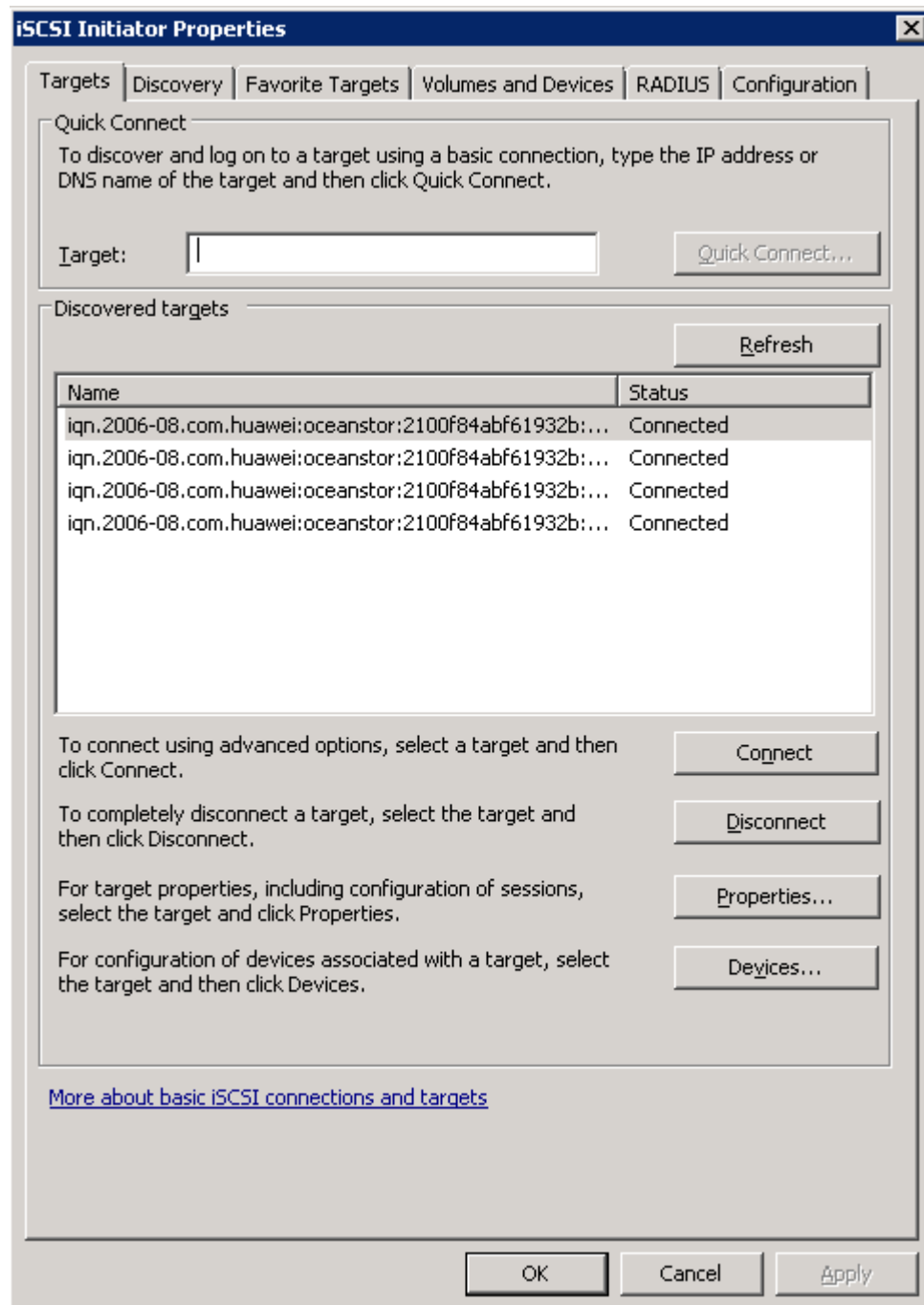
## Windows Server 2008 and Later Versions

Windows Server 2008 and later versions use the same method to configure an iSCSI initiator. This section uses Windows Server 2008 as an example to describe how to configure an iSCSI initiator.

- Step 1** Log in to the Windows-based application server as **administrator**.
- Step 2** Choose **Start > All Programs** and run **iSCSI Initiator**.

The **iSCSI Initiator Properties** dialog box is displayed, as shown in **Figure 3-25**.

**Figure 3-25 iSCSI Initiator Properties dialog box**



 **NOTE**

If a target has been logged in to, log out of the target as follows:

1. Click the **Targets** tab. In the **Discovered targets** area, select the target that has been logged in to.
2. Click **Disconnect**, and the status of the target will become **Inactive**.
3. Click the **Discovery** tab. In the **Target Portals** area, select the target that has been disconnected and click **Remove**.

**Step 3 Optional:** Rename the initiator.

When multiple application servers are connected to the storage system, you are advised to change the names of initiators to quickly locate the desired initiator. The name of an initiator must be unique. Otherwise, the connection between the storage system and the application server fails.

1. On the **Configuration** tab page of the **iSCSI Initiator Properties** dialog box, click **Change**. The **iSCSI Initiator Name** dialog box is displayed.
2. In **New initiator name**, enter a new initiator name.

 **NOTE**

The name can contain only letters, digits, periods (.), hyphens (-), and colons (:) and must not start with a hyphen (-). If an initiator name contains illegal characters, the application server will be unable to connect to the storage system.

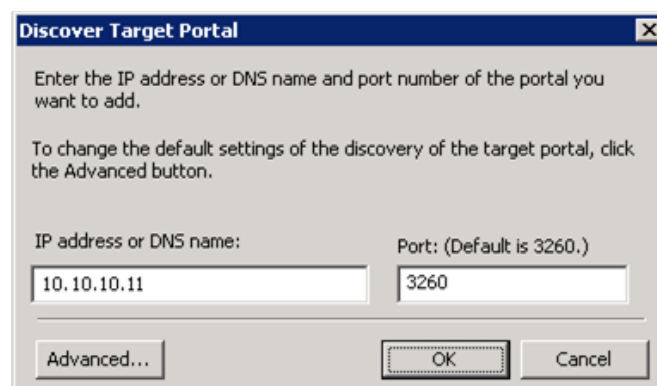
3. Click **OK**.  
The the **iSCSI Initiator Name** dialog box is closed.

**Step 4** Configure the IP address of the target.

1. In the **iSCSI Initiator Properties** dialog box, click the **Discovery** tab.
2. In the **Target Portals** area, click **Discover Portal...** The **Discover Target Portal** dialog box is displayed.
3. In **IP address or DNS name**, enter the IP address of the iSCSI host port connected to the application server.
4. In **Port**, enter an available port number for iSCSI connection.

The default port number is **3260**.

**Figure 3-26 Discover Target Portal** dialog box



5. Click **OK**.

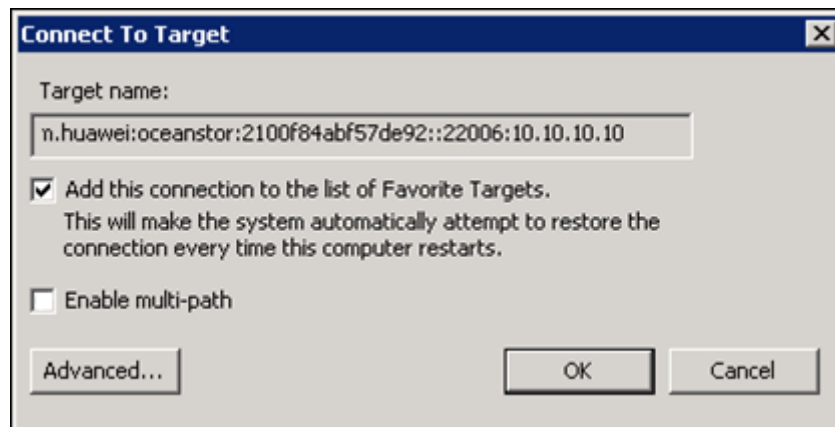
You have finished configuring the IP address of the target. The newly added target port is displayed in the **Target Portals** area.

**Step 5** Log in to the target.

1. In the **iSCSI Initiator Properties** dialog box, click the **Targets** tab.
2. In the **Discovered targets** area, select the desired target (the value of **Status** is **Inactive**) and click **Connect**.

The **Connect To Target** dialog box is displayed, as shown in [Figure 3-27](#).

**Figure 3-27** Connect To Target dialog box



3. In the **Connect To Target** dialog box, select **Add this connection to the list of Favorite Targets**.
  - If this check box is selected, the application server can constantly access the storage system through the target port.
  - If this check box is not selected, you must establish the iSCSI connection again using this target port after the application server restarts.
4. Configure the multipathing policy.
  - Do not select **Enable multi-path** if UltraPath is installed on the application server because UltraPath will conflict with the multipathing software provided by Microsoft iSCSI Initiator.
  - If no multipathing software is installed on the application server, select **Enable multi-path** and perform the following steps:
    - i. Click **Advanced...**. The **Advanced Settings** dialog box is displayed.
    - ii. From the **Local adapter** list, select **Microsoft iSCSI Initiator**.
    - iii. From the **Initiator IP** list, select the IP address of the application server.
    - iv. From the **Target Portal** list, select the IP address of the iSCSI host port connected to the application server.
    - v. Click **OK** to return to the **Connect To Target** dialog box.
    - vi. Click **OK** to return to the **iSCSI Initiator Properties** dialog box.

**Step 6** Click **OK**.

The initiator configuration is complete.

 **NOTE**

If the login fails, CHAP authentication may be enabled on the storage system for the initiator. In this case, set the CHAP user name and password on the application server.

----End

### 3.8.1.3.2 Configuring an Initiator (SUSE)

This section describes how to configure an initiator on an application server running SUSE 10 and later versions.

#### Prerequisites

The service network port on the application server is communicating properly with the service host port on the storage system.

On the application server, run the **ping ip** command, where *ip* indicates the IP address of the service host port connected to the application server. If the application server receives the data packets sent from the service host port, the communication between the application server and storage system is normal. If the application server fails to receive the data packets, use either of the following methods to ensure normal communication:

- Configure the IP addresses of the service host port and service network port onto the same network segment.
- If the two IP addresses are on different network segments, add a route to establish a connection between them.

#### Context

For SUSE 10 and later versions, the iSCSI installation program is **open-iscsi**.

#### Procedure

**Step 1** Log in to the application server as user **root**.

**Step 2** Run the **rpm -qa | grep iscsi** command to check whether an iSCSI initiator **open-iscsi** is installed.

- If not installed, go to **Step 3**.
- If installed, go to **Step 5**.

**Step 3** Upload the iSCSI installation program to a specified directory such as **/opt**.

**Step 4** Run the **cd** command to go to the directory of the iSCSI installation program and run the **rpm -ivh package\_name** command to install the iSCSI program. *package\_name* indicates the full name of the iSCSI program.

 **NOTE**

The iSCSI installation program must be an executable software package. Otherwise, run the **tar** command to decompress the program.

**Step 5** Start the iSCSI service.

Run the **chkconfig open-iscsi on** command to set the startup mode of the iSCSI service to automatic startup. Then run the **/etc/init.d/open-iscsi status** command to check the startup status of the iSCSI service.



### Step 6 Optional: Change the name of the initiator.

When multiple application servers are connected to the storage system, you are advised to change the names of initiators to quickly locate the desired initiator. The name of an initiator must be unique. Otherwise, the connection between the storage system and the application server fails.

This section uses SUSE 10 as an example to describe how to rename an initiator.

1. Run the **vi /etc/iscsi/initiatorname.iscsi** command to open the **initiatorname.iscsi** file.

The following output is displayed.

```
## /etc/iscsi/iscsi.initiatorname
##
## Default iSCSI Initiatorname.
##
## DO NOT EDIT OR REMOVE THIS FILE!
## If you remove this file, the iSCSI daemon will not start.
## If you change the InitiatorName, existing access control lists
## may reject this initiator. The InitiatorName must be unique
## for each iSCSI initiator. Do NOT duplicate iSCSI InitiatorNames.
InitiatorName=iqn.1996-04.de.SUSE:01:a086b6aa34b7
~
"/etc/iscsi/initiatorname.iscsi" 11L, 422C          1, 1
All
```

2. Press **i** to enter the editing mode and then edit the **initiatorname.iscsi** file.
3. Enter a new initiator name after **InitiatorName=**.
4. Press **Esc** to exit the editing mode.
5. Run the **:wq** command and press **Enter** to save the changes and close the **initiatorname.iscsi** file.

### Step 7 Configure the IP address of the target and log in to the target.

#### NOTE

The IP address of the target is actually the IP address of the service host port connected to the application server.

1. Run the **iscsiadm -m discovery -t st -p IP** command to discover the target. *IP* indicates the service port IP address of the storage system.

```
# iscsiadm -m discovery -t st -p 192.168.10.6
```

#### NOTE

If the storage system is connected to an application server using multiple service ports, run the command for the IP address of each service port.

2. Run the **iscsiadm -m node -l** command to log in to the target.

#### NOTE

To log in to a certain target, run **iscsiadm -m node -p ipaddress -l**, where *ipaddress* indicates the IP address of the target.

3. Run the **vi** command to edit the **/etc/iscsi/iscsid.conf** file. Enable the iSCSI service to be automatically connected after the application server is restarted.

In **Startup settings**, set **node.startup** to **automatic**.

```
node.startup=automatic
```

4. **Optional:** Set the multipathing mode. If UltraPath is installed on the application server, you must set **node.session.timeo.replacement\_timeout=1** in the **/etc/iscsi/iscsid.conf** file.

The following information is displayed:

```
node.session.timeo.replacement_timeout=1
```

**Step 8** After the target is configured, run the `/etc/init.d/open-iscsi restart` command to restart the iSCSI service to enable the configuration to take effect.

----End

## Result

After performing the operations, run the `iscsiadm -m node` command to check the target that you have logged in to.

### 3.8.1.3.3 Configuring an Initiator (Red Hat)

This section describes how to configure an initiator on an application server running Red Hat.

## Prerequisites

The service network port on the application server is communicating properly with the Ethernet port on the storage system. On the application server, run the `ping ip` command, where `ip` indicates the IP address of the Ethernet port connected to the application server. If the application server receives the data packets sent from the Ethernet port, the communication between the application server and storage system is normal. If the application server fails to receive the data packets, use either of the following methods to ensure normal communication:

- Configure the IP addresses of the Ethernet port and service network port onto the same network segment.
- If the two IP addresses are on different network segments, add a route to establish a connection between them.

## Context

The method used to configure the iSCSI service varies according to different Red Hat versions.

- Red Hat Linux AS4  
Edit the `/etc/iscsi.conf` file to configure the iSCSI service.
- Red Hat Linux AS5 and later versions  
Run the `iscsiadm` command to configure the iSCSI service.

## Procedure

**Step 1** Log in to the Red Hat application server as user `root`.

**Step 2** Run the `rpm -qa | grep iscsi` command to check whether an iSCSI initiator is installed on the Red Hat-based application server.

- If not installed, go to [Step 3](#).
- If installed, go to [Step 5](#).

**Step 3** Upload the iSCSI installation program to a specified directory such as `/opt`.

**Step 4** Run the `cd` command to go to the directory of the iSCSI installation program and run the `rpm -ivh package_name` command to install the iSCSI program. `package_name` indicates the full name of the iSCSI program.

 **NOTE**

The iSCSI installation program must be an executable software package. Otherwise, run the **tar** command to decompress the program.

**Step 5** Run the **chkconfig iscsi on** command to set the startup mode of the iSCSI service to automatic startup. Then run the **/etc/init.d/iscsi status** command to check the startup status of the iSCSI service.

**Step 6 Optional:** Rename the initiator.

When multiple application servers are connected to the storage system, you are advised to change the names of initiators to quickly locate the desired initiator. The name of an initiator must be unique. Otherwise, the connection between the storage system and the application server fails. The method used to rename an initiator is the same in different RedHat versions. The only difference lies in the file that is edited.

- Red Hat Linux AS4  
Edit the **/etc/initiatorname.iscsi** file to rename the initiator.
- Red Hat Linux AS5 and later versions  
Edit the **/etc/iscsi/initiatorname.iscsi** file to rename the initiator.

This section uses Red Hat Linux 5.8 as an example to describe how to rename an initiator.

1. Run the **vi /etc/iscsi/initiatorname.iscsi** command in the root directory to open the **initiatorname.iscsi** file.
2. Press **i** to enter the editing mode and then edit the **initiatorname.iscsi** file.  
Enter a new initiator name after **InitiatorName=**.

For example, change the initiator name to **iqn.2005-03.com.RedHat:01.219d22e88e9c**.  
The following output is displayed after the change is made:  

```
InitiatorName=iqn.2005-03.com.RedHat:01.219d22e88e9c
```

3. Press **Esc** to exit the editing mode.
4. Run the **:wq** command and press **Enter** to save the changes and close the **initiatorname.iscsi** file.

**Step 7** Configure the IP address of the target and log in to the target.

 **NOTE**

The IP address of the target is actually the IP address of the service host port connected to the application server.

- Red Hat Linux AS4
  - a. Run the **vi /etc/iscsi.conf** command to open the **iscsi.conf** file.
  - b. Press **i** to enter the editing mode and then edit the **iscsi.conf** file.
  - c. Enter the IP address of the iSCSI host port connected to the application server in the **iscsi.conf** file.

For example, if the IP address of the iSCSI host port is **192.168.10.6**, enter the following information:

```
DiscoveryAddress=192.168.10.6
```

 **NOTE**

In the **iscsi.conf** file, the comment character (**#**) before **DiscoveryAddress** indicates that this row is a comment. Delete the sign in initial configuration.

- d. **Optional:** Set the multipathing mode. If UltraPath is installed on the application server, you must set **Multipath=portal** and **ConnfailTimeout=1** in the **iscsi.conf** file.

The following information is displayed:

```
Multipath=portal
ConnfailTimeout=1
DiscoveryAddress=192.168.10.6
```

- e. Press **Esc** to exit the editing mode. Run the **:wq** command and press **Enter** to exit the **iscsi.conf** file.

- Red Hat Linux AS5 and later versions

- a. Run the **iscsiadm -m discovery -t st -p IP** command to discover the target. *IP* indicates the service port IP address of the storage system.

```
# iscsiadm -m discovery -t st -p 192.168.10.6
```

- b. Run the **iscsiadm -m node -l** command to log in to the target.

 **NOTE**

To log in to a certain target, run **iscsiadm -m node -p ipaddress -l**, where *ipaddress* indicates the IP address of the target.

- c. Run the **vi** command to edit the **/etc/iscsi/iscsid.conf** file. Enable the iSCSI service to be automatically connected after the application server is restarted.

In **Startup Setting**, set **node.startup** to **automatic**.

```
node.startup=automatic
```

- d. **Optional:** Set the multipathing mode. If UltraPath is installed on the application server, you must set **node.session.timeo.replacement\_timeout=1**.

The following information is displayed:

```
node.session.timeo.replacement_timeout=1
```

**Step 8** Run the **/etc/init.d/iscsi restart** command to restart the iSCSI service and make the settings take effect.

----End

## Result

After performing the operations, check the target that you have logged in to.

- Red Hat Linux AS4  
Run the **iscsi-ls** command to check the target.
- Red Hat Linux AS5 and later versions  
Run the **iscsiadm -m node** command to check the target.

### 3.8.1.3.4 Configuring an Initiator (Solaris)

This section describes how to configure an initiator on an application server running Solaris.

## Prerequisites

- The service network port on the application server is communicating properly with the Ethernet port on the storage system.  
On the application server, run the **ping ip** command, where *ip* indicates the IP address of the Ethernet port connected to the application server. If the application server receives the data packets sent from the Ethernet port, the communication between the application

server and storage system is normal. If the application server fails to receive the data packets, use either of the following methods to ensure normal communication:

- Configure the IP addresses of the Ethernet port and service network port onto the same network segment.
- If the two IP addresses are on different network segments, add a route to establish a connection between them.
- The operating system running on the application server must be Solaris 10 1/06 or a later version. Otherwise, the iSCSI protocol is not supported.

Run the **cat /etc/release** command to check the version of the Solaris operating system running on the application server.

## Procedure

**Step 1** Log in to the application server as user **root**.

**Step 2** Run the **pkginfo | grep iscsi** command to check whether the iSCSI initiator is installed.

- If not installed, go to **Step 3**.
- If installed, go to **Step 4**.

**Step 3** Insert the operating system installation CD-ROM into the server's CD-ROM drive. Run the **pkgadd** command to install the iSCSI software.

```
# pkgadd -d /cdrom/Solaris_10/Product SUNWiscsir
```

**Step 4** Run the **svcs -a | grep iscsi** command to check whether the iSCSI service is enabled on the application server. If the iSCSI service is disabled, run the **svcadm enable iscsitgt** command to enable it.

**Step 5 Optional:** Change the name of the initiator.

When multiple application servers are connected to the storage system, you are advised to change the names of initiators to quickly locate the desired initiator. The name of an initiator must be unique. Otherwise, the connection between the storage system and the application server fails.

1. Run the **vi /etc/iscsi/initiatorname.iscsi** command in the root directory to open the **initiatorname.iscsi** file.
2. Press **i** to enter the editing mode and then edit the **initiatorname.iscsi** file.  
Enter a new initiator name after **InitiatorName=**.

For example, change the initiator name to **initiator01**. The following output is displayed after the change is made:

```
InitiatorName=initiator01
```

3. Press **Esc** to exit the editing mode.
4. Run the **:wq** command and press **Enter** to save the changes and close the **initiatorname.iscsi** file.

**Step 6** Configure the IP address of the target and log in to the target.

### NOTE

The IP address of the target is actually the IP address of the Ethernet port connected to the application server.

Run the following command to configure the IP address of the target.

```
# iscsiadm add discovery-address 192.168.10.6:3260
```

In this example, the IP address of the target is *192.168.10.6* and the port number is *3260*.

After configuring the IP address of the target, run the **iscsiadm list discovery-address -v** command to verify that the IP address of the target is correctly configured. If the following output is displayed, the IP address of the target is successfully configured.

```
# Discovery Address:192.168.10.6:3260
      Target name: iqn.2006-08.com.huawei:OceanStor:
210000e0fc000005::192.168.10.6
Target address      :192.168.10.6:3260,13
```

### Step 7 Enable the target discovery mode.

Solaris supports two target discovery modes: dynamic target discovery and static target discovery.

- Dynamic target discovery mode

There are two dynamic target discovery modes: SendTargets and Internet Storage Name Service (iSNS).

- SendTargets dynamic discovery

If iSCSI nodes connect to a large number of targets, the storage system provides the mapping relationship between iSCSI node IP addresses and port numbers and allows the iSCSI initiator to use the SendTargets function to search for targets.

```
# iscsiadm modify discovery --sendtargets enable
```

- iSNS dynamic discovery

iSNS allows the iSCSI initiator to search for accessible targets and to limit the number of accessible targets. It also provides the status change notification function to notify the iSCSI initiator of the status change of a storage node. To enable the iSNS dynamic discovery mode, the storage system must provide the mapping relationship between iSNS server IP addresses and port numbers and allow the iSCSI initiator to search for specified iSNS servers. The default port number of the iSNS server is 3205.

```
# iscsiadm modify discovery --isns enable
```

- Static target discovery mode

If an iSCSI node has a small number of targets or the target that the initiator attempts to access is restricted, you can configure **target-name** in static mode based on the naming conventions of static target addresses.



Do not use static and dynamic discovery modes at the same time. Otherwise, the storage system performance may deteriorate when communicating with an iSCSI target.

---

Run the following command to enable the static target discovery mode:

```
# iscsiadm modify discovery --static enable
```

 **NOTE**

Run the **iscsiadm list discovery** command to query the current discovery mode.

**Step 8** Run the **devfsadm -i iscsi** command to set up an iSCSI connection between the application server and storage system.

**Step 9** Configure the multipathing software.

Solaris supports UltraPath (developed by Huawei) and StorEdge Traffic Manager Software (STMS, delivered with the Solaris host system). STMS is used as an example to describe how to configure the multipathing software. For details about how to install and configure UltraPath, see the user guide specific to your product.

- Solaris 10

The method used to enable the multipathing software on the host system varies according to different asymmetrical logical unit access (ALUA) modes (enabled or disabled).

- ALUA is enabled.

After ALUA is enabled on the storage system, you do not need to configure the host system. Run the **stmsboot -D fp -e** command.

```
# stmsboot -D fp -e  
  
WARNING: This operation will require a reboot.  
  
Do you want to continue ? [y/n] (default: y) y  
  
The changes will come into effect after rebooting the system.  
  
Reboot the system now ? [y/n] (default: y) y  
  
updating /platform/sun4u/boot_archive
```



## NOTICE

After the preceding command is executed, the operating system will restart.

---

- ALUA is disabled.

If ALUA is disabled on the storage system, you must modify the configuration file on the host system. In this way, the multipathing software can take over the LUNs mapped by the storage system.

- i. Run the **format** command, select a mapped disk, and click **inquiry** to query **Vendor ID** and **Product ID** of the LUN.

- ii. Modify the **/kernel/drv/scsi\_vhci.conf** configuration file and add **Vendor ID** and **Product ID** of the LUN to the configuration file. For example, if **Vendor ID** is **HUAWEI** and **Product ID** is **XXXXXX**, configure the file as follows:

```
device-type-scsi-options-list =  
  
"HUAWEI XXXXXX", "symmetric-option";
```

- iii. Run the **stmsboot -D fp -e** command to activate the STMS function. The STMS takes effect after the operating system restarts.

- Solaris 11

The method used to enable the multipathing software on the host system varies according to different ALUA modes (enabled or disabled).

- ALUA is enabled.

The configuration method is the same as that in Solaris 10.

- ALUA is disabled.

- i. Run the **format** command, select a mapped disk, and click **inquiry** to query **Vendor ID** and **Product ID** of the LUN.

- ii. Run the `cp /kernel/drv/scsi_vhci.conf /etc/driver/drv/scsi_vhci.conf` command to copy content of the `/kernel/drv/scsi_vhci.conf` file to the `/etc/driver/drv/scsi_vhci.conf` file.
- iii. Modify the `/etc/driver/drv/scsi_vhci.conf` configuration file and add **Vendor ID** and **Product ID** of the LUN to the configuration file. For example, if **Vendor ID** is **HUAWEI** and **Product ID** is **XXXXXX**, configure the file as follows:

```
scsi-vhci-failover-override =  
"HUAWEI XXXXXX", "f_sym";
```
- iv. Run the `stmsboot -D fp -e` command to activate the STMS function. The STMS takes effect after the operating system restarts.

---End

## Result

Run the `iscsiadm list target` command to query the target connected to the Solaris-based application server.

- If the following output is displayed, the Solaris-based application server is properly connected to the storage system.

```
# iscsiadm list target  
  
Target: iqn.2006-08.com.huawei:OceanStor:210000e0fc000005::192.168.10.6  
  
Alias: -  
TPGT: default  
  
ISID: 4000002a0000  
  
Connections: 0
```

- If no output is displayed, the Solaris-based application server failed to be connected to the storage system.

Run the `vi /var/adm/messages` command to open the `message` file for troubleshooting.

### 3.8.1.3.5 Configuring an Initiator (AIX)

This section describes how to configure an initiator on an application server running AIX.

## Prerequisites

The service network port on the application server is communicating properly with the iSCSI host port on the storage system. On the application server, run the `ping ip` command, where `ip` indicates the IP address of the iSCSI host port connected to the application server. If the application server receives the data packets sent from the iSCSI host port, the communication between the application server and storage system is normal. If the application server fails to receive the data packets, use either of the following methods to ensure normal communication:

- Configure the IP addresses of the iSCSI host port and service network port onto the same network segment.
- If the two IP addresses are on different network segments, add a route to establish a connection between them.



## Context

This section uses AIX 6.1 as an example to describe how to configure an iSCSI initiator. Other versions of AIX use the same method.

## Procedure

- Step 1** Log in to the application server as user **root**.
- Step 2** Run the **lslpp -l | grep devices.iscsi** command to check whether the iSCSI initiator is installed.
- If not installed, go to [Step 3](#).
  - If installed, go to [Step 6](#).

**Figure 3-28** Viewing the iSCSI software

```
-bash-3.2# lslpp -l |grep devices.iscsi
devices.iscsi.disk.rte      6.1.6.15  COMMITTED  iSCSI Disk Software
devices.iscsi.tape.rte     6.1.0.0   COMMITTED  iSCSI Tape Software
devices.iscsi_sw.rte       6.1.9.15  COMMITTED  iSCSI Software Device Driver
devices.iscsi_sw.rte       6.1.9.15  COMMITTED  iSCSI Software Device Driver
-bash-3.2#
```

- Step 3** Insert the operating system installation CD-ROM into the server's CD-ROM drive.
- Step 4** Run the **smitty update\_all** command to go to the installation and configuration page. After the installation and configuration page is displayed, press **Esc + 4**. The page for selecting an installation source is displayed. Select **/dev/cd0**.

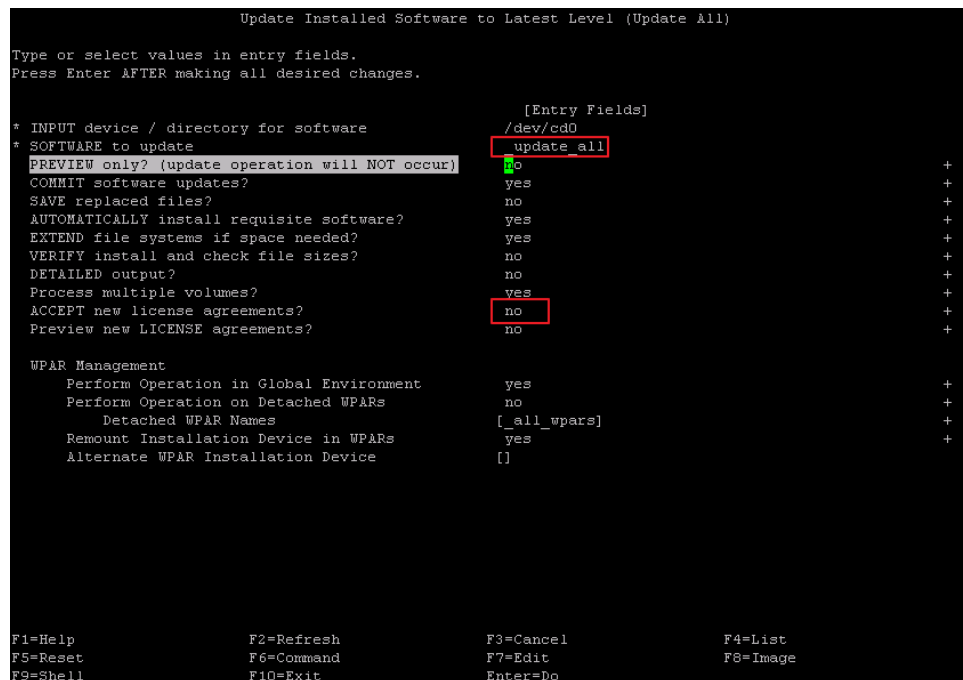
**Figure 3-29** Page for selecting an installation source

```
-----+-----
                INPUT device / directory for software
-----+-----
Move cursor to desired item and press Enter.
 /dev/cd0          (SAT& DVD-R&M Drive)
 /usr/sys/inst.images (Installation Directory)

F1=Help           F2=Refresh       F3=Cancel
F8=Image          F10=Exit         Enter=Do
/=Find            n=Find Next
```

- Step 5** After selecting an installation source, press **Enter**. The software installation page is displayed. Select the software that you want to install.

**Figure 3-30** Software installation page



On the software installation page, move the cursor to **SOFTWARE to update** and press **Esc + 4**. The page for selecting the software package is displayed. Press **F7** and select the four software packages in [Figure 3-28](#). Set **ACCEPT new license agreements** to **yes** and press **Enter** to start the installation.

**Step 6 Optional:** Change the name of the initiator.

When multiple application servers are connected to the storage system, you are advised to change the names of initiators to quickly locate the desired initiator. The name of an initiator must be unique. Otherwise, the connection between the storage system and the application server fails.

1. Run the **smit iscsi** command.

The **iSCSI** screen is displayed, as shown in [Figure 3-31](#).

**Figure 3-31** iSCSI screen



2. Select **iSCSI Protocol Device** and press **Enter**.

The **iSCSI Protocol Device** screen is displayed, as shown in [Figure 3-32](#).

**Figure 3-32** iSCSI Protocol Device screen

```
iSCSI Protocol Device

Move cursor to desired item and press Enter.

List All iSCSI Protocol Devices
Change / Show Characteristics of an iSCSI Protocol Device
Generate Error Report
Trace iSCSI Protocol Device
Remove iSCSI Protocol Device
```

3. Select **Change/Show Characteristics of an iSCSI Protocol Device** and press **Enter**. The available iSCSI protocol device is displayed. In this case, *iscsi0* is available, as shown in [Figure 3-33](#).

**Figure 3-33** Available iSCSI protocol devices

```
iSCSI Protocol Device

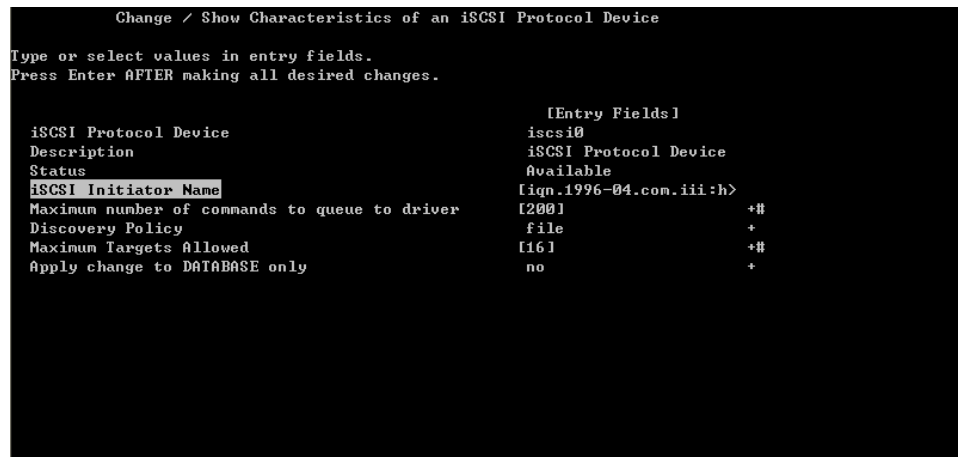
Move cursor to desired item and press Enter.

List All iSCSI Protocol Devices
Change / Show Characteristics of an iSCSI Protocol Device
Generate Error Report
Trace iSCSI Protocol Device
Remove iSCSI Protocol Device

-----+-----+
|                                     |
|                                     |
|                                     |
| Move cursor to desired item and press Enter. |
|                                     |
| iscsi0 Available iSCSI Protocol Device |
|                                     |
| Esc+1=Help           Esc+2=Refresh       Esc+3=Cancel |
| Esc+8=Image         Esc+0=Exit           Enter=Do |
| Es /=Find           n=Find Next |
|-----+-----+
```

4. Press **Enter**. The **Change/Show Characteristics of an iSCSI Protocol Device** screen is displayed, as shown in [Figure 3-34](#).

**Figure 3-34** Change/Show Characteristics of an iSCSI Protocol Device screen



5. Select and edit **iSCSI Initiator Name**.

 **NOTE**

- **iSCSI Initiator Name** contains only lowercase letters, digits, periods (.), hyphens (-), and colons (:). It contains not more than 223 characters.
- If you want to enable CHAP authentication later, the AIX operating system will use the initiator name as a CHAP user name. To ensure that the initiator name satisfies CHAP user name requirements, the initiator name must contain 4 to 25 characters and starts with a letter or digit.

6. Press **Enter**.
7. Press **ESC+0** to exit the **iSCSI** screen.
8. After changing the initiator name, run the **lsattr -El iscsi0** command to verify that the initiator name is updated.

In this case, the new initiator name is *iqn.localhost.hostid.7f000001*, as shown below.

```

# lsattr -El iscsi0
disc_filename /etc/iscsi/targets Configuration
file False
disc_policy file Discovery
Policy True
initiator_name iqn.localhost.hostid.7f000001 iSCSI Initiator
Name True
isns_srvnames auto iSNS Servers IP
Addresses True
isns_srvports iSNS Servers Port
Numbers True
max_targets 16 Maximum Targets
Allowed True
num_cmd_elems 200 Maximum number of commands to
queue to driver True
    
```

**Step 7** Configure the information about the target.

 **NOTE**

- The target is actually the iSCSI host port connected to the application server.
- Log in to the storage system using PuTTY, and run the **show iscsi target\_name port\_id** command to query the target name. In the preceding command, *port\_id* indicates the iSCSI port connecting the application server.

```
admin:/>show iscsi target_name eth_port_id=CTE0.A.IOM1.P0

iSCSI Target Name : iqn.2006-08.com.huawei:oceanstor:
2100001882f31578::20100:192.168.10.6
```

1. Run the **vi /etc/iscsi/targets** command to open the **targets** file.
2. Press **i** to edit the **targets** file.
3. Add the name and IP address of the target in the **targets** file.

Type the information in the format of **Target IP address Port number Target name**.

For example, if the target name is **iqn.2006-08.com.huawei:oceanstor:**

**2100001882f31578;**, the target IP address is **192.168.10.6**, and the port number is **3260**, type the information in the **targets** file, as shown in the following.

```
"/etc/iscsi/targets" 106 lines, 3717 characters

#           ; "."
#
# ChapSecret = %x22 *( any character )%x22
#           ; "
#           ; ChapSecret is a string enclosed in double quotes. The
#           ; quotes are required, but are not part of the secret.
#
# EXAMPLE 1: iSCSI Target without CHAP(MD5) authentication
#           Assume the target is at address 192.168.3.2,
#           the valid port is 5003
#           the name of the target is iqn.com.aaa-4125-23WTT26
#           The target line would look like:
#           192.168.3.2 5003 iqn.com.aaa-4125-23WTT26

#192.168.9.200 3260 iqn.1992-04.com.aaa:cx.ckm00083801516.a3
192.168.10.6 3260 iqn.2006-08.com.huawei:oceanstor:
2100001882f31578::192.168.10.6
```

4. Press **Esc** to exit the editing mode.
5. Run the **:wq** command and press **Enter** to save the changes and close the **targets** file.

**Step 8** Run the **cfgmgr -v** command to query the information about the iSCSI host port connected to the application server.

In the storage system, you can find the initiator that corresponds to the application server.

----End

## Follow-up Procedure

Due to the special processing mechanism of AIX-based application servers, the initiator is not connected to the storage system after being configured and **Status** is **Link Down** on the screen. However, the initiator is available and you can add it to the host.

### 3.8.1.3.6 Configuring an Initiator (HP-UX)

This section describes how to configure an initiator on an application server running HP-UX.

## Prerequisites

The service network port on the application server is communicating properly with the iSCSI host port on the storage system. On the application server, run the **ping ip** command, where *ip*

indicates the IP address of the iSCSI host port connected to the application server. If the application server receives the data packets sent from the iSCSI host port, the communication between the application server and storage system is normal. If the application server fails to receive the data packets, use either of the following methods to ensure normal communication:

- Configure the IP addresses of the iSCSI host port and service network port onto the same network segment.
- If the two IP addresses are on different network segments, add a route to establish a connection between them.

## Procedure

- Step 1** Log in to the application server as user **root**.
- Step 2** Run the **swlist iSCSI-00** command to check whether an iSCSI initiator is installed.
- If not installed, go to **Step 3**.
  - If installed, go to **Step 8**.
- Step 3** Go to the HP official website to download the required software package, and upload it to a location (such as **/bash**) of the operating system.
- Step 4** Run the **swinstall -s /bash/iSCSI-00\_B.11.31.03b\_HP-UX\_B.11.31\_IA\_PA.depot** command to go to the installation and configuration page. **/bash/iSCSI-00\_B.11.31.03b\_HP-UX\_B.11.31\_IA\_PA.depot** indicates the iSCSI software package name.
- Step 5** Select the software that you want to install and select **Mark For Install m** in **Actions** to mark the software.
- Step 6** After marking the software, select **Install...** in **Actions** to install the software.
- Step 7** The system analyzes the software. After the analysis is complete, click **OK** to start installation.
- After the iSCSI software is installed successfully, the system will generate an iSCSI management tool **icsiutil** in the **/opt/icsi/bin/icsiutil** directory.



## NOTICE

After the software is installed successfully, the system automatically restarts.

---

- Step 8 Optional:** Change the name of the initiator and configure an alias for the initiator.
- When multiple application servers are connected to the storage system, you are advised to change the names of initiators to quickly locate the desired initiator. The name of an initiator must be unique. Otherwise, the connection between the storage system and the application server fails.
  - For the storage system to properly identify the initiator of an HP-UX-based application server, you need to configure an alias for the initiator.
1. Run the **icsiutil -i -N newname** command to change the name of the initiator. In the preceding command, **newname** indicates the new initiator name.
- For example, change the name of the initiator to **iqn.1986-03.com.hp:renyuan.1234567890**.

```
# iscsiutil -i -N iqn.1986-03.com.hp:renyuan.1234567890

iscsiutil: Initiator Name "iqn.1986-03.com.hp:renyuan.1234567890" has been
successfully updated.

bash-4.0#

bash-4.0# iscsiutil -l

Initiator Name           : iqn.1986-03.com.hp:renyuan.1234567890
Initiator Alias          :

Authentication Method    :

CHAP Method              : CHAP_UNI
Initiator CHAP Name      :
CHAP Secret              :
NAS Hostname             :
NAS Secret               :
Radius Server Hostname   :
Header Digest            : None,CRC32C (default)
Data Digest              : None,CRC32C (default)
SLP Scope list for iSLPD :
```

2. Run the **iscsiutil -i -A *alias*** command to configure an alias for the initiator. *alias* is the alias for the initiator.

For example, change the name of the initiator to **china**.

```
# iscsiutil -i -A china

iscsiutil: Initiator Alias "china" has been successfully updated.

bash-4.0# iscsiutil -l

Initiator Name           : iqn.1986-03.com.hp:renyuan.1234567890
Initiator Alias          : china

Authentication Method    :

CHAP Method              : CHAP_UNI
Initiator CHAP Name      :
CHAP Secret              :
NAS Hostname             :
NAS Secret               :
Radius Server Hostname   :
Header Digest            : None,CRC32C (default)
Data Digest              : None,CRC32C (default)
```

```
SLP Scope list for iSLPD :
```

3. Run the **iscsiutil -l** command to check configured parameters.

### Step 9 Configure the IP address of the target.

#### NOTE

The IP address of the target is actually the IP address of the iSCSI host port connected to the application server.

1. Run the following command to configure the IP address of the target.

```
# iscsiutil -a -I 192.168.10.6
```

In this example, the IP address of the target is *192.168.10.6*.

2. After configuring the IP address of the target, run the **iscsiutil -p -D** command to view the added target.

The following output is displayed.

```
# iscsiutil -p -D
Discovery Target Information
-----
Target      #1
-----
IP Address      : 192.168.10.6
iSCSI TCP Port  : 3260
iSCSI Portal Group Tag : 1
```

After performing the preceding operations, you can find the initiator that corresponds to the application server on the storage system side.

### Step 10 Run the **/usr/sbin/ioscan -NH 64000** command to log in to the target and create a file containing the target information.

The following output is displayed.

```
# /usr/sbin/ioscan -NH 64000
H/W Path          Class          Description
=====
64000/0x0         usbmsvbus      SB Mass Storage
64000/0x0/0x0     escsi_ctlr     USB Mass Storage Virt Ctlr
64000/0x0/0x0.0x0 tgtpath
        usb target served by usb_ms_scsi driver, target port id 0x0
64000/0x0/0x0.0x0.0x0 lunpath        LUN path for disk5
64000/0x2         iscsi          iSCSI Virtual Root
64000/0x2/0x0     escsi_ctlr     iSCSI Virtual Controller
64000/0xfa00      esvroot        Escsi virtual root
64000/0xfa00/0x0 disk           HP          DG146BB976
64000/0xfa00/0x1 disk           HP          DG146BB976
64000/0xfa00/0x2 disk           TEAC        DVD-ROM DW-224EV
64000/0xfa00/0x57 ctl           ENGENIO    INF-01-00
64000/0xfa00/0x58 disk           ENGENIO    INF-01-00
64000/0xfa00/0x59 disk           ENGENIO    INF-01-00
64000/0xfa00/0x5a ctl           XXXX
64000/0xfa00/0x5b disk           XXXX
```

In the command output, **XXXX** indicates a specific product model or brand.

----End

### 3.8.1.3.7 Configuring an Initiator (VMware)

This section describes how to configure an initiator on an application server running VMware.



## Prerequisites

The service network port on the application server is communicating properly with the iSCSI host port on the storage system. On the application server, run the `ping ip` command, where `ip` indicates the IP address of the iSCSI host port connected to the application server. If the application server receives the data packets sent from the iSCSI host port, the communication between the application server and storage system is normal. If the application server fails to receive the data packets, use either of the following methods to ensure normal communication:

- Configure the IP addresses of the iSCSI host port and service network port onto the same network segment.
- If the two IP addresses are on different network segments, add a route to establish a connection between them.

## Context

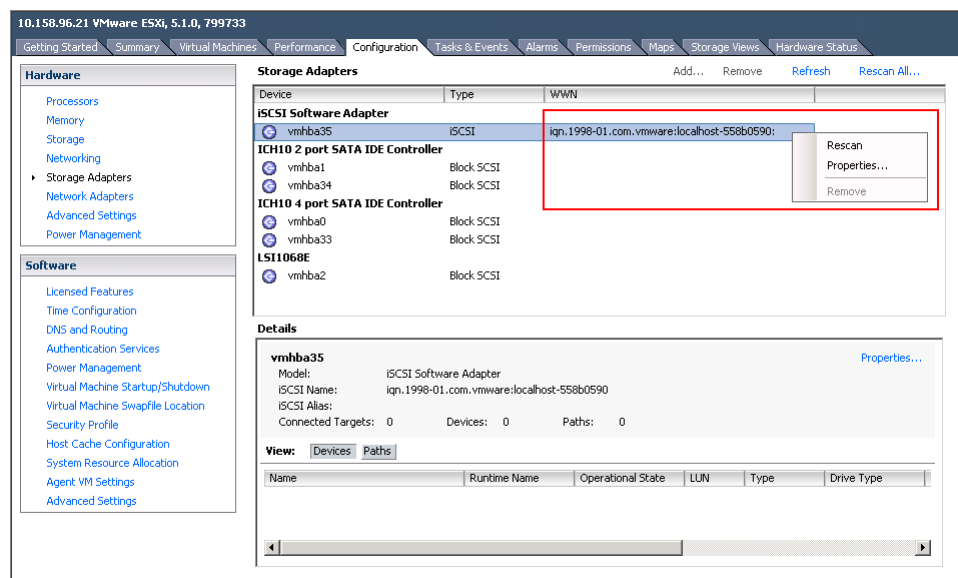
For VMware ESXi 4.1 and earlier versions, an iSCSI adapter already exists in a storage adapter. You can directly enable the iSCSI adapter. For VMware ESXi 5.0 and later versions, you must add an iSCSI adapter and then perform the follow-up configuration.

This section uses VMware ESXi 5.1 as an example to describe how to configure an initiator. The configuration method remains the same for other versions.

## Procedure

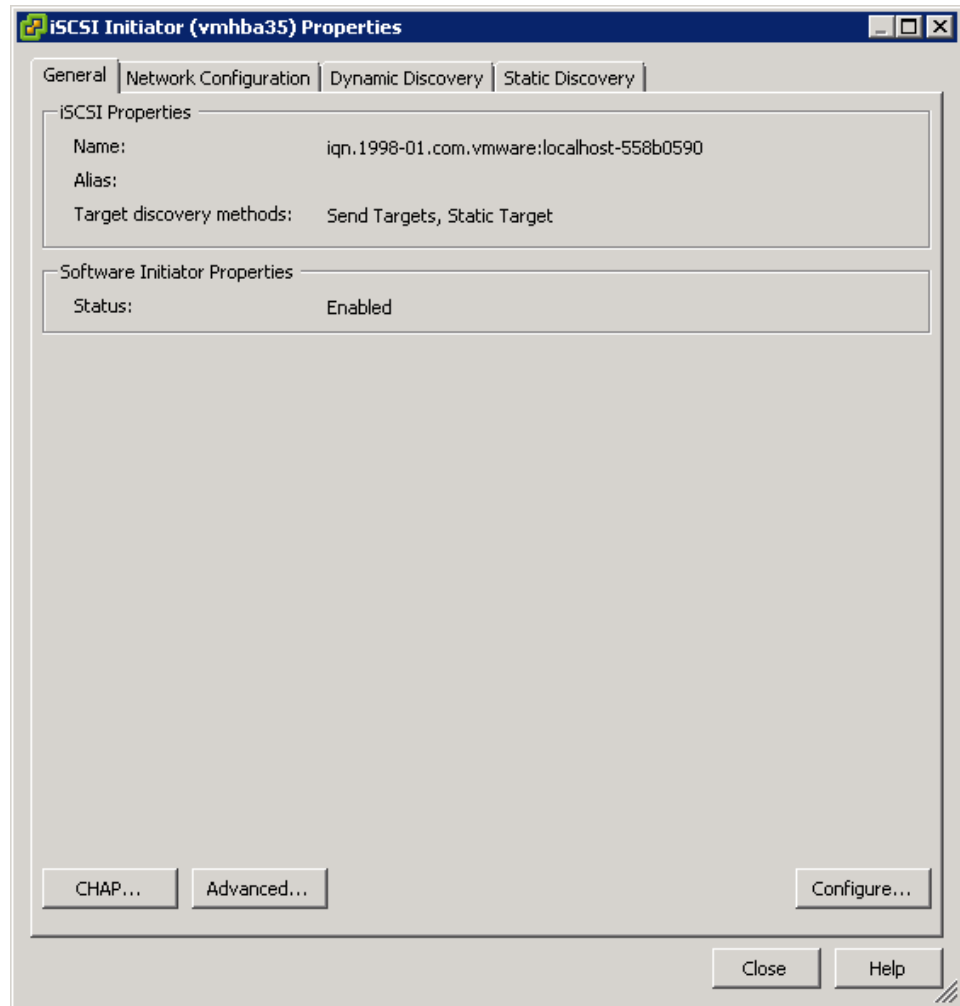
- Step 1** Go to the **iSCSI Initiator Properties** dialog box.
1. On the vSphere Client, click the **Configuration** tab.
  2. On the navigation bar, click **Storage Adapters**. In the function pane, click **Add**.
  3. Click **Add Software iSCSI Adapter**.
  4. After the addition, view the name of the initiator corresponding to the newly added software iSCSI adapter, as shown in **Figure 3-35**.

**Figure 3-35** Storage Adapters main page



5. Choose **Properties** from the shortcut menu.  
The **iSCSI Initiator Properties** dialog box is displayed, as shown in [Figure 3-36](#).

**Figure 3-36** iSCSI Initiator Properties dialog box

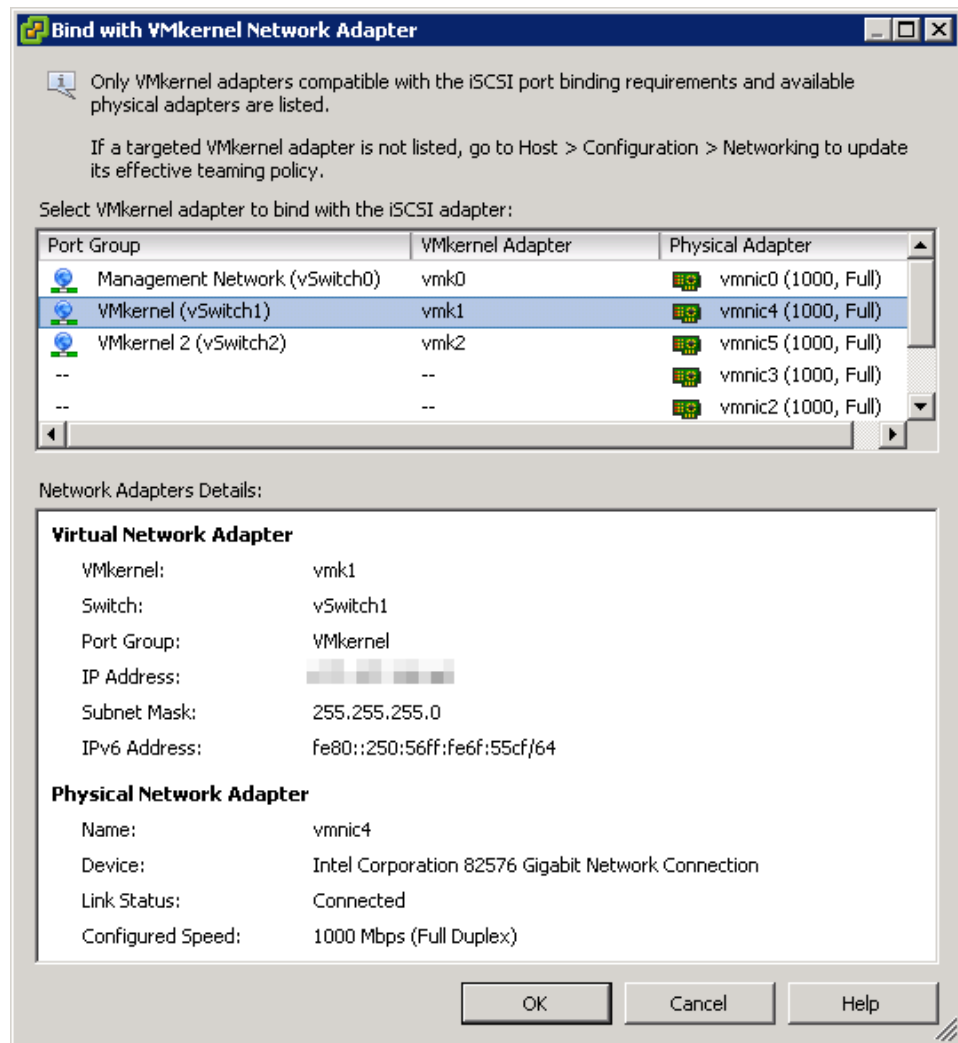


**Step 2** Bind with a VMKernel network adapter.

1. Click the **Network Configuration** tab.
2. Click **Add**.

The **Bind with VMkernel Network Adapter** dialog box is displayed, as shown in [Figure 3-37](#).

Figure 3-37 Bind with VMkernel Network Adapter dialog box



3. Select the VMkernel adapter to be bound with the iSCSI initiator.
4. Click **OK**.

The **iSCSI Initiator Properties** dialog box is displayed again.

**NOTE**

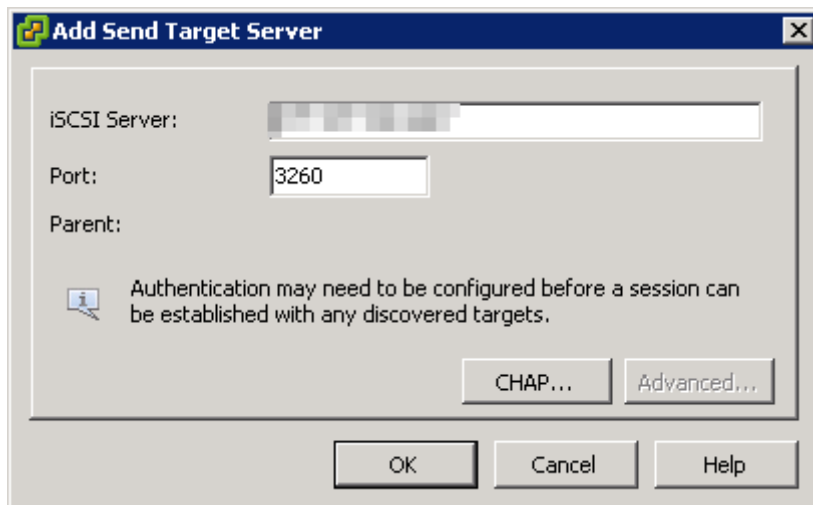
If only one path has been configured between the storage system and the application server, bind the iSCSI initiator with only one VMkernel adapter. If multiple paths have been configured, repeat the preceding steps to bind the iSCSI initiator with all the VMkernel adapters.

**Step 3** Configure the iSCSI target IP address.

1. Click the **Dynamic Discovery** tab.
2. Click **Add**.

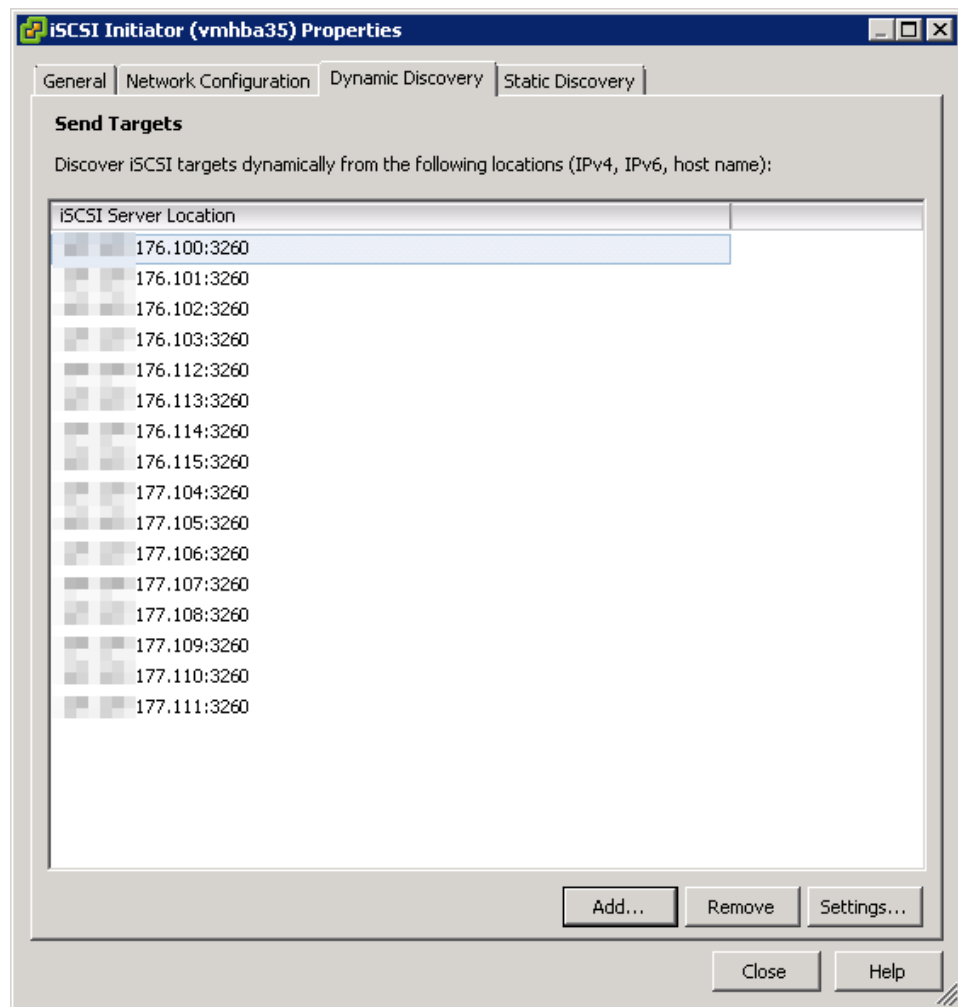
The **Add Send Target Server** dialog box is displayed, as shown in [Figure 3-38](#).

**Figure 3-38** Add Send Target Server dialog box



3. In the **iSCSI Server** text box, enter the IP address of the iSCSI target, namely the iSCSI port that connects the storage system to the application server.
4. In the **Port** text box, enter **3260**.
5. Click **OK** to add the iSCSI target to the target list, as shown in [Figure 3-39](#).

Figure 3-39 iSCSI target list



 **NOTE**

If the storage system connects to the application server through multiple paths, repeat the preceding steps to add all iSCSI port IP addresses to the target list.

**Step 4** Click **Close**.

The **Rescan** dialog box is displayed prompting you to rescan for network adapters.

**Step 5** Click **Yes**.

After the scan is completed, you have finished configuring an iSCSI initiator on a VMware-based application server.

----**End**

### 3.8.1.4 (Optional) Configuring CHAP Authentication

On a public network, any application server can access the storage system whose IP address of the iSCSI host port resides on the same network segment as that of the application server to implement data reads/writes. This poses risks to the data security of the storage system. To ensure the storage system access security, configure CHAP authentication to control the access to the storage system.

## Prerequisites

- The initiator has been added to the host.
- CHAP has been configured and enabled on the storage system for the initiator.
- No LUN is mapped to the host.

## Context

If you have configured CHAP on the storage system and enabled CHAP authentication for the initiator, the application server (or initiator) sends an iSCSI connection request to the storage system (or target) and provides the CHAP user name and password for authentication. After receiving the CHAP information, the storage system compares it with its own CHAP information. If the received CHAP user name and password match those on the storage system, the access from the application server is allowed.

### NOTE

If CHAP authentication is not enabled in iSCSI networking, spoofing may occur between an application server and a storage system.

### 3.8.1.4.1 Configuring CHAP Authentication (Windows)

After CHAP authentication is enabled on the storage system or the password used for CHAP authentication is changed, configure the CHAP user name and password on the Windows-based application server using Microsoft iSCSI Initiator to set up a connection to the storage system.

## Context

The storage system has been correctly connected to the application server through the CHAP authentication. Because of Windows protection mechanisms, although you change the CHAP authentication password on the storage system, the connection between the storage system and application server is not interrupted immediately. When the application server is restarted or a connection exception occurs, the connection will be interrupted. Therefore, you need to use the new password to configure the CHAP authentication again on the application server.

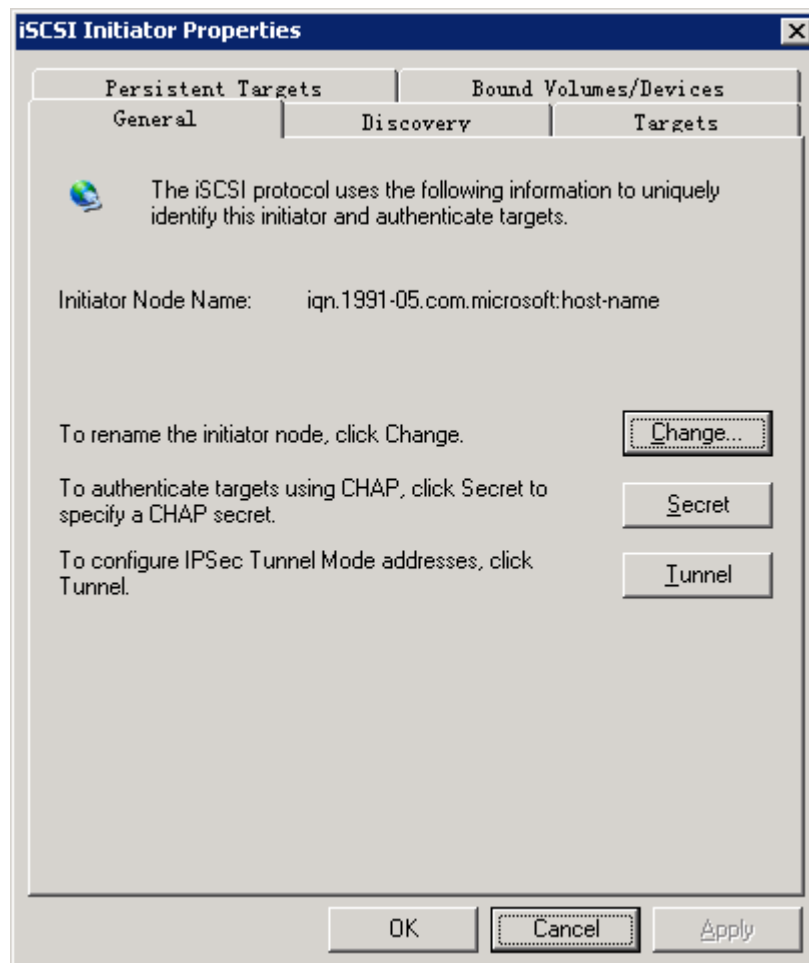
## Windows Server 2003 and Earlier Versions

Windows Server 2003 and earlier versions use the same method to configure CHAP authentication. This section uses Windows Server 2003 as an example to describe how to configure CHAP authentication.

- Step 1** Log in to the Windows-based application server as **administrator**.
- Step 2** Double-click the shortcut icon of **Microsoft iSCSI Initiator** on the desktop of the application server.

The **iSCSI Initiator Properties** dialog box is displayed, as shown in [Figure 3-40](#).

Figure 3-40 iSCSI Initiator Properties dialog box



**Step 3** Disconnect the application server from the storage system.

---

 **NOTICE**

If services are running between the application server and the storage system, disconnecting their iSCSI link interrupts the services.

---

1. In the **iSCSI Initiator Properties** dialog box, click the **Targets** tab.
2. Select the desired target and click **Details**. The **Target Properties** dialog box is displayed.
3. In the **Identifier** area, select the initiator and click **Log off**.

 **NOTE**

If a message is displayed indicating that the session is being used and cannot be logged off, check whether a LUN is mapped to the host. If a LUN is mapped to the host, delete the LUN mapping and try again.

4. Click **OK** to return to the **iSCSI Initiator Properties** dialog box.

**Step 4** On the **Persistent Targets** tab page, remove the target for which you want to configure CHAP authentication.

1. In the **iSCSI Initiator Properties** dialog box, click the **Persistent Targets** tab.
2. In the **Select a target** area, select the target port for which you want to configure CHAP authentication and click **Remove**.

**Step 5** Reconnect the target to the initiator and configure CHAP authentication.

1. In the **iSCSI Initiator Properties** dialog box, click the **Targets** tab.
2. In the **Targets** list, select the target port whose **Status** is **Inactive** and click **Log on**.

The **Log On to Target** dialog box is displayed.

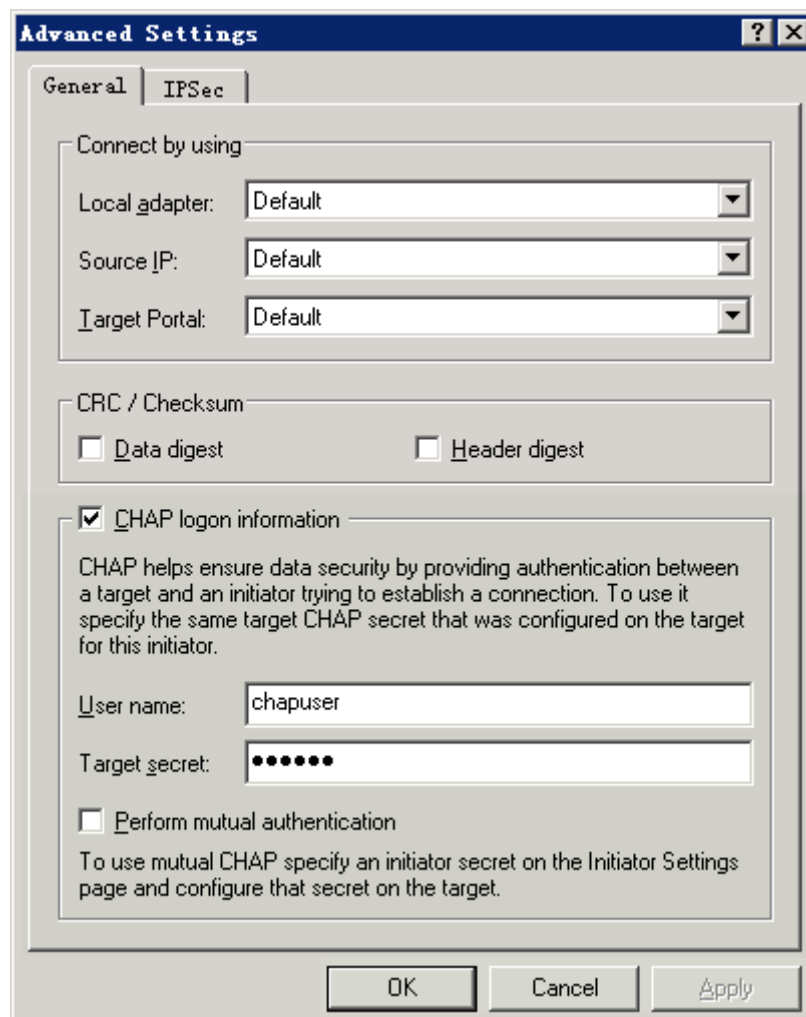
3. Click **Advanced**.

The **Advanced Settings** dialog box is displayed.

4. Select **CHAP logon information**.

**User name** and **Target secret** are available, as shown in [Figure 3-41](#).

**Figure 3-41 CHAP logon information**





5. In the **User name** and **Target secret**, enter the CHAP user name and password that are created on the storage system and added for the initiator.
6. Click **OK** to return to the **Log On to Target** dialog box.
7. Click **OK** to log in to the initiator and return to the **iSCSI Initiator Properties** dialog box.
  - If **Status** of the target port changes to **Connected** in the **Targets** list, the iSCSI connection is established between the application server and storage system.
  - If the **Authentication Failures** message is displayed, check whether the entered CHAP user name and password are incorrect and try again.

**Step 6** Click **OK**.

----End

## Windows Server 2008 and Later Versions

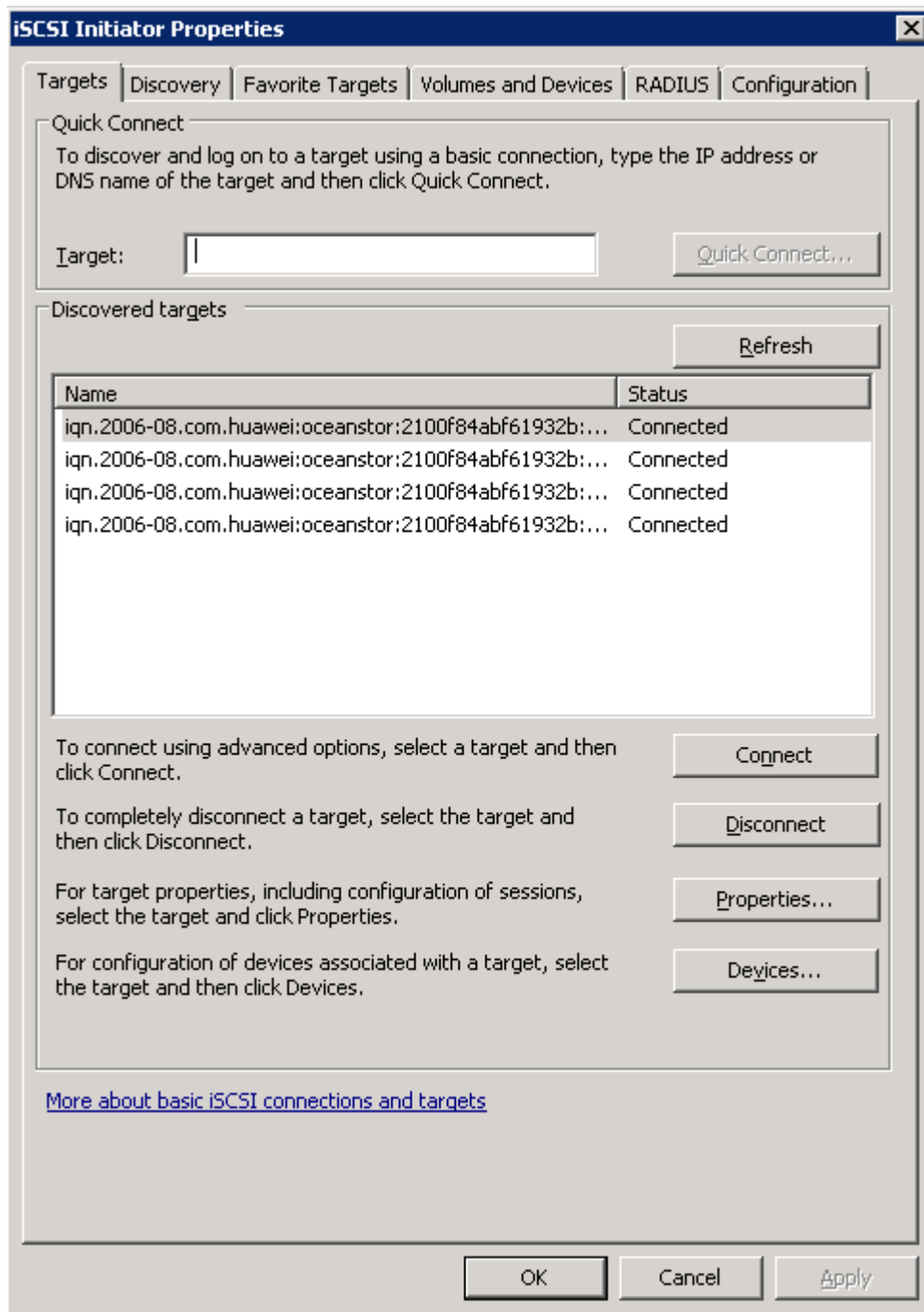
Windows Server 2008 and later versions use the same method to configure CHAP authentication. This section uses Windows Server 2008 as an example to describe how to configure CHAP authentication.

**Step 1** Log in to the Windows-based application server as **administrator**.

**Step 2** Choose **Start > All Programs** and run **iSCSI Initiator**.

The **iSCSI Initiator Properties** dialog box is displayed, as shown in [Figure 3-42](#).

Figure 3-42 iSCSI Initiator Properties dialog box



**Step 3** Disconnect the iSCSI connection between the application server and the storage system.



## NOTICE

If the iSCSI connection is disconnected, services operating between the application server and the storage system will be interrupted.

1. In the **iSCSI Initiator Properties** dialog box, click the **Targets** tab.
2. In the **Discovered targets** area, select the target to be disconnected and click **Disconnect**. The status of the target will change to **Inactive**.

 **NOTE**

If a message is displayed indicating that the session is being used and the connection cannot be disconnected, check whether a LUN is mapped to the virtual host. If a LUN is mapped to the host, delete the LUN mapping and try again.

**Step 4** Reconnect to the target and configure the CHAP authentication parameters.

1. In the **iSCSI Initiator Properties** dialog box, click the **Discovery** tab.
2. In the **Target Portals** area, click **Discover Portal...**

The **Discover Target Portal** dialog box is displayed.

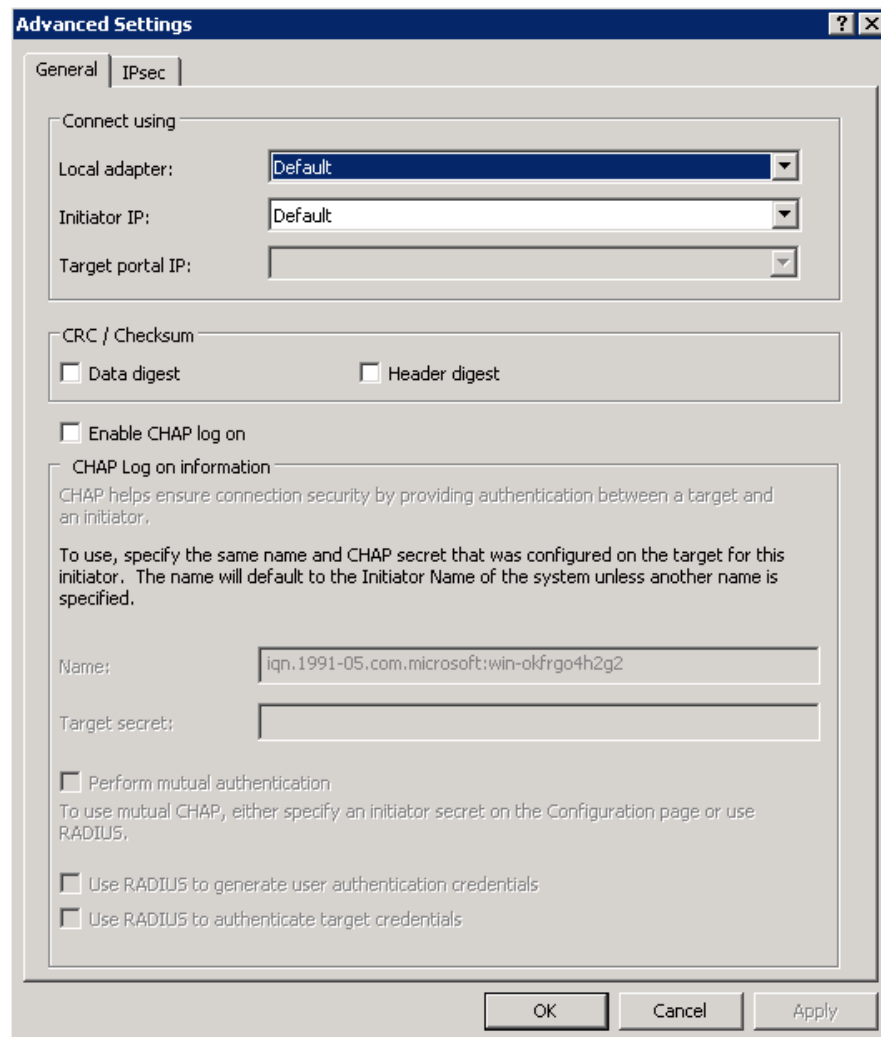
3. Click **Advanced...**

The **Advanced Settings** dialog box is displayed.

4. Select the **Enable CHAP log on** check box.

**Name** and **Target secret** become available, as shown in [Figure 3-43](#).

**Figure 3-43 CHAP login information**



5. In the **Name** and **Target secret** fields, enter the CHAP user name and password that have been created on the storage system and added to the initiator.
6. Click **OK** to return to the **Discover Target Portal** dialog box.
7. Click **OK** to log in to the initiator and return to the **iSCSI Initiator Properties** dialog box.
  - If **Status** of the target port on the **Targets** list changes to **Connected**, the iSCSI connection is established between the application server and the storage system.
  - If the **Authentication Failures** message is displayed, check whether the entered CHAP user name and password are incorrect and try again.

**Step 5** Click **OK** to complete the configuration of CHAP authentication.

---End

## Follow-up Procedure



### NOTICE

After an iSCSI connection between the application server and the storage system is successfully established, disabling the CHAP authentication will cause failure to log in to the storage system. To solve this problem, delete the information on the **Discovery** tab page and reconfigure the initiator.

---

When services are operating between the application server and the storage system, configuring the CHAP authentication will interrupt the services. If you want to restore these services, add mappings for the host again.

### 3.8.1.4.2 Configuring CHAP Authentication (SUSE)

After CHAP authentication is enabled on the storage system, configure the CHAP user name and password in the configuration file on an application server running SUSE 10 or a later version to set up a connection to the storage system.

## Procedure

**Step 1** Log in to the SUSE-based application server as user **root**.

**Step 2** Configure CHAP parameters.

1. Run the **iscsiadm -m node -u** command to stop all iSCSI services on the application server.
2. Run the **iscsiadm -m node -o update -p IP -n node.session.auth.authmethod -v CHAP** command to enable CHAP authentication. *IP* indicates the storage service port IP address.

For example, the storage service port IP address is **192.168.10.6**.

```
iscsiadm -m node -o update -p 192.168.10.6 -n node.session.auth.authmethod -v CHAP
```

3. Run the **iscsiadm -m node -o update -p IP -n node.session.auth.username -v chap\_user** command. *IP* indicates the storage service port IP address. *chap\_user*

indicates the CHAP user name that is created on the storage system and added to the initiator.

For example, the CPAP user name is **CHAP-user1**.

```
iscsiadm -m node -o update -p 192.168.10.6 -n node.session.auth.username -v CHAP-user1
```

4. Run the **iscsiadm -m node -o update -p IP -n node.session.auth.password -v password** command. *IP* indicates the storage service port IP address. *password* indicates the password of the CHAP user.

For example, the password of the CPAP user is **11aa3344BB66**.

```
iscsiadm -m node -o update -p 192.168.10.6 -n node.session.auth.password -v 11aa3344BB66
```

5. Run the **iscsiadm -m node -p IP -l** command to log in to the target again.

```
iscsiadm -m node -p 192.168.10.6 -l
```

After you log in to the target successfully, the following information will be displayed.

```
Login to [iface: default, target: iqn.2006-08.com.huawei:oceastor:21000018821b2bbb::192.168.10.6, portal: 192.168.10.6, 3260]: successful
```

---End

### 3.8.1.4.3 Configuring CHAP Authentication (Red Hat)

After CHAP authentication is enabled on the storage system, configure the CHAP user name and password on the Red Hat-based application server to set up a connection to the storage system.

## Context

The method used to configure CHAP authentication varies according to different Red Hat versions.

- Red Hat Linux AS4

The **iscsi.conf** configuration file is modified to add the CHAP user name and password.

- Red Hat Linux AS5 and later versions

Two methods are supported to configure CHAP authentication.

- Modify the **iscsid.conf** configuration file to add the CHAP user name and password.
- Run the **iscsiadm** command to set the CHAP user name and password.

## Procedure

**Step 1** Log in to the Red Hat-based application server as user **root**.

**Step 2** Configure CHAP authentication information.

- Red Hat Linux AS4

- a. Run the **/etc/init.d/iscsi stop** command to stop iSCSI services.
- b. Run the **vi /etc/iscsi.conf** command to open the **iscsi.conf** file.
- c. Press **i** to enter the editing mode.
- d. Add the CHAP user name and password before the target IP address. In **Username=** and **Password=**, enter the CHAP user name and password that are created on the storage system and added to the initiator respectively. In this example, the CHAP user name is **CHAP-user1** and the password is **11aa3344BB66**.

The following output is displayed.

```
Username=CHAP-user1  
Password=11aa3344BB66  
DiscoveryAddress=192.168.10.6
```

 **NOTE**

When you configure CHAP authentication in the configuration file on a Red Hat-based application server, you must add **Username** and **Password** before **DiscoveryAddress**. Otherwise, the initiator rejects the CHAP authentication request initiated by the target.

- e. Press **Esc** to exit the editing mode.
  - f. Run the **:wq** command to save the changes and close the **iscsi.conf** file.
  - g. Run the **/etc/init.d/iscsi restart** command to restart iSCSI services and to make the settings take effect.
- Red Hat Linux AS5 and later versions

CHAP authentication is configured by modifying the **iscsid.conf** configuration file.

- a. Run the **/etc/init.d/iscsi stop** command to stop all iSCSI services on the application server.
- b. Run the **vi /etc/iscsi/iscsid.conf** command to open the **iscsid.conf** file.
- c. Press **i** to enter the editing mode and then edit the **iscsid.conf** file.
- d. In the **CHAP Settings** area, set CHAP parameters: **node.session.auth.username** and **node.session.auth.password**.

```
# To enable CHAP authentication set node.session.auth.authmethod to CHAP  
#The default is none.  
node.session.auth.authmethod = CHAP  
# To set a CHAP user name and password for initiator authentication by  
the target(s),  
#uncomment the following lines:  
node.session.auth.username=admin  
node.session.auth.password=12345678abcd
```

 **NOTE**

In the preceding example, **admin** and **12345678abcd** are the CHAP user name and password configured on the storage system for the initiator.

- e. Press **Esc** to exit the editing mode.
- f. Run the **:wq** command to save the changes and close the **iscsid.conf** file.
- g. Run the **iscsiadm -m node -l all** command to log in to all the targets connected to the application server.
- h. Run the **/etc/init.d/iscsi restart** command to restart iSCSI services to make the settings take effect.

---End

#### 3.8.1.4.4 Configuring CHAP Authentication (Solaris)

After CHAP authentication is enabled on the storage system, configure the CHAP user name and password in the configuration file on the Solaris-based application server to set up a connection to the storage system.

### Context

The **iscsiadm** command is executed on Solaris to set the CHAP user name and password.

## Procedure

**Step 1** Log in to the Solaris-based application server as user **root**.

**Step 2** Configure CHAP authentication information.

1. Run the **iscsiadm modify initiator-node -a CHAP** command to enable CHAP authentication on the application server.
2. Run the **iscsiadm modify initiator-node -H chapname** command to change the CHAP user name. *chapname* indicates the CHAP user name that has been created on the storage system and added to the initiator.
3. Run the **iscsiadm modify initiator-node -C** command to enter and confirm the password.

 **NOTE**

The CHAP password must consist of 12 to 16 characters.

----End

### 3.8.1.4.5 Configuring CHAP Authentication (AIX)

After CHAP authentication is enabled on the storage system, configure the CHAP user name and password in the configuration file on the AIX-based application server to set up a connection to the storage system.

## Prerequisites

An iSCSI link has been established between the application server and storage system.

## Procedure

**Step 1** Log in to the AIX-based application server as user **root**.

**Step 2** Configure the CHAP user name and password.

1. Run the **vi /etc/iscsi/autosecrets** command to open the **autosecrets** file.
2. Press **i** to edit the **autosecrets** file.
3. Add the CHAP user name and password at the end of the **autosecrets** file.

For example, if the CHAP user name is **CHAP-user1** and the password is **11aa3344BB66**, type the following information:

```
CHAP-user1 "11aa3344BB66"
```

 **NOTE**

By default, **CHAP Name** has the same value as **iSCSI Initiator Name**.

4. Press **Esc** to exit the editing mode.
5. Run the **:wq** command and press **Enter** to save the settings and close the **autosecrets** file.

**Step 3** Add the CHAP user name and password to the information about the target.

1. Run the **vi /etc/iscsi/targets** command to open the **targets** file.
2. Press **i** to edit the **targets** file.
3. Add the CHAP password following the information configured in [Step 7](#).

Leave a space between the IP address of the target and the CHAP password and enclose the CHAP password with double quotation marks. Using the initiator configured in [3.8.1.3.5 Configuring an Initiator \(AIX\)](#) as an example, add the CHAP password as follows:

```
192.168.10.6 3260 iqn.2006-08.com.huawei:oceanstor:2100001882f31578:notconfig:
192.168.10.6 "11aa3344BB66"
```

4. Press **Esc** to exit the editing mode.
5. Run the **:wq** command and press **Enter** to save the changes and close the **targets** file.

**Step 4** Run the **/etc/init.d/iscsi restart** command to restart iSCSI services to make the settings take effect.

----End

### 3.8.1.4.6 Configuring CHAP Authentication (HP-UX)

After CHAP authentication is enabled on the storage system, configure the CHAP user name and password on the HP-UX-based application server to set up a connection to the storage system.

## Prerequisites

An iSCSI link has been established between the application server and storage system.

## Procedure

**Step 1** Log in to the HP-UX-based application server as user **root**.

**Step 2** Enable CHAP authentication on the target.

- If the application server connects to one storage system only, the following command is used as an example to enable the CHAP authentication mode:

```
iscsiutil -u -H CHAP_UNI
```

In this example, the CHAP security authentication is in unidirectional authentication mode.

#### NOTE

The command syntax is **iscsiutil -u -H <chap-authentication-type>**.

- If the application server connects to multiple storage systems, the following command is used as an example to enable the CHAP authentication mode:

```
iscsiutil -u -H CHAP_UNI -I 192.168.10.6 -M 1
```

In this example, the IP address of the target is **192.168.10.6** and unidirectional CHAP authentication is configured.

#### NOTE

The command syntax is **iscsiutil -u -H <chap-authentication-type> [-I <ip-address>] [-M <portal-grp-tag>]**, where the value of *portal-grp-tag* behind **-M** can be obtained by running the **iscsiutil -p -D** command.

**Step 3** Configure CHAP parameters.

1. Configure the CHAP user name.
  - If the application server connects to one storage system only, the following command is used as an example to configure the CHAP user name:

```
iscsiutil -u -N chap-1
```



In this example, the CHAP user name is **chap-1** for the initiator.

 **NOTE**

The command syntax is `iscsiutil -u -N <chap-initiator-name>`.

- If the application server connects to multiple storage systems, you need to configure a corresponding account for each storage system. The following command is used as an example to configure the CHAP user name:

```
iscsiutil -u -N chap-1 -I 192.168.10.6 -M 1
```

In this example, the CHAP user name is **chap-1** for the initiator whose IP address is **192.168.10.6**.

 **NOTE**

The command syntax is `iscsiutil -u -N <chap-initiator-name> [-I <ip-address>] [-M <portal-grp-tag>]`, where the value of *portal-grp-tag* behind `-M` can be obtained by running the `iscsiutil -p -D` command.

2. Configure the CHAP password.

- If the application server connects to one storage system only, the following command is used as an example to configure the CHAP password:

```
# iscsiutil -u -W 11aa3344BB66
```

In this example, the CHAP password is **11aa3344BB66** for the initiator.

 **NOTE**

The command syntax is `iscsiutil -u -W <chap-initiator-secret>`.

- If the application server connects to multiple storage systems, you need to configure a corresponding password for each storage system. The following command is used as an example to configure the CHAP password:

```
# iscsiutil -u -W 11aa3344BB66 -I 192.168.10.6 -M 1
```

In this example, the CHAP password is **11aa3344BB66** for the initiator whose IP address is **192.168.10.6**.

 **NOTE**

The command syntax is `iscsiutil -u -W <chap-initiator-secret> [-I <ip-address>] [-M <portal-grp-tag>]`, where the value of *portal-grp-tag* behind `-M` can be obtained by running the `iscsiutil -p -D` command.

**Step 4** Run the `iscsiutil -l` command to verify that the CHAP parameters are correctly configured.

----End

### 3.8.1.4.7 Configuring CHAP Authentication (VMware)

After CHAP authentication is enabled on the storage system, configure the CHAP user name and password on the VMware ESX-based application server to set up a connection to the storage system.

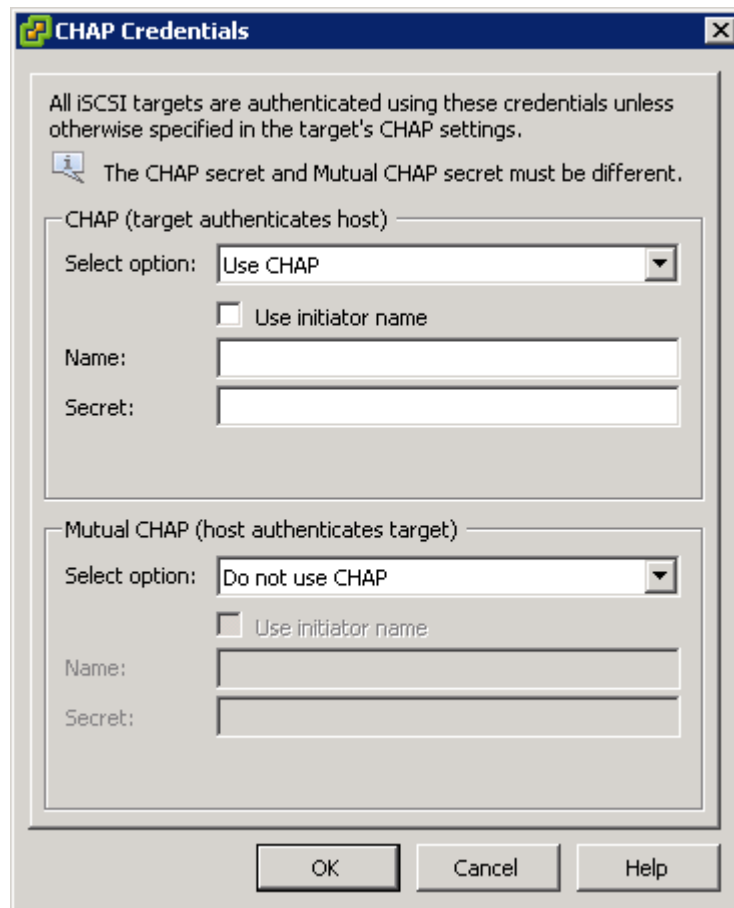
## Procedure

**Step 1** Go to the **CHAP Credentials** dialog box.

1. On the vSphere Client, click the **Configuration** tab.
2. On the navigation bar, click **Storage Adapters**.
3. On the **Storage Adapters** page, right-click the iSCSI initiator.
4. Choose **Properties** from the shortcut menu.

- The **iSCSI Initiator Properties** dialog box is displayed.
5. Click **CHAP**.  
The **CHAP Credentials** dialog box is displayed, as shown in **Figure 3-44**.

**Figure 3-44** CHAP Credentials dialog box



**Step 2** Configure CHAP parameters.

---

 **NOTICE**

After you have successfully established an iSCSI connection between the application server and storage system, if the CHAP authentication is disabled, the storage system becomes inaccessible. In this case, you need to configure the initiator again.

- 
1. In the **CHAP (target authenticates host)** area, select **Use CHAP** from the **Select option** drop-down list.
  2. In the **Name** and **Secret** text boxes, enter the CHAP user name and password that have been created on the storage system and added for the initiator.
  3. In the **Mutual CHAP (host authenticates target)** area, select **Do not use CHAP** from the **Select option** drop-down list.

**Step 3** Click **OK**.

---End

### 3.8.1.5 Setting Ethernet Port Information

Configure Ethernet port parameters to ensure proper communication between the storage system and application server.



#### Precautions

Note the following items when setting the properties of an Ethernet port:

- The default IP addresses of the internal heartbeat on the dual-controller storage system are **127.127.127.10** and **127.127.127.11**, and the default IP addresses of the internal heartbeat on the four-controller storage system are **127.127.127.10**, **127.127.127.11**, **127.127.127.12**, and **127.127.127.13**. Therefore, the IP address of a port cannot fall within the 127.127.127.XXX segment. Besides, the IP address of the gateway cannot be **127.127.127.10**, **127.127.127.11**, **127.127.127.12**, or **127.127.127.13**. Otherwise, routing will fail. (Internal heartbeat links are established between controllers for these controllers to detect each other's working status. You do not need to separately connect cables. In addition, internal heartbeat IP addresses have been assigned before delivery, and you cannot change these IP addresses).
- For 2000, 2000F, 5000, 5000F, 6000 and 6000F series storage systems, the IP address of the Ethernet port cannot be in the same network segment as the management network port. For 18000 and 18000F series storage systems, the IP address of the Ethernet port cannot be in the same network segment as the service processor (SVP) and engine management network ports.
- The IP address of the Ethernet port cannot be in the same network segment as that of a maintenance network port.
- If the Ethernet port connects to an application server, the IP address of the Ethernet port must be in the same network segment as that of the service network port on the application server. If the Ethernet port connects to another storage device, the IP address of the Ethernet port must be in the same network segment as that of the Ethernet port on the other storage device. If the network segment has insufficient available IP addresses, see [3.8.1.6 \(Optional\) Adding Routes](#).

#### Procedure

**Step 1** Go to the **Ethernet Port** dialog box.

1. On the right navigation bar, click  **System**.
2. Click the controller enclosure where the Ethernet port resides.
3. Click  to switch to the rear view.
4. Click the Ethernet port whose information you want to view.  
The **Ethernet Port** dialog box is displayed.
5. Click **Modify**.

**Ethernet Port**

Location: CTE0.B.P0  
Health Status: Normal  
Running Status: Link up  
Working Rate (Gbit/s): 1  
Max. Working Rate (Gbit/s): 2

IPv4 Address:   
Subnet Mask:

IPv6 Address:   
Prefix:

MAC Address: 0022a105a50c  
Port Switch: Enable  
MTU (Byte): 1500   
Bond Name: --  
iSCSI Target Name: --

Apply Cancel Help <<

**Step 2** Set the Ethernet port.

1. In the **IPv4 Address** or **IPv6 Address** text box, enter an IP address for the Ethernet port.
2. In the **Subnet Mask** or **Prefix** area, enter the subnet mask or prefix of the Ethernet port.
3. In **MTU (Byte)**, type a maximum transfer unit (MTU) for the packets transferred between the Ethernet port and the application server.  
The MTU must be an integer ranging from 1500 to 9000.

**Step 3** Confirm the Ethernet port configuration.

1. Click **Apply**.  
The **Danger** dialog box is displayed.
2. Confirm the information in the dialog box and select **I have read and understood the consequences associated with performing this operation**.
3. Click **OK**.  
The **Success** message box is displayed, indicating that the operation succeeded.
4. Click **OK**.

----End

### 3.8.1.6 (Optional) Adding Routes

If iSCSI networking is adopted and data needs to be transmitted across network segments, you need to configure routes.

## Prerequisites

The Ethernet port has been assigned an IP address.

## Procedure

**Step 1** Log in to DeviceManager.

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

**Step 3** Select the Ethernet port for which you want to add a route and click **Route Management**.  
The **Route Management** dialog box is displayed.

**Step 4** Configure the route information for the Ethernet port.

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

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



### NOTICE

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

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

There are three route options:

- Default route

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

- Host route

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

- Network segment route

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

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

**Step 5** Click **OK**. The route information is added to the route list.

A security alert dialog box is displayed.

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

**Step 7** Click **OK**.

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

 **NOTE**

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

**Step 8** Click **Close**.

---End

## 3.8.2 Fibre Channel Networking

This section describes how to configure the connectivity between host and storage system through FC networking.

### 3.8.2.1 Configuring Fibre Channel Switches

Configuring zones for Fibre Channel switches can avoid conflicts and improve flexibility of service systems.

#### 3.8.2.1.1 Querying the Switch Model and Version

Before using Fibre Channel switches, you need to query the switch model and version.

### Context

The commonly used Fibre Channel switches are mainly from Brocade, Cisco, and QLogic. The following uses a Brocade switch as an example to explain how to configure switches.

## Procedure

**Step 1** Log in to the Brocade switch from a web browser.

On a web browser, enter the IP address of the Brocade switch. The Web Tools switch login dialog box is displayed. Enter the account and password. The default account and password are **admin** and **password**. The switch management page is displayed.

---



### NOTICE

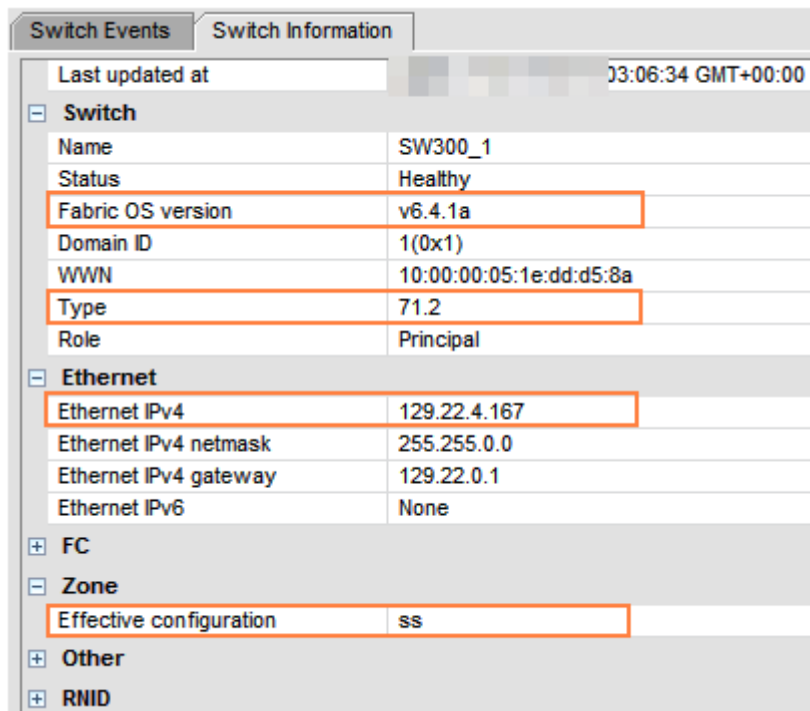
Web Tools works correctly only when Java is installed on the host. Java 1.6 or later is recommended.

---

**Step 2** View the switch information.

On the switch management page that is displayed, click **Switch Information**. The switch information is displayed, as shown in [Figure 3-45](#).

**Figure 3-45** Switch information



Switch Information	
Last updated at	03:06:34 GMT+00:00
<b>Switch</b>	
Name	SW300_1
Status	Healthy
Fabric OS version	v6.4.1a
Domain ID	1(0x1)
WWN	10:00:00:05:1e:dd:d5:8a
Type	71.2
Role	Principal
<b>Ethernet</b>	
Ethernet IPv4	129.22.4.167
Ethernet IPv4 netmask	255.255.0.0
Ethernet IPv4 gateway	129.22.0.1
Ethernet IPv6	None
<b>FC</b>	
<b>Zone</b>	
Effective configuration	ss
<b>Other</b>	
<b>RNID</b>	

You can obtain the following information from [Figure 3-45](#):

- **Fabric OS version:** indicates the switch version information.

 **NOTE**

The interoperability between switches and storage systems varies with the switch version. Only switches of authenticated versions can interconnect correctly with storage systems. For details about the interoperability between switches and storage systems, use [OceanStor Interoperability Navigator](#).

- **Type:** This parameter is a decimal consisting of an integer and a decimal fraction. The integer indicates the switch model and the decimal fraction indicates the switch template version. You only need to pay attention to the switch model. [Table 3-18](#) describes switch model mapping.

**Table 3-18** Mapping between switch types and names

Switch Type	Switch Name	Switch Type	Switch Name
1	Brocade 1000 Switch	58	Brocade 5000 Switch
2,6	Brocade 2800 Switch	61	Brocade 4424 Embedded Switch
3	Brocade 2100,2400 Switches	62	Brocade DCX Backbone
4	Brocade 20x0,2010,2040,2050 Switches	64	Brocade 5300 Switch
5	Brocade 22x0,2210,2240,2250 Switches	66	Brocade 5100 Switch
7	Brocade 2000 Switch	67	Brocade Encryption Switch
9	Brocade 3800 Switch	69	Brocade 5410 Blade
10	Brocade 12000 Director	70	Brocade 5410 Embedded Switch
12	Brocade 3900 Switch	71	Brocade 300 Switch
16	Brocade 3200 Switch	72	Brocade 5480 Embedded Switch
17	Brocade 3800VL	73	Brocade 5470 Embedded Switch
18	Brocade 3000 Switch	75	Brocade M5424 Embedded Switch
21	Brocade 24000 Director	76	Brocade 8000 Switch
22	Brocade 3016 Switch	77	Brocade DCX-4S Backbone
26	Brocade 3850 Switch	83	Brocade 7800 Extension Switch



Switch Type	Switch Name	Switch Type	Switch Name
27	Brocade 3250 Switch	86	Brocade 5450 Embedded Switch
29	Brocade 4012 Embedded Switch	87	Brocade 5460 Embedded Switch
32	Brocade 4100 Switch	90	Brocade 8470 Embedded Switch
33	Brocade 3014 Switch	92	Brocade VA-40FC Switch
34	Brocade 200E Switch	95	Brocade VDX 6720-24 Data Center Switch
37	Brocade 4020 Embedded Switch	96	Brocade VDX 6730-32 Data Center Switch
38	Brocade 7420 SAN Router	97	Brocade VDX 6720-60 Data Center Switch
40	Fibre Channel Routing (FCR) Front Domain	98	Brocade VDX 6730-76 Data Center Switch
41	Fibre Channel Routing, (FCR) Xlate Domain	108	Dell M8428-k FCoE Embedded Switch
42	Brocade 48000 Director	109	Brocade 6510 Switch
43	Brocade 4024 Embedded Switch	116	Brocade VDX 6710 Data Center Switch
44	Brocade 4900 Switch	117	Brocade 6547 Embedded Switch
45	Brocade 4016 Embedded Switch	118	Brocade 6505 Switch
46	Brocade 7500 Switch	120	Brocade DCX 8510-8 Backbone
51	Brocade 4018 Embedded Switch	121	Brocade DCX 8510-4 Backbone
55.2	Brocade 7600 Switch	-	-

- **Ethernet IPv4:** indicates the switch IP address.
- **Effective configuration:** indicates the currently effective configurations. This parameter is important and is related to zone configurations. In this example, the currently effective configuration is **ss**.

---End

### 3.8.2.1.2 Configuring Zones

Zone configuration is important for Fibre Channel switches. This section describes how to configure switch zones.

#### Context

The zone function of a Fibre Channel switch is similar to the VLAN function of an Ethernet switch. It allocates devices on a SAN network (such as hosts and storage devices) into different zones, and devices in different zones cannot communicate with each other. In this way, network devices are isolated and will not interfere with each other. When you are configuring zone information, small zones are preferred, namely, adding two ports carrying services to one zone.

---

#### NOTICE

If the host port and the storage port cannot reside in the same zone, you are advised to configure the zone in a way that high-throughput services (such as backup services) and real-time services are isolated during network configuration to avoid impacts on real-time services caused by bandwidth preemption.

---

#### Procedure

**Step 1** Log in to the Brocade switch from a web browser. This step is the same as that in section [3.8.2.1.1 Querying the Switch Model and Version](#).

**Step 2** Check the switch port status.

Normally, the switch port indicators are steady green, as shown in [Figure 3-46](#).

**Figure 3-46** Switch port indicator status



If ports connecting the host or storage system are not identified by the switch, check the connectivity between the host or storage system and the switch ports.

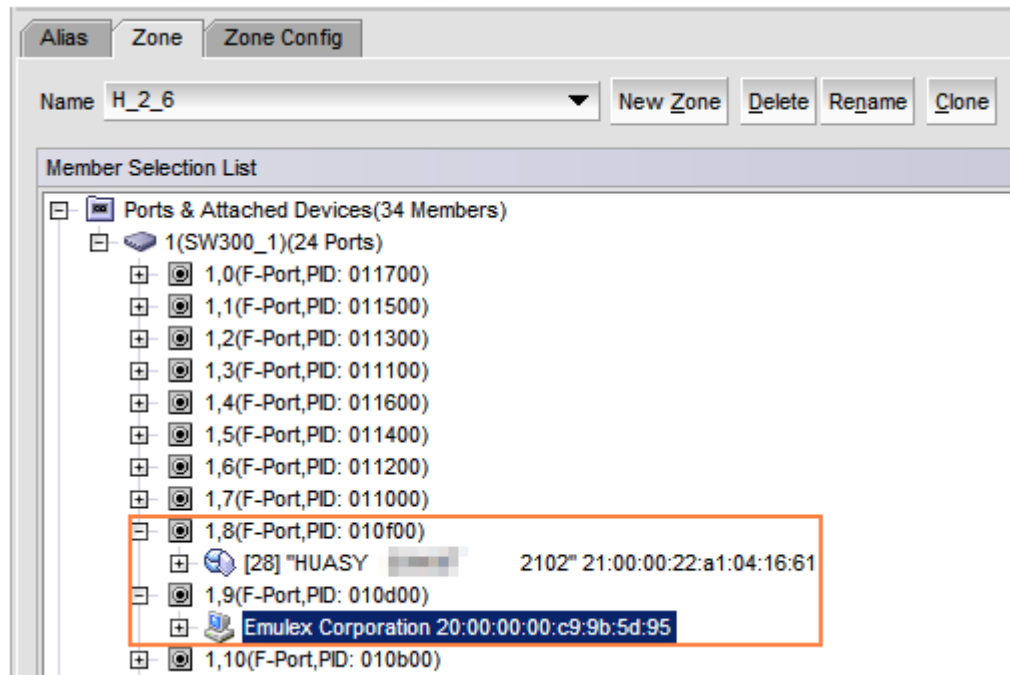
**Step 3** Go to the **Zone Admin** page.

In the navigation tree of **Web Tools**, choose **Task > Manage > Zone Admin**. You can also choose **Manage > Zone Admin** in the navigation bar.

**Step 4** Check whether the switch identifies hosts and storage systems.

On the **Zone Admin** page, click the **Zone** tab. In **Ports&Attached Devices**, check whether all related ports are identified, as shown in **Figure 3-47**.

**Figure 3-47** Zone tab page

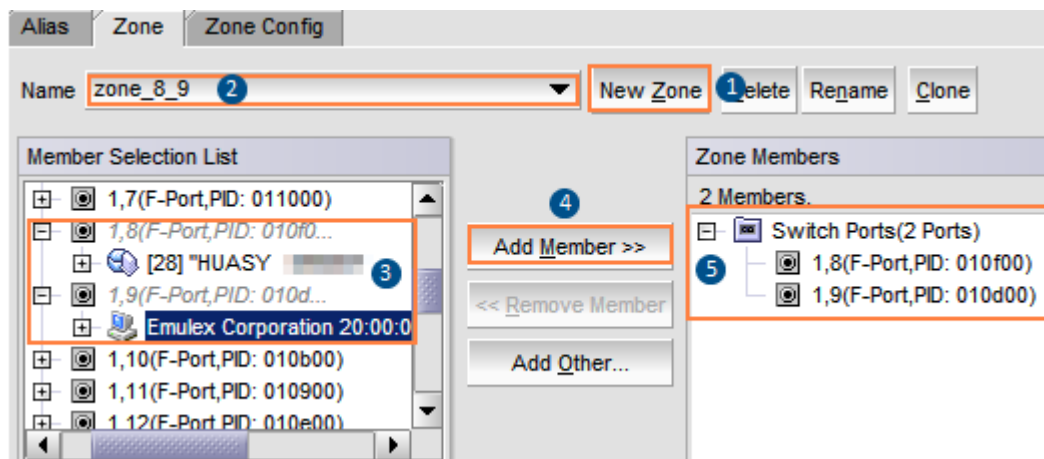


**Figure 3-47** shows that ports 1,8 and 1,9 in use are correctly identified by the switch. If ports connecting the host or storage system are not identified by the switch, check the connectivity between the host or storage system and the switch ports.

**Step 5** Create a zone.

On the **Zone** tab page, click **New Zone** to create a zone and name it **zone\_8\_9**. Select ports 1,8 and 1,9 and click **Add Member** to add them to the new zone, as shown in **Figure 3-48**.

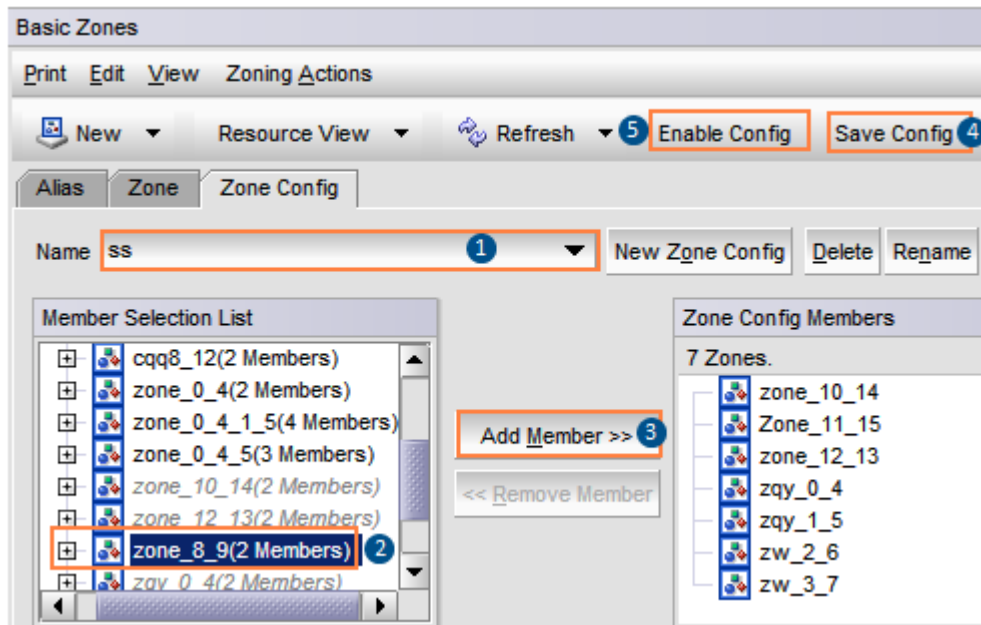
**Figure 3-48** Zone configuration



- Step 6** Add the new zone to the configuration file and activate the new zone.
1. On the **Zone Admin** page, click the **Zone Config** tab. In the **Name** drop-down list, choose the currently effective configuration **ss**.
  2. In **Member Selection List**, select zone **zone\_8\_9** and click **Add Member** to add it to the configuration file.
  3. Click **Save Config** to save the configuration and click **Enable Config** to make the configuration take effect.

Figure 3-49 shows the **Zone Config** page.

Figure 3-49 Zone Config tab page



- Step 7** Verify that the configuration takes effect.

In the navigation tree of **Web Tools**, choose **Task > Monitor > Name Server** to go to the **Name Server** page. You can also choose **Monitor > Name Server** in the navigation bar. Figure 3-50 shows the **Name Server** page.

Figure 3-50 Name Server page

Domain	...	Device Port	WWN	Device Name	WWN Company ID	Member Of Zones
1(0x1)	0	10:00:00:00:c9:64:fe:1b		Emulex LPe111-H FV2.8...	Emulex Corporation	zone_0_4_1_5, zone_12_13
1(0x1)	1	10:00:00:00:c9:64:fe:91		Emulex LPe111-H FV2.8...	Emulex Corporation	zone_0_4, zone_0_4_1_5
1(0x1)	2	20:18:36:32:33:39:38:34			2...	zw_2_6*
1(0x1)	3	20:08:36:32:33:39:38:34			2...	zw_3_7*
1(0x1)	4	20:08:00:22:a1:03:7e:bf			2...	zone_0_4, zone_0_4_1_5
1(0x1)	5	20:18:00:22:a1:03:7e:bf			2...	zone_0_4_1_5, zone_12_13
1(0x1)	6	21:01:00:1b:32:26:1c:7d			Qlogic Corp.	zw_2_6*
1(0x1)	7	21:00:00:1b:32:06:1c:7d			Qlogic Corp.	zw_3_7*
1(0x1)	8	20:09:00:22:a1:04:16:61			2...	cqq8_12, zone_8_9*
1(0x1)	9	10:00:00:00:c9:9b:5d:95			Emulex Corporation	zone_8_9*
1(0x1)	10	50:06:01:69:30:20:97:f5			0226 Clariion	Zone_10_14, zone_10_15
1(0x1)	11	50:06:01:60:30:20:97:f5			0226 Clariion	Zone_11_15*
1(0x1)	12	20:18:00:22:a1:04:16:61			2...	cqq8_12, zone_12_13*
1(0x1)	13	10:00:00:00:c9:9b:5d:94			Emulex Corporation	zone_12_13*

The preceding figure shows that ports 8 and 9 are members of **zone\_8\_9** that is now effective. An effective zone is marked by an asterisk (\*).

---End

### 3.8.2.2 Querying a Host WWPN

Before connecting a host to a storage system, check whether a host HBA can be identified (whether the driver is properly installed) and record the WWPN of the HBA's port.

#### 3.8.2.2.1 Querying the WWPN of a Host HBA's Port (Windows)

##### Prerequisites

The method used to query the WWPN of an HBA varies according to different HBA management tools. [Table 3-19](#) lists mainstream HBA management tools.

**Table 3-19** Mainstream HBA management tools

Vendor	Management Software
QLogic	SANsurfer
Emulex	OneCommand Manager
Brocade	Brocade Adapter Software
ATTO	Windows Host Adapter Utilities

Windows provides **Fibre Channel Information Tool**. The tool can be used to query HBA information. You can download the tool from Microsoft website.

Windows Server 2012 and later versions provide the **Get-InitiatorPort** command. You can use the command to query HBA information.

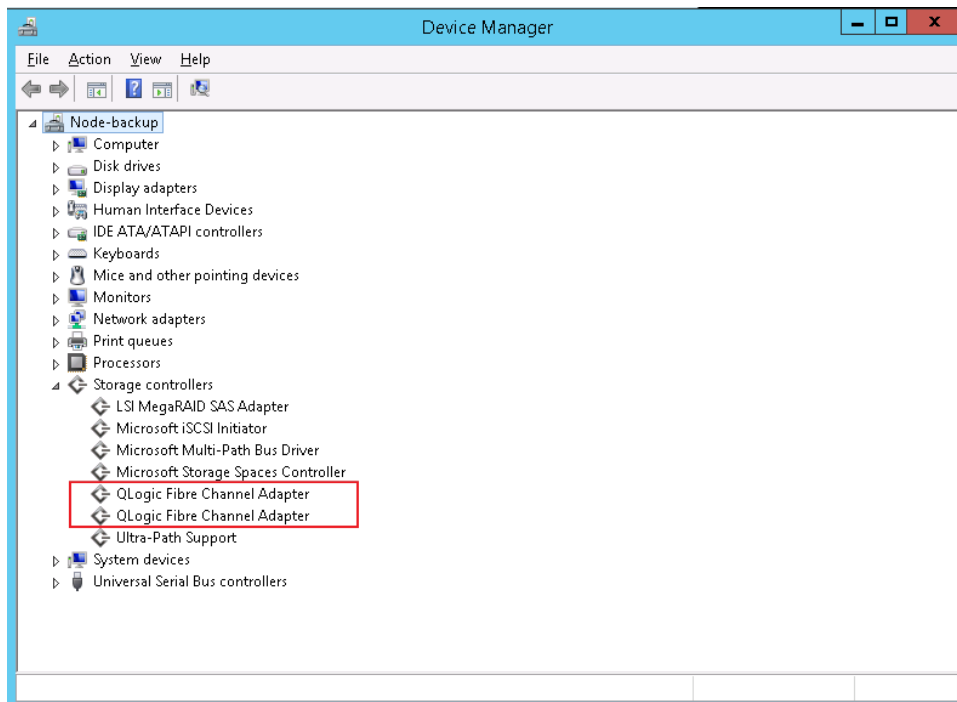
##### Procedure

**Step 1** Enable the host to identify an HBA. After an HBA is installed on the host, you can view whether the device exists in **Device Management**.

- If the device exists, the physical connection of the device is correct. Then check whether there is a question mark or exclamation mark on the device name. If there is no such mark, the driver is normal.
- If the device does not exist, check the physical connection between the HBA and the host.

If the HBA is a Fibre Channel HBA, insert the optical module. Then check whether the driver is properly installed by viewing whether light comes out from the optical module outlet.

**Figure 3-51** Checking whether the HBA is properly installed in **Device Management**

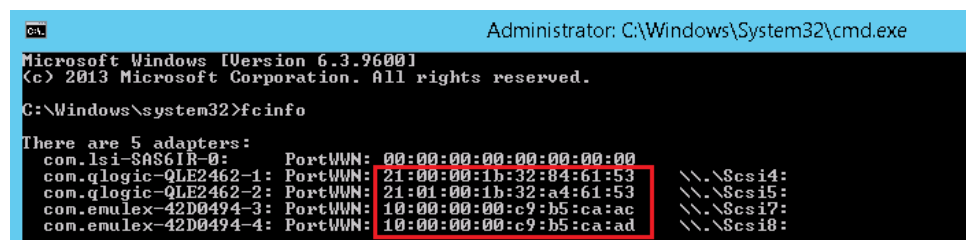


**Step 2** Query the WWPN of an HBA using either of the following methods:

- Use **Fibre Channel Information Tool** to query the WWPN of the HBA.

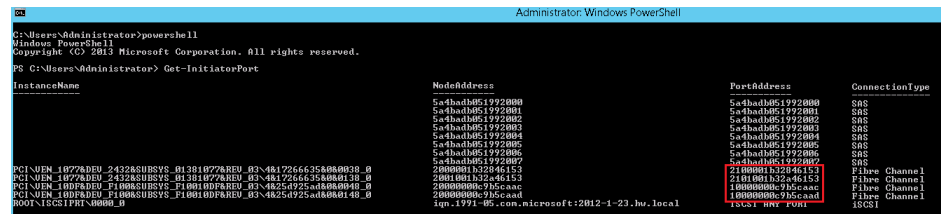
In the CMD window, enter **fcinfo** to check the WWPN of the HBA, as shown in **Figure 3-52**.

**Figure 3-52** Running the **fcinfo** command to view the HBA information



- Run the **Get-InitiatorPort** command to query the WWPN of the HBA.
  - a. In the CMD window, enter **powershell** to open the **powershell** command window.
  - b. Enter **Get-InitiatorPort** to view the WWPN of the HBA, as shown in **Figure 3-53**.

**Figure 3-53** Running the **Get-InitiatorPort** command in Windows Server 2012 to view the HBA information



----End

### 3.8.2.2.2 Querying the WWPN of a Host HBA's Port (SUSE)

This section describes how to query the WWPN of an HBA in an environment running SUSE 10 or a later version.

#### Procedure

- Step 1** Enable the host to identify an HBA. After an HBA is installed on the host, run the **lspci|grep Fibre** command on the host to check whether the host has identified the HBA.

```
# lspci|grep Fibre

03:00.0 Fibre Channel: Emulex Corporation Saturn-X: LightPulse Fibre Channel Host Adapter (rev 03)

03:00.1 Fibre Channel: Emulex Corporation Saturn-X: LightPulse Fibre Channel Host Adapter (rev 03)
```

The command output indicates that the host has identified two Fibre Channel HBAs' ports.

- Step 2** Query the WWPN of an HBA.

View the **/sys/class/fc\_host/host\*/port\_name** file to see the WWPN information about the Fibre Channel HBA.

```
# cat /sys/class/fc_host/host*/port_name

0x210000e08b907955

0x210000e08b902856
```

After the preceding command is executed, the command output shows that the WWPNs of the HBAs are **210000e08b907955** and **210000e08b902856**.

----End

### 3.8.2.2.3 Querying the WWPN of a Host HBA's Port (Red Hat)

#### Procedure

- Step 1** Enable the host to identify an HBA. After an HBA is installed on the host, run the **lspci|grep Fibre** command on the host to check whether the host has identified the HBA.

```
# lspci|grep Fibre

03:00.0 Fibre Channel: Emulex Corporation Saturn-X: LightPulse Fibre Channel Host Adapter (rev 03)
```

```
03:00.1 Fibre Channel: Emulex Corporation Saturn-X: LightPulse Fibre Channel Host
Adapter (rev 03)
```

The command output indicates that the host has identified two Fibre Channel HBAs' ports.

**Step 2** Query the WWPN of an HBA. The method used to query the WWPN varies according to different operating system versions.

- Red Hat Linux AS4

View the `/proc/scsi/qla2xxx/*` file to see the WWPN information about the Fibre Channel HBA.

 **NOTE**

Directory `/proc/scsi/qla2xxx` contains two files: files 1 and 2 or files 3 and 4. These files contain configuration information about Fibre Channel HBAs.

```
# grep scsi /proc/scsi/qla2xxx/3

Number of reqs in pending_q= 0, retry_q= 0, done_q= 0, scsi_retry_q= 0

scsi-qla0-adapter-node=20000018822d7834;

scsi-qla0-adapter-port=21000018822d7834;

scsi-qla0-target-0=202900a0b8423858;

scsi-qla0-port-0=200800a0b8423858:202900a0b8423858:0000e8:1;
```

- Red Hat Linux AS5 and later versions

View the `/sys/class/fc_host/host*/port_name` file to see the WWPN information about the Fibre Channel HBA.

```
# cat /sys/class/fc_host/host*/port_name

0x210000e08b907955

0x210000e08b902856
```

----End

### 3.8.2.2.4 Querying the WWPN of a Host HBA's Port (Solaris)

#### Procedure

**Step 1** Enable the host to identify an HBA. After an HBA is installed on the host, run the `cfgadm -al` command on the host to check whether the host has identified the HBA.

```
# cfgadm -al

Ap_Id                                     Type           Receptacle   Occupant     Condition
c0                                         scsi-bus      connected    configured   unknown
c0::dsk/c0t0d0                             CD-ROM        connected    configured   unknown
c1                                         scsi-sata     connected    configured   unknown
c1::dsk/c1t0d0                             disk          connected    configured   unknown
c1::dsk/c1t1d0                             disk          connected    configured   unknown
c1::dsk/c1t2d0                             disk          connected    configured   unknown
c1::dsk/c1t3d0                             disk          connected    configured   unknown
```



c7	<b>fc-private</b>	connected	configured	unknown
c7::2013323232323232	disk	connected	configured	unknown
c8	<b>fc-private</b>	connected	configured	unknown
c8::2003323232323232	disk	connected	configured	unknown
usb0/1	unknown	empty	unconfigured	ok
usb0/2	unknown	empty	unconfigured	ok
usb0/3	unknown	empty	unconfigured	ok
usb1/1.1	unknown	empty	unconfigured	ok
usb1/1.2	unknown	empty	unconfigured	ok
usb1/1.3	unknown	empty	unconfigured	ok
usb1/1.4	unknown	empty	unconfigured	ok
usb1/2	unknown	empty	unconfigured	ok
usb1/3	unknown	empty	unconfigured	ok
usb2/1	unknown	empty	unconfigured	ok
usb2/2	unknown	empty	unconfigured	ok
usb2/3	unknown	empty	unconfigured	ok
usb2/4	unknown	empty	unconfigured	ok
usb2/5	unknown	empty	unconfigured	ok
usb2/6	unknown	empty	unconfigured	ok
usb2/7	unknown	empty	unconfigured	ok
usb2/8	unknown	empty	unconfigured	ok

The command output indicates that two Ap\_Ids (**c7** and **c8**) are of **fc-private** type. The host operating system has identified the two Fibre Channel HBAs' ports.

**Step 2** Query the WWPN of an HBA. The method used to query the WWPN varies according to different operating system versions.

- Solaris 8/9
  - a. Obtain the name of the Fibre Channel HBA device. Run the **cfgadm -lv num** command to view the device name. In the command, *num* indicates a Fibre Channel HBA's **Ap\_Id** that has been obtained.

```
bash-3.2# cfgadm -lv c7
```

Ap_Id	Receptacle	Occupant	Condition	Information
When	Type	Busy	Phys_Id	
c7	connected	configured	unknown	
unavailable	fc-private	n		/devices/pci@1f,700000/pci@0/fibre-channel@2/fp@0,0:fc

The preceding output indicates that the complete device name of **c7** is **/devices/pci@1f,700000/pci@0/fibre-channel@2/fp@0,0:fc**.

- b. Obtain the WWPN information about the Fibre Channel HBA by running the **luxadm -e dump\_map Phys\_Id** command. In the preceding command, *Phys\_Id* indicates the Fibre Channel HBA's device name that has been obtained.

```
# luxadm -e dump_map /devices/pci@1f,700000/pci@0/fibre-channel@2/
fp@0,0:fc

Pos AL_PA ID Hard_Addr Port WWN          Node WWN          Type
0   1   7d   0       10000000c96fa382 20000000c96fa382 0x1f (Unknown
Type,Host Bus Adapter)

1    b6  1c   b6      2013323232323232 2100323232323232 0x0  (Disk
device)
```

The preceding output indicates that the WWPN of the Fibre Channel HBA is **10000000c96fa382**.

- Solaris 10, 11, and later versions

Solaris 10, 11, and later versions provide the **fcinfo** command to query HBA information.

```
bash-3.2# fcinfo hba-port

HBA Port WWN: 10000000c96fa382

    OS Device Name: /dev/cfg/c7

    Manufacturer: Emulex

    Model: LP11002-E

    Firmware Version: 2.10a10 (B2F2.10A10)

    FCode/BIOS Version: Boot:1.70a3 Fcode:none

    Serial Number: VM74944560

    Driver Name: emlxs

    Driver Version: 2.60k (2011.03.24.16.45)

    Type: L-port

    State: online

    Supported Speeds: 1Gb 2Gb 4Gb

    Current Speed: 4Gb

    Node WWN: 20000000c96fa382

HBA Port WWN: 10000000c96fa383

    OS Device Name: /dev/cfg/c8

    Manufacturer: Emulex

    Model: LP11002-E

    Firmware Version: 2.10a10 (B2F2.10A10)

    FCode/BIOS Version: Boot:1.70a3 Fcode:none

    Serial Number: VM74944560

    Driver Name: emlxs

    Driver Version: 2.60k (2011.03.24.16.45)

    Type: L-port

    State: online
```

```
Supported Speeds: 1Gb 2Gb 4Gb

Current Speed: 4Gb

Node WWN: 20000000c96fa383

bash-3.2#
```

After the preceding command is executed, the command output shows that the WWPNS of the HBAs are **1000000c96fa382** and **1000000c96fa383**.

----End

### 3.8.2.2.5 Querying the WWPN of a Host HBA's Port (AIX)

#### Procedure

**Step 1** Enable the host to identify an HBA. After the HBA is installed on the host, run the **lsdev -Cc adapter |grep fc** command on the host to check whether the host can identify the HBA.

```
# lsdev -Cc adapter |grep fc

fcs0    Available 06-00 4Gb FC PCI Express Adapter (df1000fe)

fcs1    Available 06-01 4Gb FC PCI Express Adapter (df1000fe)

fcs2    Available 05-00 8Gb PCI Express Dual Port FC Adapter (df1000f114108a03)

fcs3    Available 05-01 8Gb PCI Express Dual Port FC Adapter (df1000f114108a03)
```

After the preceding command is executed, four Fibre Channel HBAs' ports are displayed in the command output. Among them, two Fibre Channel host ports work at a rate of 4 Gbit/s and the other two at a rate of 8 Gbit/s. In addition, a physical hardware identifier such as **fcs0** that is allocated by the host to each HBA port is also displayed in the command output.

**Step 2** Query the WWPN of an HBA. After the host identifies the HBAs that have been installed, run the **lscfg -vpl fcsX** command to check the WWPN of an HBA. In the command, *fcsX* indicates a physical hardware identifier.

```
# lscfg -vpl fcs2

fcs2          U78A0.001.DNWXHBR-P1-C2-T1  8Gb PCI Express Dual Port FC
Adapter (df1000f114108a03)

Part Number.....10N9824

Serial Number.....1B0080484B

Manufacturer.....001B

EC Level.....D76482B

Customer Card ID Number.....577D

FRU Number.....10N9824

Device Specific.(ZM).....3

Network Address.....10000000C99B5D94

ROS Level and ID.....02781135

Device Specific.(Z0).....31004549
```

```

Device Specific.(Z1).....00000000
Device Specific.(Z2).....00000000
Device Specific.(Z3).....09030909
Device Specific.(Z4).....FF781110
Device Specific.(Z5).....02781135
Device Specific.(Z6).....07731135
Device Specific.(Z7).....0B7C1135
Device Specific.(Z8).....20000000C99B5D94
Device Specific.(Z9).....US1.10X5
Device Specific.(ZA).....U2D1.10X5
Device Specific.(ZB).....U3K1.10X5
Device Specific.(ZC).....000000EF
Hardware Location Code.....U78A0.001.DNWGHBR-P1-C2-T1

PLATFORM SPECIFIC

Name:  fibre-channel
      Model:  10N9824
      Node:  fibre-channel@0
      Device Type:  fcp
      Physical Location:  U78A0.001.DNWGHBR-P1-C2-T1
    
```

In the command output, the WWPN of the HBA is **10000000C99B5D94**.

----End

### 3.8.2.2.6 Querying the WWPN of a Host HBA's Port (HP-UX)

#### Procedure

- Step 1** Enable the host to identify an HBA. After an HBA is installed on the host, run the **ioscan -funC fc** command on the host to check whether the host has identified the HBA.

```

# ioscan -funC fc
Class      I  H/W Path          Driver S/W State   H/W Type   Description
=====
fc         2  0/0/0/7/0/0/0    fcd   CLAIMED        INTERFACE   HP 451871-B21 8Gb Dual
Port PCIe Fibre Channel Mezzanine (FC Port 1)
          /dev/fcd2
fc         3  0/0/0/7/0/0/1    fcd   CLAIMED        INTERFACE   HP 451871-B21 8Gb Dual
    
```

```
Port PCIe Fibre Channel Mezzanine (FC Port 2)
                                     /dev/fcd3
```

After the preceding command is executed, two Fibre Channel HBAs' ports are discovered: **/dev/fcd2** and **/dev/fcd3**.

**Step 2** Query the WWPN of an HBA. In HP-UX, the **fcmsutil** and **scsimgr** commands can be used to query the WWPN.

- Run the **fcmsutil** command to check the WWPN.

```
# fcmsutil /dev/fcd2

Vendor ID is = 0x1077
Device ID is = 0x2422
PCI Sub-system Vendor ID is = 0x103C
PCI Sub-system ID is = 0x12D6
PCI Mode = PCI-X 133 MHz
ISP Code version = 4.4.4
ISP Chip version = 3
Topology = PTTOPT_FABRIC
Link Speed = 8Gb
Local N_Port_id is = 0x011100
Previous N_Port_id is = None
N_Port Node World Wide Name = 0x50014380062fe2f5
N_Port Port World Wide Name = 0x50014380062fe2f4
Switch Port World Wide Name = 0x201100051e895ee0
Switch Node World Wide Name = 0x100000051e895ee0
N_Port Symbolic Port Name = y_fcd2
N_Port Symbolic Node Name = y_HP-UX_B.11.31
Driver state = ONLINE
Hardware Path is = 0/0/0/7/0/0/0
Maximum Frame Size = 2048
Driver-Firmware Dump Available = NO
Driver-Firmware Dump Timestamp = N/A
Driver Version = @(#) fcd B.11.31.0903 Dec 14 2008
```

- Run the **scsimgr** command to check the WWPN.

```
# scsimgr get_info -D /dev/fcd2

STATUS INFORMATION FOR SCSI CONTROLLER : /dev/fcd2
```

```
Generic Status Information

SCSI services internal state           = IDLE
Target paths probed                   = 0
Target paths registered (active/inactive) = 0
LUN paths registered                  = 0
Trace buffer size                     = 0
Port name                             = 0x50014380062fe2f4
Port id                               = 0x30200
Protocol                              = fibre_channel
I/F driver version                    = @(#) fcd B.11.31.1109 May 23
2011
Firmware version                      = 5.4.4
Operating negotiated/configured speed = 8Gb
Maximum supported speed               = 8Gb
Capability                            = "Boot Dump"
Type                                  = "Physical"
Number of I/O objects                 = 1
I/O objects :

    Object index = 0, cpu = 8
```

In the outputs of the preceding two commands, the HBA WWPN is **0x50014380062fe2f4**.

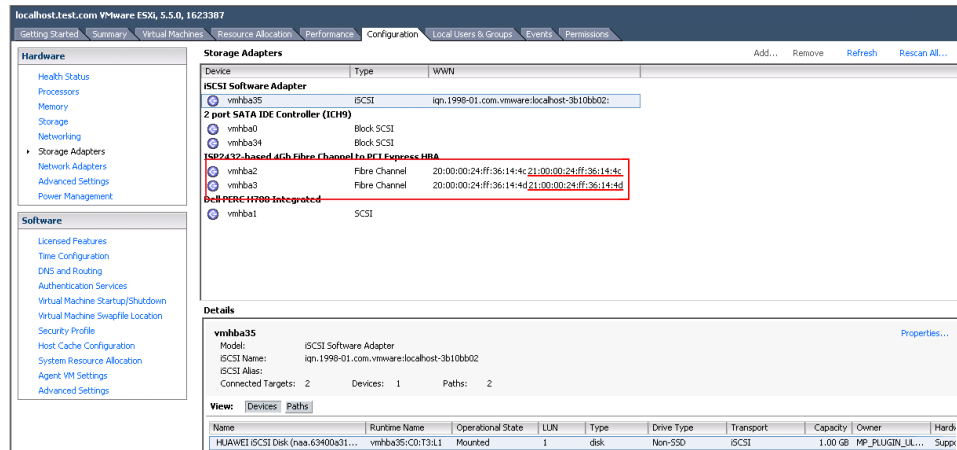
----End

### 3.8.2.2.7 Querying the WWPN of a Host HBA's Port (VMware)

#### Procedure

- Step 1** Enable the host to identify an HBA. After an HBA is installed on the host, you can check the HBA information. Go to the configuration management page and click **Storage Adapters**. In the function pane, view the HBA information, as shown in [Figure 3-54](#).

Figure 3-54 Viewing the HBA information



As shown in the preceding figure, the host has identified two Fibre Channel host ports.

**Step 2** Record the WWPNs of the HBAs. In this example, the WWPNs of the two ports are **21000024ff36144c** and **21000024ff36144d** (the WWPN is the last 16 characters).

----End

## Follow-up Procedure

You can view detailed information about HBAs on the CLI. The method for viewing HBA information varies according to different ESXi versions:

- Versions earlier than ESXi 5.5
  - QLogic HBA
 

Run the **cat /proc/scsi/qla2xxx/1 (1,2.....N)** command to check the HBA information.
  - Emulex HBA
 

Run the **cat /proc/scsi/lpfcxxx/1 (1,2.....N)** command to check the HBA information.
  - Brocade HBA
 

Run the **cat /proc/scsi/bfxxx/1 (1,2.....N)** command to check the HBA information.
- ESXi 5.5 and later versions
 

Run the **esxcli storage core adapter list** and **esxcfg-module -i qlnativefc** commands to check the HBA information. *qlnativefc* indicates the HBA driver that is queried by running the **esxcli storage core adapter list** command.

### 3.8.2.3 (Optional) Setting Fibre Channel Port Information

Configure Fibre Channel port parameters to ensure proper communication between the storage system and application server.

## Prerequisites

The HBA information, including the HBA identifier and speed, has been obtained on the application server.



## Context

Note the following when you set Fibre Channel ports:

- If the storage device connects to an application server through a Fibre Channel port, ensure that the rate of the Fibre Channel port on the storage device is the same as that of the peer host bus adapter (HBA) port on the application server.
- When two storage devices connect to each other through Fibre Channel ports, ensure that the rates of the Fibre Channel ports on both storage devices are the same.

## Procedure

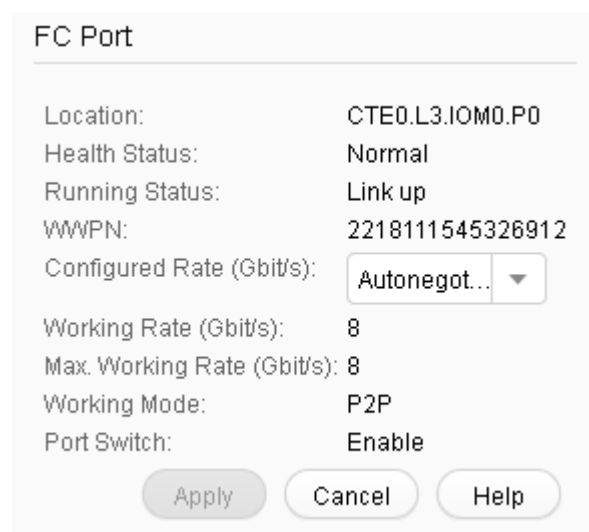
**Step 1** Go to the **FC Port** dialog box.

1. On the right navigation bar, click  **System**.
2. Click the controller enclosure where the Fibre Channel port resides.
3. Click  to switch to the rear view.
4. Click the Fibre Channel port whose information you want to modify.  
The **FC Port** dialog box is displayed.

**Step 2** Click **Modify**.

**Step 3** In **Configured Rate (Gbit/s)**, select a data transfer rate for the Fibre Channel port.

**Figure 3-55** FC Port



FC Port	
Location:	CTE0.L3.IOM0.P0
Health Status:	Normal
Running Status:	Link up
WWPN:	2218111545326912
Configured Rate (Gbit/s):	Autonegot... ▼
Working Rate (Gbit/s):	8
Max. Working Rate (Gbit/s):	8
Working Mode:	P2P
Port Switch:	Enable
Apply Cancel Help	



---



## NOTICE

- The rate and mode of the Fibre Channel port on a storage system must be consistent with those of the Fibre Channel HBA on the peer application server. If the rates and modes are inconsistent, the communication will fail.
- The rate and mode of the Fibre Channel ports on two storage systems that are connected to each other must be consistent. If the rates and modes are inconsistent, the communication will fail.

---

Available rates of a Fibre Channel port are **2 Gbit/s**, **4 Gbit/s**, **8 Gbit/s**, **16 Gbit/s**, and **Autonegotiation**. Select a fixed value after learning the rate of the peer Fibre Channel port.



### NOTE

- If the configured maximum rate of a port is 8 Gbit/s, you can set the value to be **2 Gbit/s**, **4 Gbit/s**, or **8 Gbit/s**.
- If the configured maximum rate of a port is 16 Gbit/s, you can set the value to be **4 Gbit/s**, **8 Gbit/s**, or **16 Gbit/s**.
- The system selects **Autonegotiation** by default. The rate of the Fibre Channel port on the storage system automatically becomes the same as that on the host.

#### Step 4 Confirm the Fibre Channel port configuration.

1. Click **OK**.  
The **Danger** dialog box is displayed.
2. Confirm the information in the dialog box and select **I have read and understood the consequences associated with performing this operation..**
3. Click **OK**.  
The **Success** message box is displayed, indicating that the operation succeeded.
4. Click **OK**.

----End

## 3.8.3 FCoE Networking

This section introduces how to establish FCoE connections.

### 3.8.3.1 Configuring FCoE Switches

FCoE protocol allows Fibre Channel frames to be transmitted over Ethernet. In an FCoE solution, Ethernet cards and FCoE Forwarder (FCF) switches that support the FCoE protocol are used to achieve I/O consolidation. FCF switches replace the traditional Ethernet switches and Fibre Channel switches, greatly reducing the number of NICs, switches, and cables, alleviating maintenance workload, and cutting the TCO. This section introduces how to configure FCoE switches.

#### Prerequisites

- FCoE interface modules (four-port) or SmartIO interface modules are connected to the storage systems.

 **NOTE**

SmartIO interface modules support three modes: FC, FCoE/iSCSI, and Cluster. When SmartIO interface modules are set to FCoE mode, the corresponding switches must be set to Intel DCBX (CEE) mode because FCoE only supports Intel DCBX (CEE) mode. For details about how to confirm and modify the mode, see the product documentation of switches. When SmartIO interface modules are set to FCoE mode, the networking is the same as four-port FCoE interface modules.

- FCoE converged network adapters (CNAs) or Fibre Channel HBAs are connected to servers.

## Context

To implement lossless Ethernet on a converged data center network, both ends of an FCoE link must have the same priority-based flow control (PFC) and enhanced transmission selection (ETS) parameter settings. Data Center Bridging eXchange (DCBX), as a link discovery protocol, enables DCB devices at both ends of a link to discover and exchange DCB configurations, reducing workloads of administrators. Two standards are available for DCBX protocol: IEEE DCBX and Intel DCBX. When a switch connects to a different manufacturer's device, the two devices must use the same DCBX version. Otherwise, DCBX negotiation fails.

The following uses a Cisco Nexus 5010 FCoE switch as an example to introduce how to configure FCoE switches.

## Procedure

### Step 1 Enable FCoE on the switch.

```
configure terminal
feature fcoe
exit
```

After the configuration is complete, run the following command to verify the configuration:

```
show fcoe
```

### Step 2 Configure 10GE ports.

```
configure terminal
interface ethernet 1/1
switchport mode trunk
spanning-tree port type edge trunk
no flowcontrol receive
no flowcontrol send
priority-flow-control mode auto
exit
```

After the configuration is complete, run the following command to verify the configuration:

```
show interface ethernet 1/1
```

### Step 3 Create a VFC interface and bond it to the corresponding 10GE port.

```
configure terminal
interface vfc 1
bind interface ethernet 1/1
no shutdown
exit
```

After the configuration is complete, run the following command to verify the configuration:

```
show interface vfc 1
```

### Step 4 Create a VSAN.

A SAN network is segmented into multiple logical SAN networks (VSAN). Each VSAN is separated from each other and provides services independently, enhancing network adaptability and security with more efficient services.

```
configure terminal
vsan database
vsan 100
exit
```

After the configuration is complete, run the following command to verify the configuration:

```
show vsan 100
```

**Step 5** Create an FCoE VLAN and map it to a VSAN.

```
configure terminal
vlan 100
fcoe vsan 100
exit
```

After the configuration is complete, run the following command to verify the configuration:

```
show vlan fcoe
```

**Step 6** Add a 10GE port to the VLAN.

```
configure terminal
interface ethernet 1/1
switchport trunk allowed vlan 100
exit
```

After the configuration is complete, run the following command to verify the configuration:

```
show vlan
```

**Step 7** Add a VFC port to the corresponding VSAN.

```
configure terminal
vsan database
vsan 100 interface vfc 1 (vsan 100 interface fc1/43)
exit
```

After the configuration is complete, run the following command to verify the configuration:

```
show vsan membership
```

---End

### 3.8.3.2 Configuring Zones

A VSAN is further divided into zones. Different N\_Ports (from servers or storage systems) are added to the zones for different purposes. N\_Ports in different zones are separated for access control.

#### Prerequisites

A VSAN has been created.



If the host port and the storage port cannot reside in the same zone, you are advised to configure the zone in a way that high-throughput services (such as backup services) and real-time services are isolated during network configuration to avoid impacts on real-time services caused by bandwidth preemption.

---

## Context

- A zoneset is a group of zones. A zone consists of zone members. Each member is an N\_port. An N\_port member can be identified by its PWWN (the WWN of an N\_port) and FC address.
- A VSAN can have many zonesets. A zoneset can contain many zones. A zone can have many zonemembers.
- However, a VSAN can only have one active zoneset at a time.
- A zone member should not belong to multiple zones.

## Procedure

### Step 1 Create a zoneset.

```
configure terminal
zoneset name zoneset100 vsan 100
exit
```

After the configuration is complete, run the following command to verify the configuration:

```
show zoneset
```

### Step 2 Create a zone.

```
configure terminal
zone name zone100 vsan 100
exit
```

After the configuration is complete, run the following command to verify the configuration:

```
show zone
```

### Step 3 Add the zone to the zoneset.

```
configure terminal
zoneset name zoneset100 vsan 100
member zone100
exit
```

After the configuration is complete, run the following command to verify the configuration:

```
show zoneset
```

### Step 4 Add members (N\_Ports) to the zone.

```
configure terminal
zone name zone100 vsan 100
member interface fc2/1
member pwn hh:hh:hh:hh:hh:hh:hh:hh
exit
```

After the configuration is complete, run the following command to verify the configuration:

```
show zone
```

### Step 5 Activate the zoneset.

```
configure terminal
zoneset activate name zoneset100 vsan 100
exit
```

After the configuration is complete, run the following command to verify the configuration:

```
show zoneset activate
```

----End

## 3.9 Creating a Host

Create a host to establish a connection between a storage system and an application server, and add an initiator for the host to establish a mapping relationship between the host and application server.

### 3.9.1 Automatically Scanning for a Host

You can add hosts to a host list by automatically scanning for hosts to save your time.

#### Prerequisites

- Hosts have the UltraPath installed. Multipathing software provided with host operating systems is not supported.
- In an iSCSI networking environment, initiators have been configured for hosts to connect to the storage system.
- In an FC networking environment, the HBA port of a host and the port of the storage system are in the same zone.

#### Context

By default, automatic host scan is not enabled. If no hosts are found after the scan is complete, scan for disks on application servers and retry.

#### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Host**.

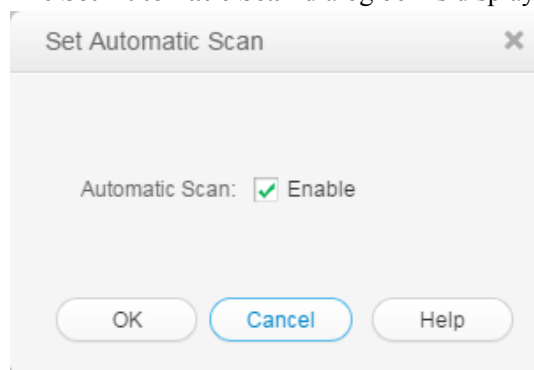
**Step 3** **Optional:** Enable automatic host scan.

#### NOTE

- If automatic host scan is enabled, skip this step.
- If the storage system automatically detects a host initiator and the initiator has not been added to any host, a 16 KB virtual disk is displayed on the host operating system. After the initiator is added to a host, the virtual disk disappears.

1. Click **Parameter Settings**.

The **Set Automatic Scan** dialog box is displayed.



2. Select **Enable** and click **OK**.  
The **Execution Result** dialog box is displayed indicating that the operation succeeded.
3. Click **OK**.

**Step 4** Choose **Create > Automatic Scan**.  
The **Confirm** dialog box is displayed.

**Step 5** Click **OK**.  
The system starts scanning for hosts. Detected hosts will be added to the host list.

**Step 6** Click **Close**.

----End

## 3.9.2 Manually Creating a Host

You can manually create a virtual host for a storage device.

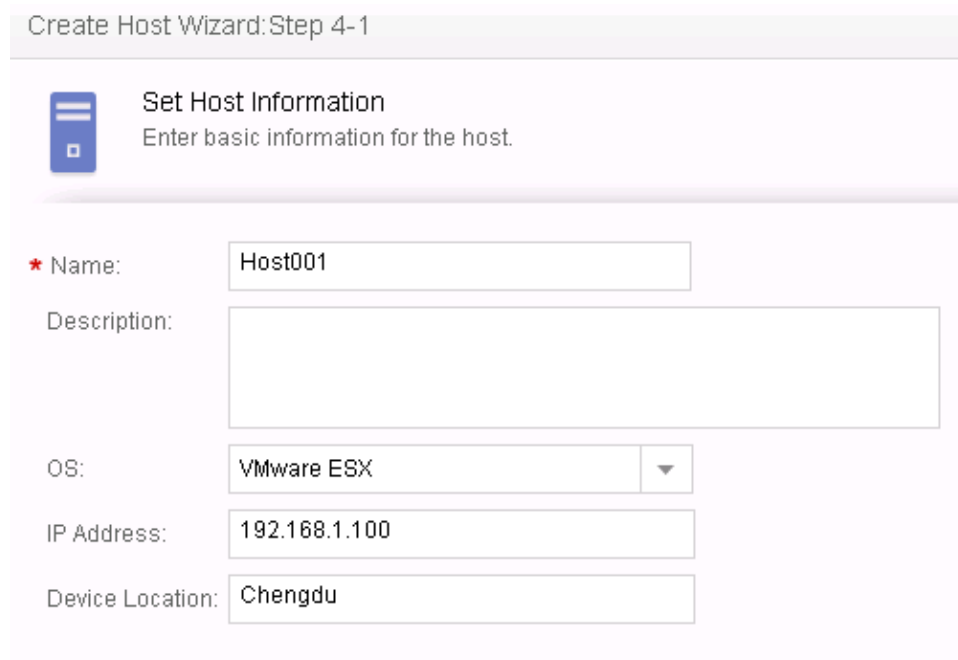
### Procedure

**Step 1** Log in to DeviceManager.


**Step 2** Choose  **Provisioning** >  **Host**.

**Step 3** Choose **Create > Manually Create**.  
The **Create Host Wizard** dialog box is displayed.

**Step 4** Set basic information for the host.



Create Host Wizard: Step 4-1

 **Set Host Information**  
Enter basic information for the host.

\* Name:

Description:

OS:

IP Address:

Device Location:

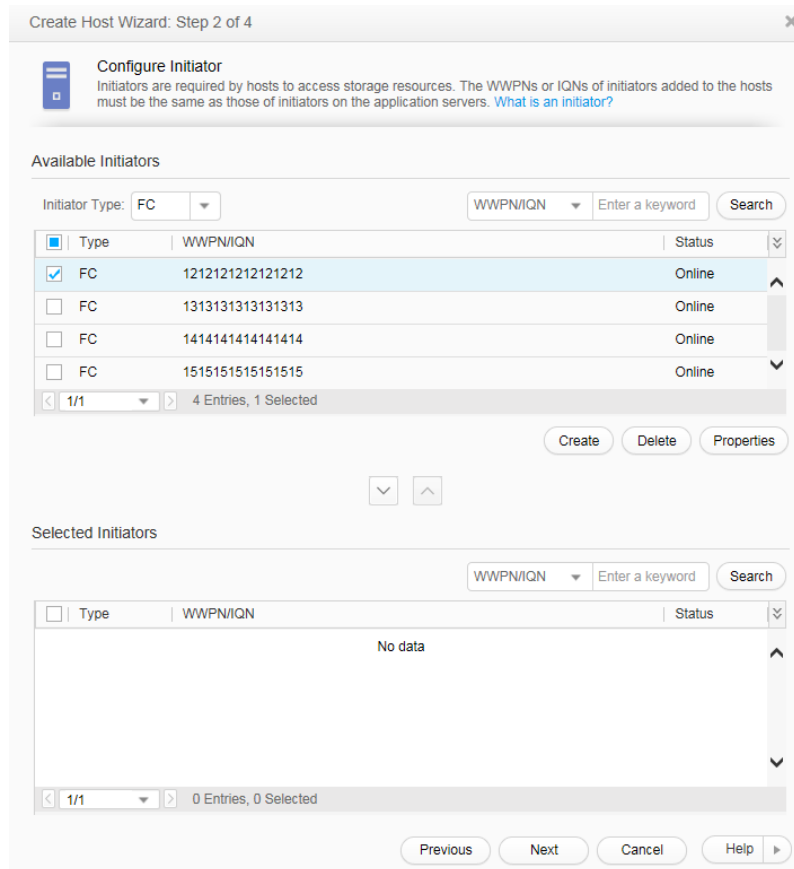
**Table 3-20** describes related parameters.


**Table 3-20** Host parameters

Parameter	Description	Setting
Name	Name of a host.	[Value range] <ul style="list-style-type: none"> <li>● The name must be unique.</li> <li>● The name can contain only letters, digits, periods (.), underscores (_), and hyphens (-).</li> <li>● The name contains 1 to 31 characters.</li> </ul> [Example] <b>Host001</b>
Description	Description of a host.	[Example] -
OS	Operating system used by a host. <b>NOTE</b> The selected operating system must be the same type of host operating system that the storage system is connected to.	[Value range] Possible values are <b>Linux, Windows, Windows Server 2012, Solaris, HP-UX, AIX, XenServer, Mac OS, VMware ESX, Oracle VM, and OpenVMS.</b> <b>NOTE</b> <ul style="list-style-type: none"> <li>● If the host runs the Windows operating system and you need to use the space reclaiming function of thin LUNs, you can only select Windows Server 2012.</li> <li>● If the application type is FusionCompute, you are advised to select <b>Linux</b> as the operating system.</li> </ul> [Example] <b>VMware ESX</b>
IP Address	IP address of a host.	[Example] <b>192.168.1.100</b> <b>NOTE</b> If the host is connected through iSCSI links, enter the real service IP address of the host for further management and search.
Device Location	Location of a host.	[Example] <b>Chengdu</b>

**Step 5** Click **Next**.

### Step 6 Configure an initiator for the host.



1. In the **Available Initiators** area, select **Initiator Type** based on your service needs.
2. In the initiator list, select one or multiple initiators.
3. Click  to add the initiator to the **Selected Initiators** area.

#### **NOTE**

- If the initiator information has been configured on the application server, the DeviceManager can automatically detect the configured initiator. You only need to select the initiator information from the initiator list rather than manually creating it, and do not add initiators on different application servers to a same host. Create an initiator if none is available in the list.
- If the host operating system is **HP-UX**, create an initiator manually.
- If the CHAP authentication is not enabled on the initiator, click **Modify**. In the **Modify Initiator** dialog box that is displayed, configure the CHAP authentication parameters.
- If the CHAP authentication has been enabled on the initiator and you want to change the CHAP authentication password, click **Modify**. In the **Modify Initiator** dialog box that is displayed, change the CHAP authentication password. When you change the CHAP authentication password, you need to enter **Old password** to improve the storage system security instead of directly changing the password.
- The CHAP authentication user name and password configured on the storage system must be the same as those configured on the application server. After changing the CHAP authentication password on the storage system, you need to use the new password to configure the CHAP authentication again on the application server.

### Step 7 Confirm the host creation.

1. Click **Next**.



The **Summary** page is displayed.

2. Click **Finish** to confirm the information of the host to be created.  
If you already added initiators to the host, execute [Step 7.3](#). If you do not add any initiator to the host, execute [Step 7.4](#).
3. The security alert dialog box is displayed. Carefully read the content of the dialog box. Then select **I have read and understood the consequences associated with performing this operation.** to confirm the information and click **OK**.
4. The **Execution Result** page is displayed, indicating that the operation succeeded. Click **Close** to finish creating a host.

---End

### 3.9.3 Batch Creating Hosts

This operation enables you batch create virtual hosts for storage devices.

#### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Host**.

**Step 3** Choose **Create** > **Batch Create**.

The **Batch Create Host** dialog box is displayed.

**Step 4** Set basic information about the host.  
[Table 3-21](#) describes related parameters.

**Batch Create Host** [X]

\* Name:

Description:

OS:  ▼

Device Location:

\* Quantity:

A maximum of 500 hosts can be created at a time. When you create multiple hosts, the system automatically appends a suffix number to each host name for host distinction. You can also specify the suffix by yourself.

Manually specify the suffix

OK Cancel Help

**Table 3-21** Host parameters

Parameter	Description	Value
Name	Name of the host.	[Value range] <ul style="list-style-type: none"> <li>● Must be unique.</li> <li>● Contains only letters, digits, underscores (_), periods (.), and hyphens (-).</li> <li>● Contains 1 to 31 characters.</li> </ul> [Example] Host001
Description	Description of the host.	[Example] -

Parameter	Description	Value
OS	Operating system of the host. <b>NOTE</b> The selected operating system must be the same type of host operating system that the storage system is connected to.	[Value range] Possible values are <b>Linux, Windows, Windows Server 2012, Solaris, HP-UX, AIX, XenServer, Mac OS, and VMware ESX, Oracle VM and OpenVMS.</b> <b>NOTE</b> <ul style="list-style-type: none"> <li>● If the host runs the Windows operating system and you need to use the space reclaiming function of thin LUNs, you can only select Windows Server 2012.</li> <li>● If the application type is FusionCompute, you are advised to select <b>Linux</b> as the operating system.</li> </ul> [Example] Windows
Device Location	Location of the host.	[Example] Chengdu
Quantity	Number of hosts to be created.	[Value range] 1 to 500 <b>NOTE</b> <ul style="list-style-type: none"> <li>● A maximum of 500 hosts can be created at a time.</li> <li>● When creating multiple hosts, the system automatically appends a number to host names for distinction. You can manually append numbers to host names.</li> </ul>

**Step 5** Click **OK**.

In the **Execution Result** dialog box that is displayed, click **Close**. You have finished batch creating hosts.

----End

## 3.10 Creating a Host Group

To allow hosts to use LUNs, you must add hosts into host groups. Then, establish mapping views between the LUN groups and host groups. By doing so, the hosts in the host groups can use the LUNs in the LUN groups. A host group can contain one or multiple hosts.

### Context

- Hosts in a host group can run different operating systems.

- A host group can include a maximum of 64 hosts.
- A host can be added to a maximum of 64 host groups.

## Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Host** > **Host Group**.

**Step 3** Click **Create**.

The **Create Host Group** dialog box is displayed.

**Step 4** Set parameters of the host group. [Table 3-22](#) describes related parameters.

**Table 3-22** Host group parameters

Parameter	Description	Setting
Name	Name of a host group.	[Value range] <ul style="list-style-type: none"> <li>● The name must be unique.</li> <li>● The name can contain only letters, digits, periods (.), underscores (_), and hyphens (-).</li> <li>● The name contains 1 to 31 characters.</li> </ul> [Example] <b>HostGroup001</b>
Description	Description of a host group.	[Example] -

**Step 5** Select the hosts you want to add to the host group.

1. In the **Available Hosts** area, select one or multiple hosts based on your service requirements.

---

### NOTICE

If hosts to be added into the host group belong to different clusters, data access conflicts may occur, resulting in data loss. Before this operation, you are advised to install cluster software to manage hosts.

---

### NOTE

By default, the **Shows only the hosts that do not belong to any host group** checkbox in the bottom left corner of the dialog box is selected to facilitate host locating.

2. Click  to add the hosts to the **Selected Hosts** area.

**Step 6** Confirm the creation of the host group.

1. Click **OK**.
  - If multiple hosts have been selected to add to a host group, a security alert dialog box is displayed. Confirm the information and click **OK**. The **Execution Result** dialog box is displayed, indicating that the operation succeeded.
  - If only one host has been selected to add to a host group, the **Execution Result** dialog box is displayed, indicating that the operation succeeded.
2. Click **Close**.

----End

### 3.11 (Optional) Creating a Port Group

A port group is a logical combination of multiple physical ports. The storage system specifies ports to set up mappings between storage resources (LUNs) and servers. This operation enables you to create a port group and add it to a mapping view. After that, LUNs of a specified LUN group use the ports of the port group to communicate with the corresponding hosts of the host group. If no port group is added to the mapping view, available ports are randomly used. A port group can be added to a maximum of 64 mapping views. A port can be added to a maximum of 64 port groups.

#### Procedure

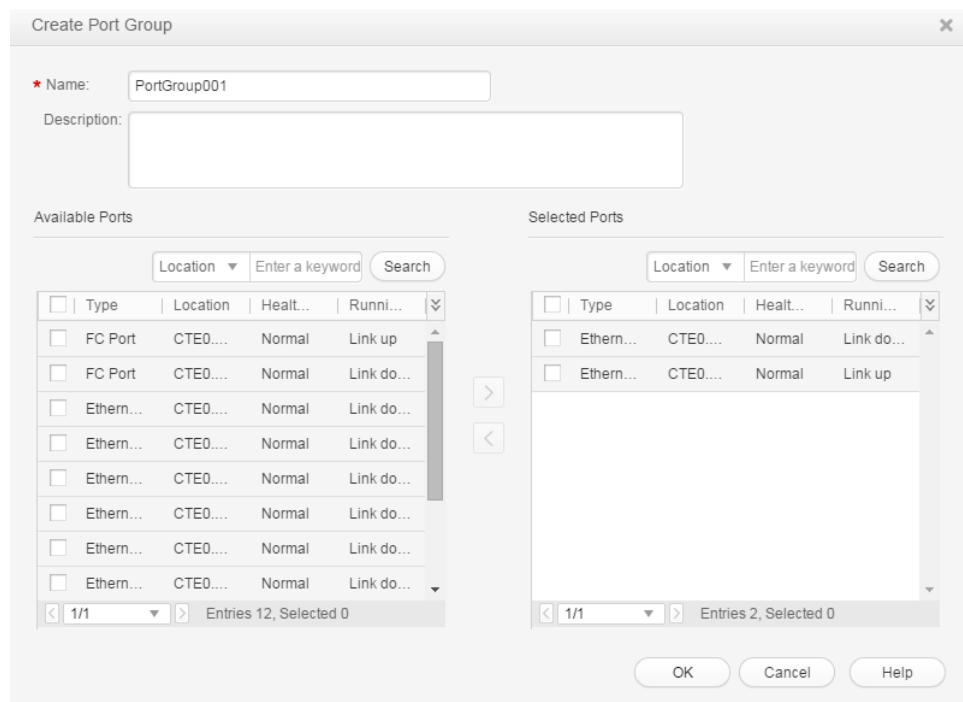
**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Port** > **Port Groups**.

**Step 3** Click **Create**.

The **Create Port Group** message box is displayed.

**Step 4** Set parameters of the port group. [Table 3-23](#) describes related parameters.



**Table 3-23** Port group parameters


Parameter	Description	Setting
Name	Name of a port group. Name a port group in accordance with the following rules so that the port group is available to host applications: <ul style="list-style-type: none"><li>● The name must be unique.</li><li>● The name can contain only letters, digits, periods (.), underscores (_), and hyphens (-).</li><li>● The value contains 1 to 31 characters.</li></ul>	[Example] <b>PortGroup001</b>
Description	Description of a host group.	[Example] <b>None</b>

**Step 5** Select the ports you want to add to the port group.

1. Select the ports you want to add to the port group in **Available Ports** list.



One port can be added to different port groups.

2. Click  and add the ports to **Selected Ports**.

**Step 6** Confirm your operation.

1. Click **OK**.  
The **Execution Result** message box is displayed, indicating that the operation succeeded.
2. Click **Close**.

----End

## Result

On the **Port Groups** page, the newly created port group is displayed in the port group list.

## 3.12 Creating a Mapping View

This operation enables you to create a mapping view and manage the mapping relationship between multiple host groups and LUN groups by adding them to the mapping view.

### Context

- A host group can be added to a maximum of 64 mapping views.
- A LUN group can be added to a maximum of 64 mapping views.
- A port group can be added to a maximum of 64 mapping views.

Based on the ports used by mapping views, mapping views can be classified into LUN masking and LUN mapping.

- LUN masking: A LUN is bound with the WWPN or IQN of a host port to establish a one-to-one or N-to-one connection and access relationship with the host port. A host can identify the same LUN regardless of whichever port on the storage system is connected to the host.
- LUN mapping: A LUN is bound with a front-end port on the storage system. The LUN that a host can access varies with the storage port connected to the host.

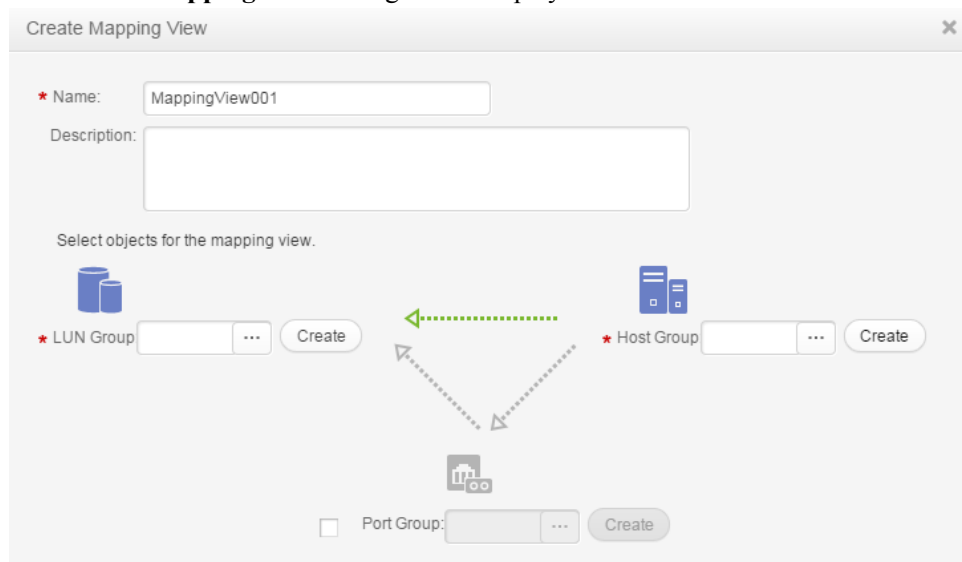
## Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Mapping View**.

**Step 3** Click **Create**.

The **Create Mapping View** dialog box is displayed.



**Step 4** Set basic properties for the mapping view.

1. In the **Name** text box, enter a name for the mapping view.
2. **Optional:** In the **Description** text box, add the mapping view description.

**Step 5** Add a host group to the mapping view.

1. In **Host Group**, click .
- The **Select Host Group** dialog box is displayed.

### **NOTE**

1. If the service requires a new host group, click **Create** to create one.
2. From the host group list, select the host group you want to add to the mapping view.
3. Click **OK**.

**Step 6** Add a LUN group to the mapping view.

1. In **LUN Group**, click .

The **Select LUN Group** dialog box is displayed.

 **NOTE**

- If the service requires a new LUN group, click **Create** to create one.
- By default, the **Show only the LUN groups that do not belong to any mapping view** checkbox in the bottom left corner of the dialog box is selected to facilitate LUN group locating.

2. **Optional:** Select **Set host LUN ID**. In **Start ID**, select an ID.

 **NOTE**

- A host LUN ID is an ID allocated by the storage system to a LUN mapped to a host.
- Starting from the selected ID, the system will automatically assign a unique host LUN ID to each LUN in the selected LUN group.
- If you do not select **Set host LUN ID** and there is no other mapped LUN in the host, the system will automatically assign a unique host LUN ID (starting from 0) to each LUN in the selected LUN group by default.

3. From the LUN group list, select the LUN group you want to add to the mapping view.
4. Click **OK**.

**Step 7 Optional:** Add a port group to the mapping view.

 **NOTE**

This operation is required if the mapping view type is port mapping.

1. Select **Port Group**

 **NOTE**

If a port group is added to the mapping view, LUNs of a specified LUN group use the ports of the port group to communicate with the corresponding hosts of the host group. If no port group is added to the mapping view, available ports are randomly used.

2. Click .

The **Select Port Group** dialog box is displayed.

 **NOTE**

If your service requires a new port group, click **Create** to create one.

3. From the port group list, select the port group you want to add to the mapping view.
4. Click **OK**.

**Step 8** Confirm the creation of the mapping view.

1. Click **OK**.

The security alert dialog box is displayed.

 **NOTE**

If multiple hosts are added to one same mapping view, it is possible that multiple hosts write data to the same LUN, this may cause data damage or inconsistent. You are advised to install cluster management software on application servers.

2. Carefully read the content of the dialog box. Then 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



## 3.13 Configuring LUN Mapping Using a Cipher Machine

Use a cipher machine to configure mapping relationships between application servers and LUNs to keep critical services running in an encrypted environment. If no cipher machine is available, skip this section.

### Prerequisites

A cipher machine has been started and initially configured.

### Context

The cipher machine can detect and encrypt LUNs and hosts, and configure mapping relationships between LUNs and hosts. You can export information about all encrypted LUNs.

### Procedure

- Use a cipher machine to configure mapping relationships between LUNs and hosts. For details, see *Cipher Machine User Guide*.

---End

## 3.14 Making Storage Space Available

After a connection is established between a storage system and an application server, the application server must discover the newly-added logical disk (that is, the storage space specified by a mapped LUN) to use it as a common disk for data reads and writes.

### Prerequisites

Note the following before using the LUN:

- The application server is communicating properly with the storage system.
- The planned storage capacity has been allocated to the application server.
- Multipathing software is installed when redundant paths exist between the application server and storage system. This prevents multiple LUNs from being repetitively mapped to the host.

#### NOTE

Check whether multipathing software is installed on the application server. If no multipathing software is installed, install a compatible multipathing program immediately by referring to the corresponding product manual.

### Precautions

When LUNs provide storage space for SQL Server databases, you can adjust relevant parameters to reduce the I/O latency and achieve the optimal performance. For details, see [8.1 In the SQL Server database scenario, how can I adjust parameters to reduce the I/O latency and achieve the optimal performance?](#)

Note the following when using the storage space of application servers:

- Do not allocate disks in use to other applications. Otherwise, data security will be compromised.
- If a host login error occurs, operations on disks affect the running of applications.
- If storage incompatibility occurs, application servers cannot stably use storage space.

## Context

The maximum LUN capacity that can be identified by an application server varies according to the operating system and file system used by the application server. **Table 3-24** lists the maximum LUN capacity supported by various operating systems.

**Table 3-24** Maximum LUN capacity supported by various operating systems

Operating System	File System	Maximum Allowed LUN Capacity
Windows Server 2003	New Technology File System (NTFS)	2 TB <b>NOTE</b> If a LUN mapped to a Windows Server 2003-based application server is larger than 2 TB, convert it into a GUID Partition Table (GPT) disk.
Windows Server 2003 SP1 and later	NTFS	256 TB
Windows XP 32-bit	NTFS	2 TB
Windows XP 64-bit	NTFS	256 TB
Windows Server 2008	NTFS	256 TB
Windows 7	NTFS	256 TB
SUSE Linux Enterprise Server	EXT3/ReiserFS/XFS	16 TB/16 TB/8 EB
Red Hat Enterprise Linux 5	EXT3/XFS	16 TB/100 TB
Red Hat Enterprise Linux 6	EXT3/EXT4/XFS	16 TB/16 TB/100 TB

 **NOTE**

Plan the capacity of a LUN before mapping it to an application server. If the maximum allowed capacity is exceeded, the application server fails to identify it.

### 3.14.1 Making Storage Space Available (Windows)

This section describes how to enable a Windows-based application server to use the space of a storage system.

## Context

A GPT disk is partitioned using the GPT scheme. The GPT scheme provides more advantages than the traditional Master Boot Record (MBR) partitioning scheme. GPT allows each disk to have 128 partitions and supports a maximum of 18 EB (1 EB = 1024 PB = 1,048,576 TB) disk capacity, whereas MBR allows each disk to have only four main partitions and supports only a maximum of 2 TB disk capacity. Therefore, if a LUN mapped to a host is larger than 2 TB, it is available only after being converted into a GPT disk.

The storage system supports Multi-Path I/O (MPIO) and UltraPath. UltraPath is recommended.

- If you want to use MPIO, you must install or enable the MPIO components.
- If you use UltraPath, see your UltraPath document.

## Windows Server 2003 and Earlier Versions

Windows Server 2003 and earlier versions use the same method to enable an application server to use the space of a storage system. This section uses Windows Server 2003 as an example to describe how to enable an application server to use the space of a storage system.

**Step 1** Log in to the Windows-based application server as **administrator**.

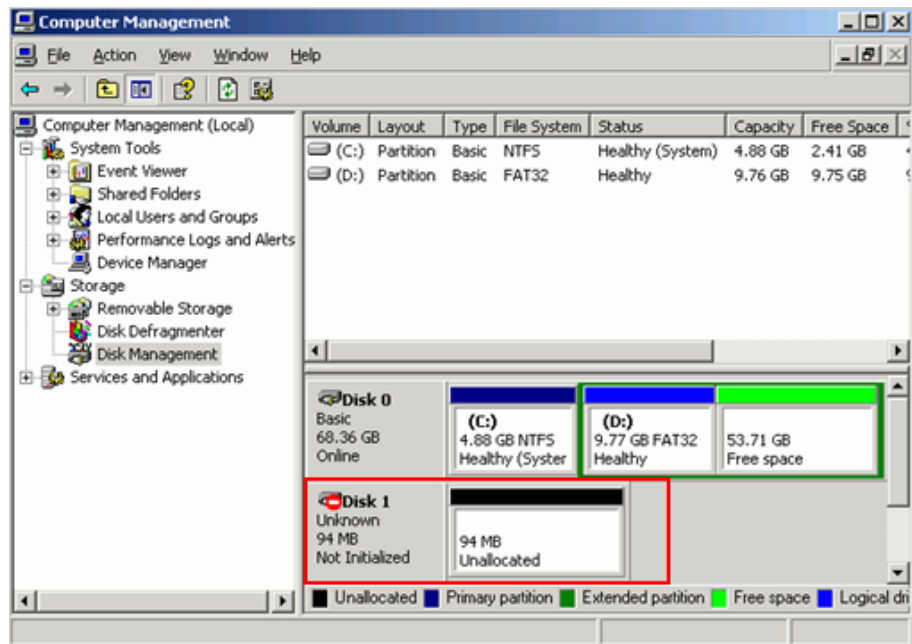
**Step 2** Go to the **Computer Management** dialog box.

Right-click the icon of **My Computer** on the desktop and choose **Manage** from the shortcut menu.

**Step 3** In the navigation tree, choose **Disk Management** and scan for new logical disks.

1. In the navigation tree on the left of the **Computer Management** dialog box, choose **Storage > Disk Management**.
2. Right-click **Disk Management** and choose **Rescan Disks** from the shortcut menu.
  - After the scan is complete, the new logical disk is displayed in the right area (using Disk 1 as an example), as shown in **Figure 3-56**. The display varies according to the disk size.

Figure 3-56 Querying the new logical disk



- If no new logical disk is detected, perform the following steps:
  - i. In the navigation tree, choose **Device Manager** > **Disk drives**.
  - ii. Right-click **Disk drives** and choose **Scan for hardware changes** from the shortcut menu.
  - iii. After the scan is complete, rescan for logical disks.

**NOTE**

If no new logical disk is detected, troubleshoot the fault and rescan for logical disks. Possible faults include:

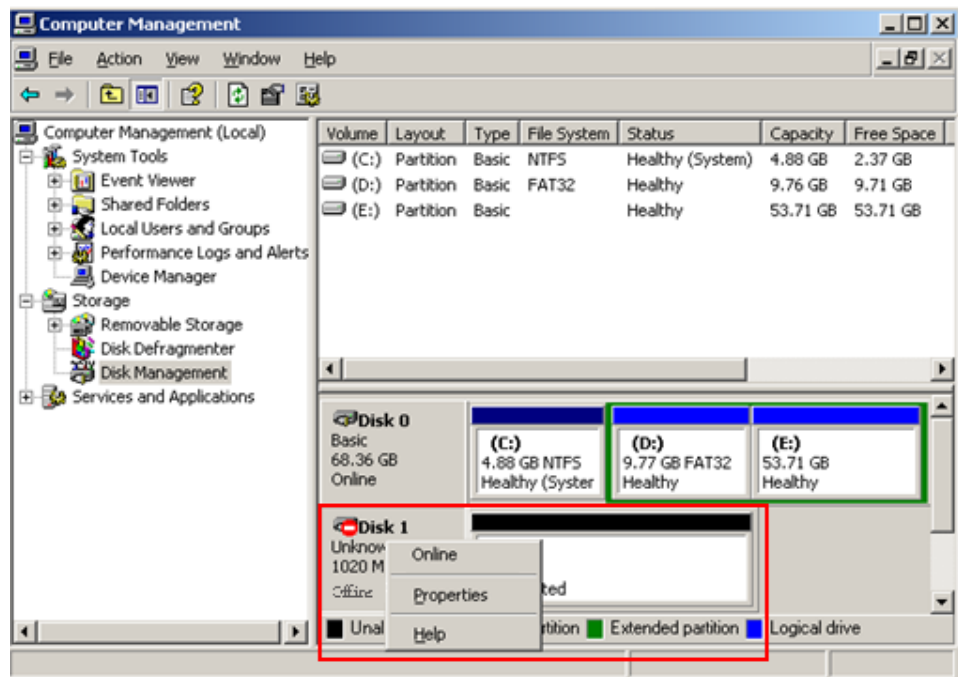
- The application server is incorrectly connected to the storage system after the network cable has been removed and reinserted.
- The link between the application server and storage system is down.
- The rate of the Fibre Channel host port is inconsistent with that of the Fibre Channel HBA on the application server.
- The HBA driver has been uninstalled.
- The storage pool fails.
- Multipathing software is not installed or an incorrect version is installed.
- The device file on the application server is lost.

For details, see **Failure to Discover LUNs by an Application Server** in the *OceanStor V3 Series V300R006 Troubleshooting*.

**Step 4** Initialize the logical disk.

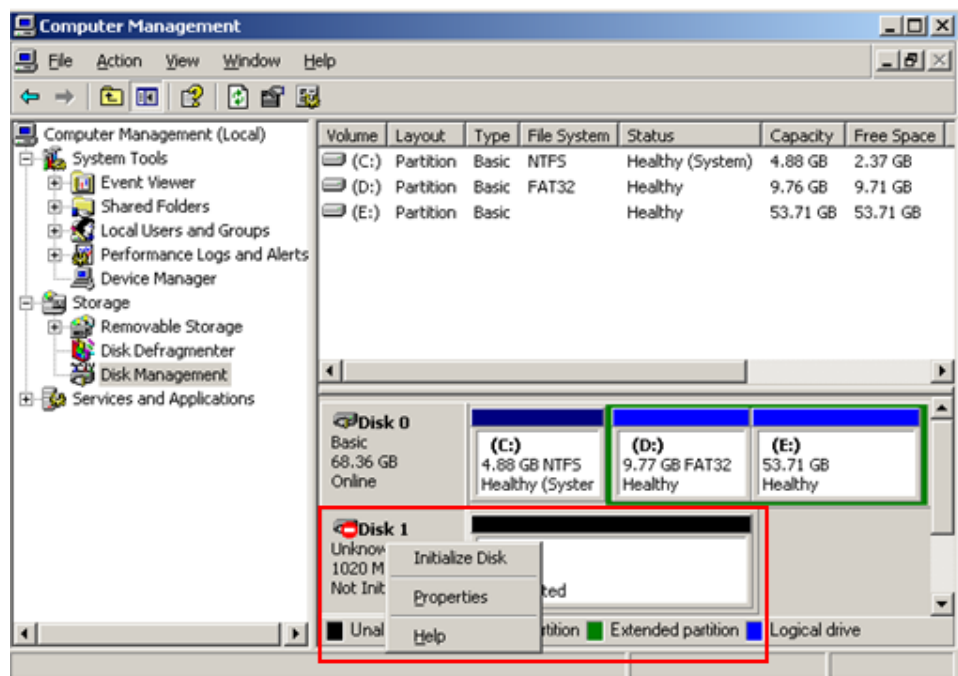
1. **Optional:** Right-click **Disk 1** (as shown in the red square of [Figure 3-57](#)) and choose **Online** from the shortcut menu. The status of **Disk 1** becomes **Not Initialized**.

Figure 3-57 Shortcut menu for Online



2. Right-click **Disk 1** (as shown in the red square of Figure 3-58) and choose **Initialize Disk** from the shortcut menu.

Figure 3-58 Shortcut menu for initializing a disk



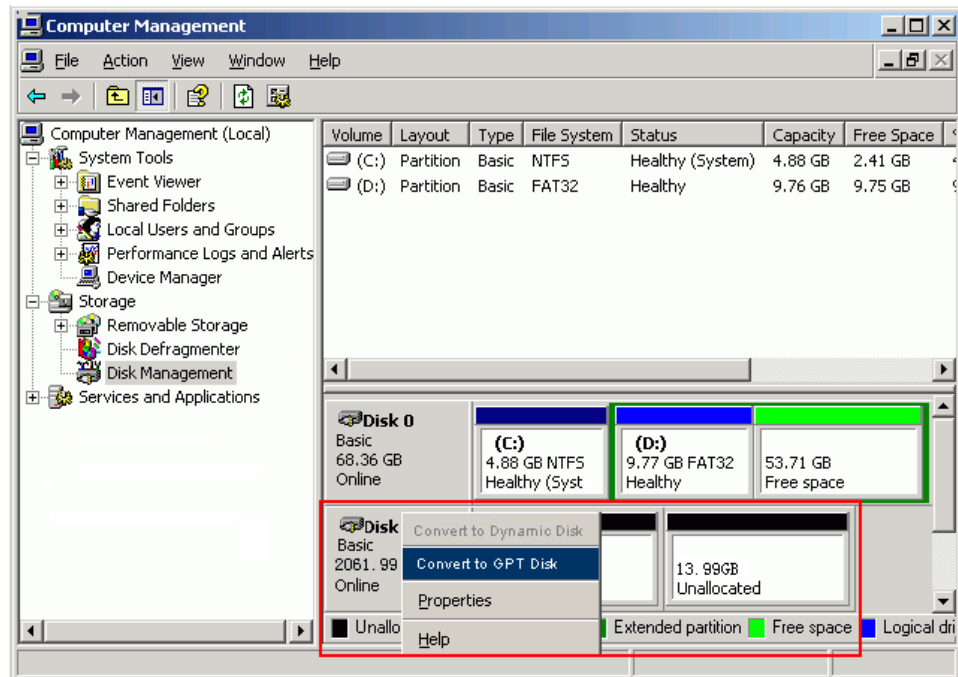
3. In the **Initialize Disk** dialog box, select the logical disk that you want to initialize and click **OK**.

Wait 1 minute. When the status of **Disk 1** becomes **Online**, the initialization is successful.

**Step 5 Optional:** If the logical disk is larger than 2 TB, convert it into a GPT disk. Otherwise, the logical disk cannot be accessed. The following uses Disk 1 as an example.

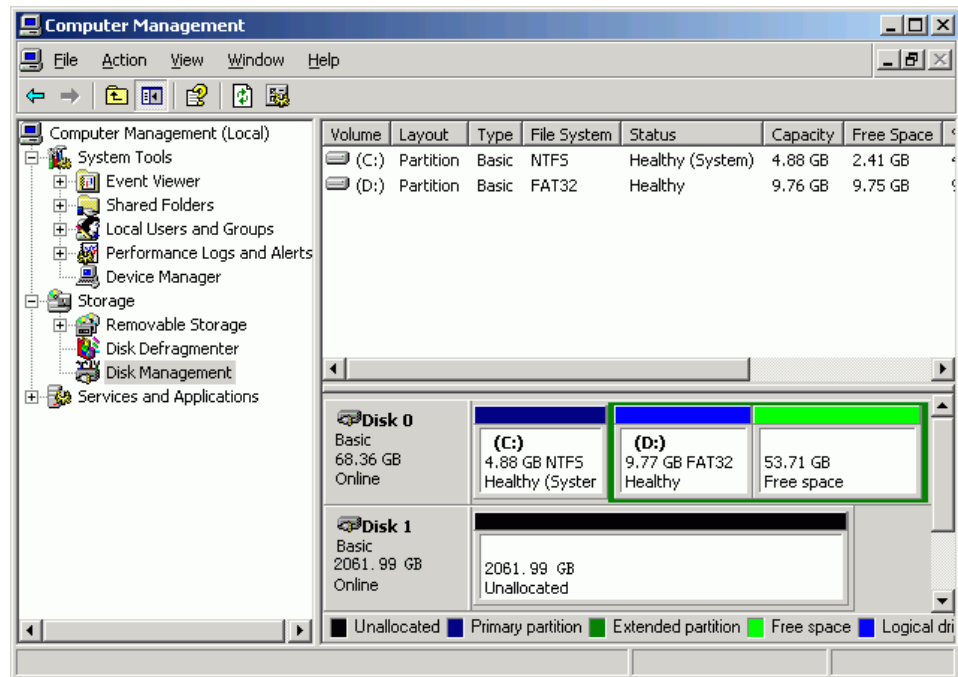
1. Right-click **Disk 1** and choose **Convert to GPT Disk** from the shortcut menu, as shown in the red square in **Figure 3-59**.

**Figure 3-59** Shortcut menu for converting an MBR disk to a GPT disk



After the conversion is successful, the logical disk has only one partition, as shown in **Figure 3-60**.

**Figure 3-60** An MBR disk converted into a GPT disk



**Step 6** Partition and format the logical disk.

**NOTE**

After you have performed formatting, do not read or write the logical disk until its status becomes **Healthy**. Otherwise, the formatting may fail. If formatting fails, try again.

**Step 7** Right-click the new logical disk and choose **Open** from the shortcut menu. Now you can read and write the logical disk.

----End

## Windows Server 2008 and Later Versions

Windows Server 2008 and later versions use the same method to enable an application server to use the space of a storage system. This section uses Windows Server 2008 as an example to describe how to enable an application server to use the space of a storage system.

**Step 1** Log in to the Windows-based application server as **administrator**.

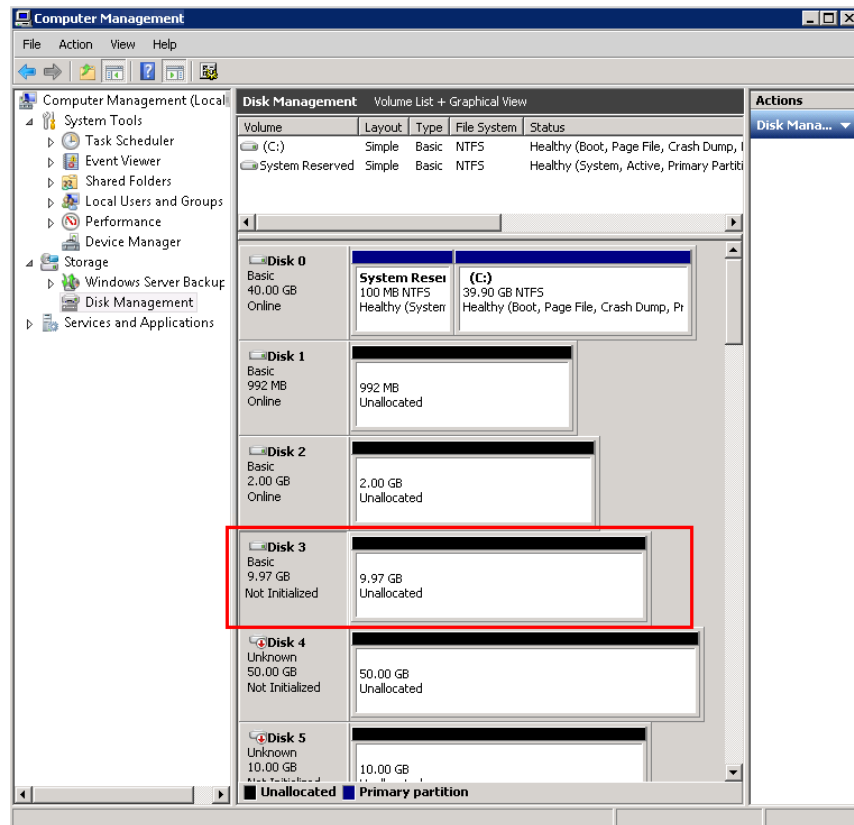
**Step 2** Go to the **Computer Management** dialog box.

Press **Windows+R** (in full screen mode if the operation needs to be performed remotely) to open the **Run** dialog box. Type **compmgmt.msc** and press Enter.

**Step 3** In the navigation tree, choose **Disk Management** and scan for new logical disks.

1. In the navigation tree of **Computer Management**, choose **Storage > Disk Management**.
2. Right-click **Disk Management** and choose **Rescan Disks** from the shortcut menu.
  - After the scan is complete, the new logical disk is displayed in the right area (using Disk 3 as an example), as shown in **Figure 3-61**. The display varies according to the disk size.

Figure 3-61 Viewing the newly added logical disk



- If no new logical disk is detected, perform the following steps:
  - i. In the navigation tree, choose **Device Manager** > **Disk drives**.
  - ii. Right-click **Disk drives** and choose **Scan for hardware changes** from the shortcut menu.
  - iii. After the scan is complete, rescan for logical disks.

 **NOTE**

For details about possible causes, see note information in [Step 3](#) in **Windows Server 2003 and Earlier Versions**.

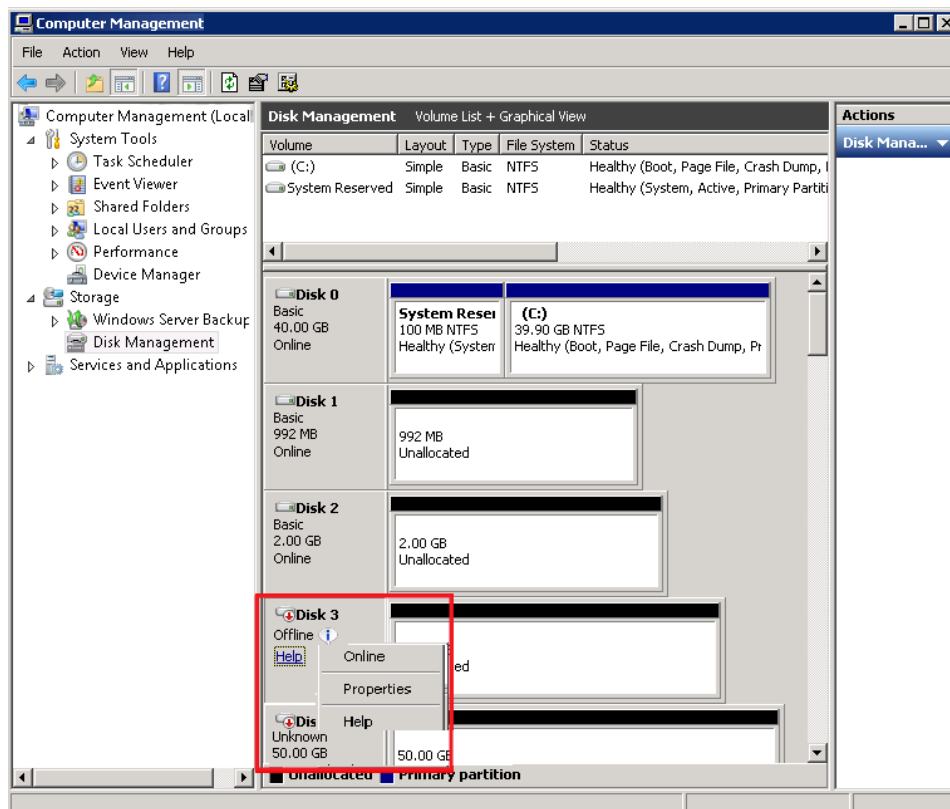
For details, see **Failure to Discover LUNs by an Application Server** in the *OceanStor V3 Series V300R006 Troubleshooting*.

**Step 4** Initialize the new logical disk.

1. **Optional:** Right-click **Disk 3** (as shown in the red square of [Figure 3-62](#)) and choose **Online** from the shortcut menu. The status of **Disk 3** becomes **Not Initialized**.

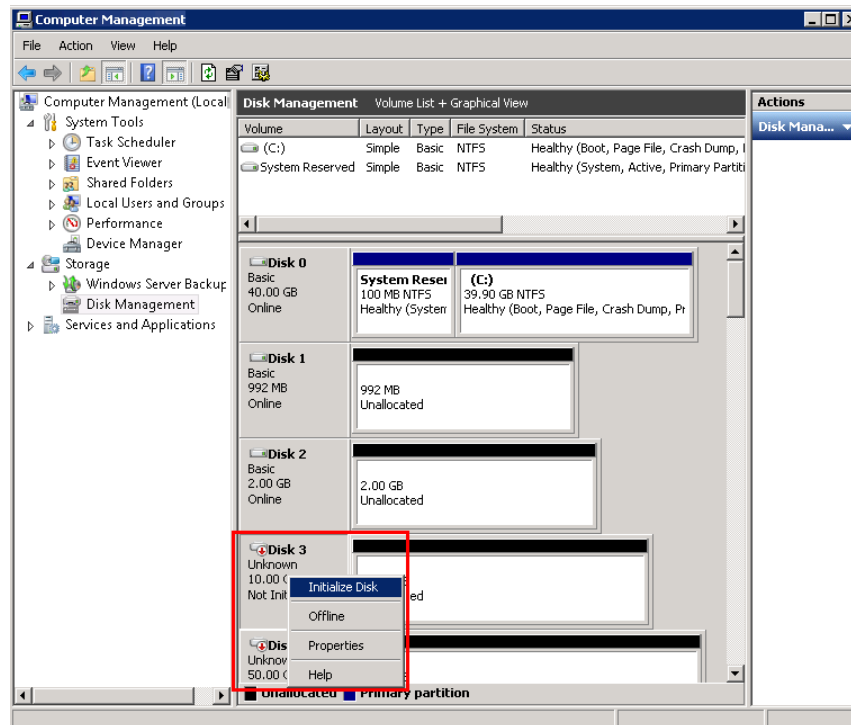


Figure 3-62 Shortcut menu for Online



2. Select and right-click **Disk 3** (as shown in [Figure 3-63](#)), and choose **Initialize Disk** from the shortcut menu.

**Figure 3-63** Initializing the disk menu



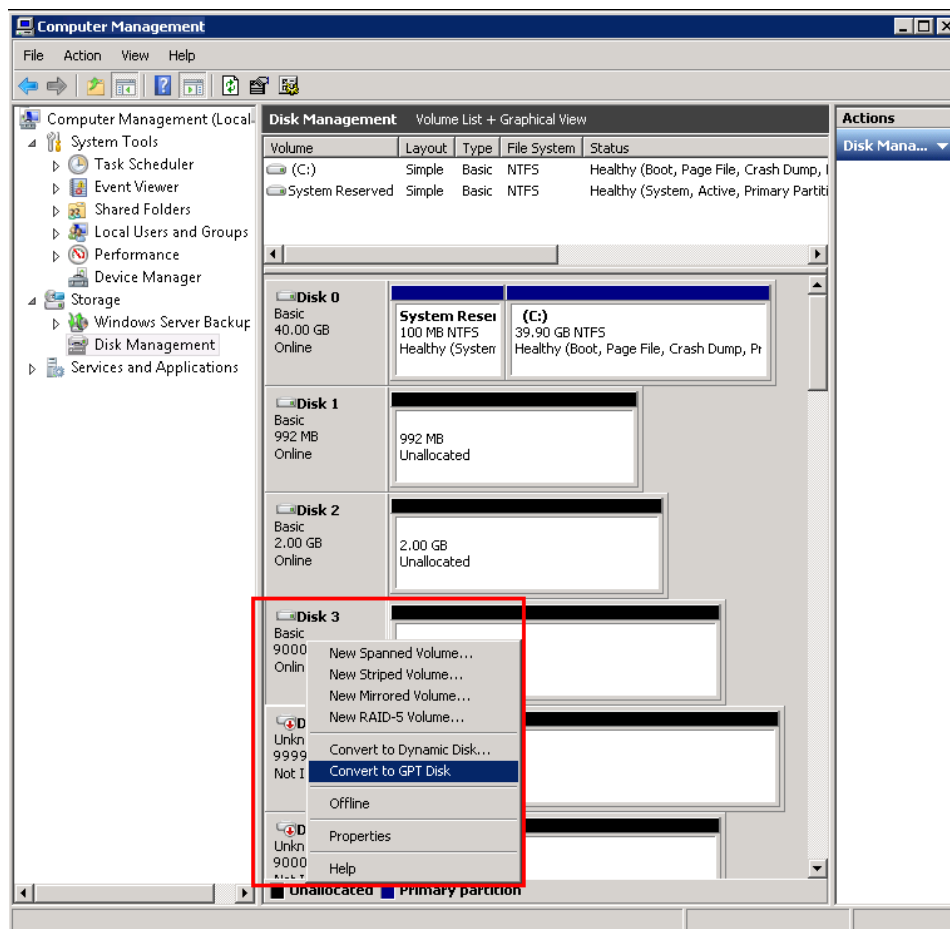
3. In the **Initialize Disk** dialog box, select the logical disk that you want to initialize and click **OK**.

Wait 1 minute. When the status of **Disk 3** becomes **Online**, the initialization is successful.

**Step 5 Optional:** If the capacity of the logical disk is larger than 2 TB, convert it into a GPT disk. Otherwise, it cannot be accessed.

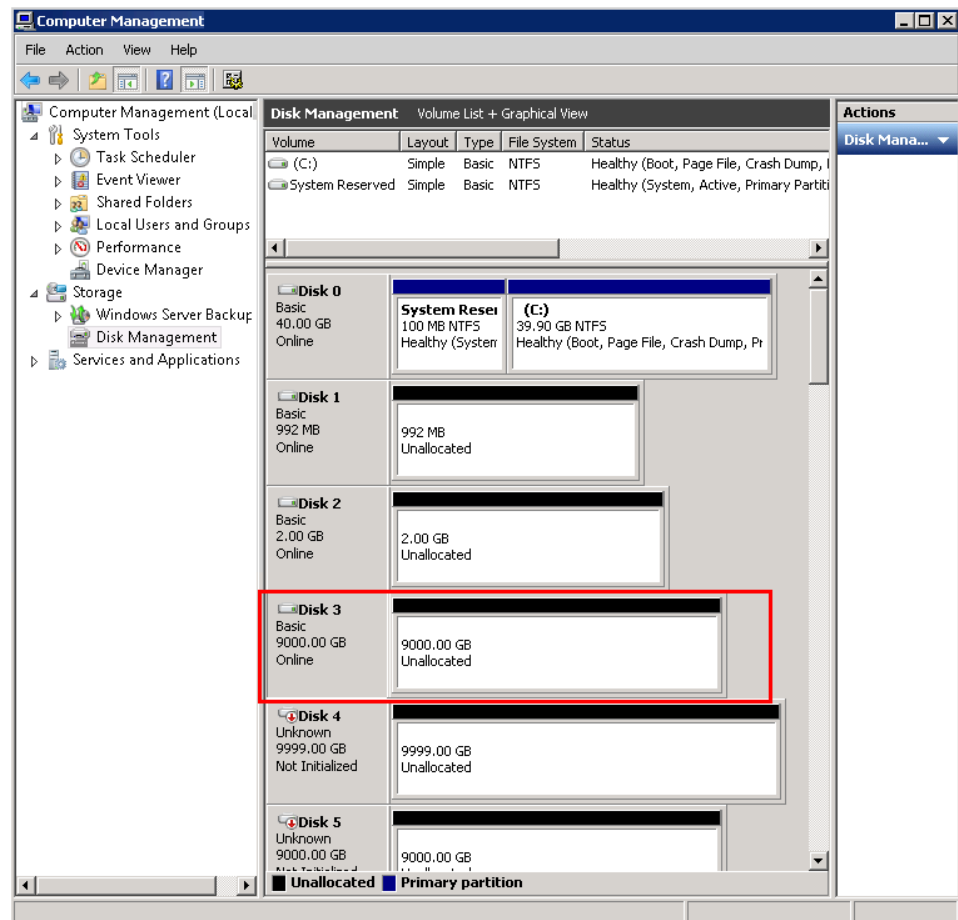
1. Select and right-click **Disk 3** and choose **Convert to GPT Disk** from the shortcut menu, as shown in [Figure 3-64](#).

**Figure 3-64** Converting a logical disk into a GPT disk



After the conversion is successful, two partitions of the logical disk are converted into one partition, as shown in [Figure 3-65](#).

Figure 3-65 Successfully converting the logical disk into a GPT disk



**Step 6** Partition and format the logical disk.

**NOTE**

When you format the disk, do not perform read or write operations on the logical disk until its status becomes **Healthy**. Otherwise, the formatting may fail. If the formatting fails, cancel it and try again.

**Step 7** Right-click the new logical disk and choose **Open** from the shortcut menu. Now you can perform read and write operations on the logical disk.

----End

### 3.14.2 Making Storage Space Available (SUSE)

This section describes how to enable a SUSE-based application server to use the space of a storage system.

#### Procedure

**Step 1** Log in to the SUSE-based application server as user **root**.

**Step 2** Scan for the LUNs mapped to the application server.

Use any of the following methods based on your networking mode.

- iSCSI networking where UltraPath is not installed

Run the `/etc/init.d/iscsi restart` command to restart the iSCSI initiator and scan for LUNs.

```
Linux:~ # /etc/init.d/iscsi restart
Stopping iSCSI: sync umount sync iscsid           done
Starting iSCSI: iscsi iscsid fsck/mount          done
```

- Fibre Channel networking where UltraPath is not installed

 **NOTE**

The following uses the QLA2460 Fibre Channel HBA as an example to explain how to scan for LUNs. For other Fibre Channel HBAs, refer to their manuals.

- Run the `lsmod` command to query the name of the Fibre Channel HBA driver.

The following output is displayed.

```
# lsmod
Module                Size      Used by
qla2xxx              293455    1
autofs4               23749     2
hidp                  23105     0
rfcomm                 42457     0
```

The output shows that the name of the Fibre Channel HBA driver is **qla2xxx**.

- Run the `rmmmod` command to deregister the Fibre Channel HBA driver.

```
# rmmmod qla2xxx
```

In this example, the deregistered Fibre Channel HBA driver is **qla2xxx**.

- Run the `modprobe` command to reload the Fibre Channel HBA driver.

```
# modprobe qla2xxx
```

In this example, the reloaded Fibre Channel HBA driver is **qla2xxx**.

- iSCSI or Fibre Channel networking where UltraPath is installed

Run the `hot_add` command to scan for LUNs.

```
# hot_add
Starting new devices re-scan...
delete LUN not mapped or mapping changed...
scan unconfigured devices...
scan qla2 HBA host /sys/class/scsi_host/host3...
  found 3:0:0:2
scan qla2 HBA host /sys/class/scsi_host/host4...
  found 4:0:0:2
scan iSCSI software initiator host /sys/class/scsi_host/host10...
  no new device found
scan iSCSI software initiator host /sys/class/scsi_host/host12...
  no new device found
run /usr/sbin/upadm start busscan...
scan mpp virtual host /sys/class/scsi_host/host8...
  found ->/dev/sdb
wait for syncing device reference count...
wait for Lun report...
found virtual host8
/usr/sbin/hot_add is completed.
```

**Step 3** Run the `fdisk -l` command to query the information about all disks on the application server.

The application server detects a LUN of 10.7 GB and named `/dev/sdb`, as shown in the following output:

```
Disk /dev/sda: 79.5 GB, 79456894976 bytes
255 heads, 63 sectors/track, 9660 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Disk identifier: 0x225f225e
```

Device	Boot	Start	End	Blocks	Id	System
/dev/sda1		1	1566	12578863+	7	HPFS/NTFS
/dev/sda2		1567	1757	1534207+	82	Linux swap / Solaris

```
/dev/sda3 *          1758          9660          63480847+  83  Linux

Disk /dev/sdb: 10.7 GB, 10737418240 bytes
64 heads, 32 sectors/track, 10240 cylinders
Units = cylinders of 2048 * 512 = 1048576 bytes
Disk identifier: 0x00000000

Disk /dev/sdb doesn't contain a valid partition table
```

 **NOTE**

If no new logical disk is detected, troubleshoot the fault and rescan for logical disks. Possible faults include:

- The application server is incorrectly connected to the storage system after the network cable has been removed and reinserted.
- The link between the application server and storage system is down.
- The rate of the Fibre Channel host port is inconsistent with that of the Fibre Channel HBA on the application server.
- The HBA driver has been uninstalled.
- The RAID is faulty.
- Multipathing software is not installed or an incorrect version is installed.
- The device file on the application server is lost.

For details, see **Failure to Discover LUNs by an Application Server** in the *OceanStor V3 Series V300R006 Troubleshooting*.

**Step 4** Run the **fdisk** command to partition the logical disk.

For example, to create a primary partition for the **/dev/sdb** logical disk, run the following command.

```
# fdisk /dev/sdb
Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 1
First cylinder (1-10240, default 1): 1
Last cylinder, +cylinders or +size{K,M,G} (1-10240, default 10240): 10240

Command (m for help): w
The partition table has been altered!

Syncing disks.
```

 **NOTE**

If the capacity of the LUN is larger than 2 TB, run the **parted** command to change it to the GPT type and then partition it.

**Step 5** Create a file system on the logical disk.

For example, to create an **ext3** file system on the **sdb1** logical disk, run the **mkfs.ext3 /dev/sdb1** command. The following output is displayed.

```
# mkfs.ext3 /dev/sdb1
mke2fs 1.38 ( 30-Jun-2005 )
Filesystem label=
OS type: Linux
Block size=1024 ( log=0 )
Fragment size=1024 ( log=0 )
78312 inodes , 313100 blocks
15655 blocks ( 5.00% ) reserved for the super user
First data block=1
Maximum filesystem blocks=67633152
39 block groups
8192 blocks per group , 8192 fragments per group
```

```

2008 inodes per group
Superblock backups stored on blocks:
    8193 , 24577 , 40961 , 57345 , 73729 , 204801 , 221185

Checking for bad blocks ( read-only test ): done          100
Writing inode tables: done
Creating journal ( 8192 blocks ): done
Writing superblocks and filesystem accounting information: done

This filesystem will be automatically checked every 23 mounts or
180 days , whichever comes first.  Use tune2fs -c or -i to override.
    
```

**Step 6** Create a file directory.

Run the following command to create a file directory:

```
# mkdir /directory
```

In this example, the *directory* directory is created.



After mounting logical disks, modify the `/etc/fstab` file, set automatic loading configuration items, and bond universally unique identifiers (UUIDs) to prevent automatic logical disk loading failures or drive letter changes when the application server is restarted. For details, contact your operating system supplier or system administrator.

**Step 7** Mount the partitioned logical disk to the directory.

Run the following command to mount the logical disk:

```
mount /dev/sdb1 /directory
```

In this example, the `/dev/sdb1` logical disk is mounted to *directory*.

---End

**Result**

Successful mounting ensures that the application server can read and write the logical disk as a normal disk. Run the **mount** command to check whether the logical disk is mounted correctly. If the following output is displayed, the mounting was successful:

```

# mount
/dev/sda2 on / type ext3 (rw)
proc on /proc type proc (rw)
sysfs on /sys type sysfs (rw)
devpts on /dev/pts type devpts (rw, gid=5, mode=620)
/dev/sda5 on /home type ext3 (rw)
/dev/sda1 on /boot type ext3 (rw)
tmpfs on /dev/shm type tmpfs (rw)
none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw)
sunrpc on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw)
none on /proc/fs/vmblock/mountPoint type vmblock (rw)
/dev/hdc on /media/RHEL_5.3 i386 DVD type iso9660 (ro, noexec, nosuid, nodev,
uid=0)
/dev/sdb1 on /directory type ext3 (rw)
    
```

**LVM Management**

Logical volume manager (LVM) can combine the space of several disks (physical volumes) into a volume group and divide the space of the volume group into logical volumes.

Use LVM as follows:

1. Run the **fdisk** command to create an LVM partition.

```
# fdisk /dev/sdc
Device contains neither a valid DOS partition table, nor Sun, SGI or OSF
disklabel
Building a new DOS disklabel with disk identifier 0x1c36ca92.
Changes will remain in memory only, until you decide to write them.
After that, of course, the previous content won't be recoverable.

Warning: invalid flag 0x0000 of partition table 4 will be corrected by w(rite)

Command (m for help): p

Disk /dev/sdc: 107.3 GB, 107374182400 bytes

255 heads, 63 sectors/track, 13054 cylinders

Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/sdc1             1           200     1606468+   83  Linux
/dev/sdc4            201        1000     6426000    5  Extended
/dev/sdc5            201           400     1606468+   8e  Linux
/dev/sdc6            401           600     1606468+   83  Linux

Command (m for help): t

Partition number (1-6): 5

Hex code (type L to list codes): 8e

Changed system type of partition 6 to 8e (Linux LVM)

Command (m for help): t

Partition number (1-6): 6

Hex code (type L to list codes): 8e

Changed system type of partition 6 to 8e (Linux LVM)

Command (m for help): p

Disk /dev/sdc: 107.3 GB, 107374182400 bytes

255 heads, 63 sectors/track, 13054 cylinders

Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/sdc1             1           200     1606468+   83  Linux
/dev/sdc4            201        1000     6426000    5  Extended
```



```
/dev/sdc5          201          400          1606468+  8e  Linux LVM
/dev/sdc6          401          600          1606468+  8e  Linux LVM
```

2. Run the **pvcreate** command to create a physical volume.

```
# pvcreate /dev/sdc5

Physical volume "/dev/sdc5" successfully created

# pvcreate /dev/sdc6

Physical volume "/dev/sdc6" successfully created
```

After creating the physical volume, run the **pvdisplay -v** command to check whether the physical volume is created successfully.

3. Run the **vgcreate** command to create a volume group.

```
# vgcreate vg0 /dev/sdc5 /dev/sdc6

Volume group "vg0" successfully created
```

4. Run the **lvcreate** command to create a logical volume.

```
# lvcreate -L 10m -n lv0 vg0

Rounding up size to full physical extent 12.00 MB

Logical volume "lv0" created
```

After creating the logical volume, run the **vgdisplay -v** command to confirm the logical volume information.

5. Run the **mkfs.xx** command to create a file system. The ext3 format is used as an example here.

```
# mkfs.ext3 /dev/vg0/lv0

mke2fs 1.39 (29-May-2006)

Filesystem label=
OS type: Linux
Block size=1024 (log=0)
Fragment size=1024 (log=0)
3072 inodes, 12288 blocks
614 blocks (5.00%) reserved for the super user
First data block=1
Maximum filesystem blocks=12582912
2 block groups
8192 blocks per group, 8192 fragments per group
1536 inodes per group
Superblock backups stored on blocks:

    8193

Writing inode tables: done
Creating journal (1024 blocks): done
Writing superblocks and filesystem accounting information: done
```

```
This filesystem will be automatically checked every 20 mounts or
180 days, whichever comes first. Use tune2fs -c or -i to override.
```

6. Create a mount point to mount the logical volume.

```
# mkdir /test/mnt1
# mount /dev/vg0/lv0 /test/mnt1/
```

### 3.14.3 Making Storage Space Available (Red Hat)

This section describes how to enable a Red Hat-based application server to use the space of a storage system.

#### Procedure

- Step 1** Log in to the Red Hat-based application server as user **root**.

- Step 2** Scan for the LUNs mapped to the application server.

Use any of the following methods based on your networking mode.

- iSCSI networking where UltraPath is not installed

Run the **/etc/init.d/iscsi restart** command to restart iSCSI services and scan for LUNs.

```
[root@localhost ~] # /etc/init.d/iscsi restart
Stopping iSCSI daemon:
iscsid dead but pid file exists [ OK ]
Turning off network shutdown. Starting iSCSI daemon: [ OK ]
[ OK ]
[ OK ]
[root@localhost ~]# ifconfig
```

- Fibre Channel networking where UltraPath is not installed

#### NOTE

The following uses the QLA2460 Fibre Channel HBA as an example to explain how to scan for LUNs. For other Fibre Channel HBAs, see their corresponding manuals.

- a. Run the **lsmod** command to query the name of the Fibre Channel HBA driver.

The following output is displayed.

```
# lsmod
Module          Size  Used by
qla2xxx         749473  0
autofs4         23749  2
hidp            23105  0
rfcomm          42457  0
```

The output shows that the name of the Fibre Channel HBA driver is **qla2xxx**.

- b. Run the **rmod** command to deregister the Fibre Channel HBA driver.

For example:

```
# rmod qla2xxx
```

In this example, the deregistered Fibre Channel HBA driver is **qla2xxx**.

- c. Run the **modprobe** command to reload the Fibre Channel HBA driver.

For example:

```
# modprobe qla2xxx
```

In this example, the reloaded Fibre Channel HBA driver is **qla2xxx**.

- iSCSI or Fibre Channel networking where UltraPath is installed

Run the **hot\_add** command to scan for LUNs.

```
starting new devices re-scan...
  scan mptsas HBA host /sys/class/scsi_host/host1...
  no new device found run /usr/sbin/upTools -s busscan...
found 2:0:0:0->/dev/sdb found 2:0:0:1->/dev/sdc /usr/sbin/hot_add is
completed.
```

**Step 3** Run the **fdisk -l** command to query the information about all disks on the application server.

The application server detects a LUN of 1073 MB and named **/dev/sdb**, as shown below.

```
Disk /dev/sda: 8589 MB, 8589934592 bytes 255 heads, 63 sectors/track,
 1044 cylinders Units = cylinders of 16065 * 512 = 8225280 bytes

Device Boot      Start         End      Blocks   Id  System /dev/sda1
*                1           13        104391   83  Linux /dev/sda2
                 14          1044       8281507+  8e  Linux LVM
Disk /dev/sdb: 1073 MB, 1073741824 bytes 34 heads, 61 sectors/track,
1011 cylinders Units = cylinders of 2074 * 512 = 1061888 bytes
Disk /dev/sdb doesn't contain a valid partition table
```

 **NOTE**

If no new logical disk is detected, troubleshoot the fault and rescan for logical disks. Possible faults include:

- The application server is incorrectly connected to the storage system after the network cable has been removed and reinserted.
- The link between the application server and storage system is down.
- The rate of the Fibre Channel host port is inconsistent with that of the Fibre Channel HBA on the application server.
- The HBA driver has been uninstalled.
- The storage pool fails.
- Multipathing software is not installed or an incorrect version is installed.
- The device file on the application server is lost.

For details, see **Failure to Discover LUNs by an Application Server** in the *OceanStor V3 Series V300R006 Troubleshooting*.

**Step 4** Run the **fdisk** command to partition the logical disk.

For example, to create a primary partition for the **/dev/sdb** logical disk, run the following command.

```
# fdisk /dev/sdb
Command (m for help): n
Command action e   extended
p   primary partition (1-4)
p Partition number (1-4): 1
First cylinder (1-1011, default 1): 1
Last cylinder (1-1011, default 1011): 1011
Command (m for help): w
The partition table has been altered!
Calling ioctl () to re-read partition table. Syncing disks.
```

 **NOTE**

If the capacity of the LUN is larger than 2 TB, run the **parted** command to change it to the GPT type and then partition it.

**Step 5** Create a file system on the logical disk.

Run the following command to create a file system on the logical disk:

```
mkfs.ext3 /dev/sdb1
```

In this example, an **ext3** file system is created for the **/dev/sdb1** logical disk.

The following output is displayed.

```
mke2fs 1.38 (30-Jun-2005) /dev/sdb is entire device, not just one partition!  
Proceed anyway? (y,n) y  
Filesystem label= OS type:  
Linux Block size=4096 (log=2)  
Fragment size=4096 (log=2)  
131072 inodes, 262144 blocks 13107 blocks (5.00%) reserved for the super user  
First data block=0 8 block groups 32768 blocks per group,  
32768 fragments per group 16384 inodes per group Superblock backups stored on  
blocks: 32768, 98304, 163840, 229376  
Writing inode tables: done Creating journal (8192 blocks): done Writing  
superblocks and filesystem accounting information: done  
This filesystem will be automatically checked every 39 mounts or 180 days,  
whichever comes first.  
Use tune2fs -c or -i to override.
```

### Step 6 Create a file directory.

Run the following command to create a file directory:

```
mkdir /directory
```

In this example, the `/directory` directory is created.



## NOTICE

After mounting logical disks, modify the `/etc/fstab` file, set automatic loading configuration items, and bond UUIDs to prevent automatic logical disk loading failures or drive letter changes when the application server is restarted. For details, contact your operating system supplier or system administrator.

### Step 7 Mount the partitioned logical disk to the directory.

Run the following command to mount the logical disk:

```
mount /dev/sdb1 /directory
```

In this example, the `/dev/sdb1` logical disk is mounted to `/directory`.

----End

## Result

Successful mounting ensures that the application server can read and write the logical disk as a normal disk. Run the `mount` command to check whether the logical disk is properly mounted. If the following output is displayed, the mounting was successful:

```
# mount  
/dev/mapper/VolGroup-lv_root on / type ext4 (rw)  
proc on /proc type proc (rw)  
sysfs on /sys type sysfs (rw)  
devpts on /dev/pts type devpts (rw,gid=5,mode=620)  
tmpfs on /dev/shm type tmpfs (rw,rootcontext="system_u:object_r:tmpfs_t:s0")  
/dev/sda1 on /boot type ext4 (rw)  
none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw)  
sunrpc on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw)  
/dev/sdb1 on /directory type ext3 (rw)
```

## LVM Management

LVM can combine the space of several disks (physical volumes) into a volume group and divide the space of the volume group into logical volumes.

Use LVM as follows:

1. Run the **fdisk** command to create an LVM partition.

```
# fdisk /dev/sdc
Device contains neither a valid DOS partition table, nor Sun, SGI or OSF
disklabel
Building a new DOS disklabel with disk identifier 0x1c36ca92.
Changes will remain in memory only, until you decide to write them.
After that, of course, the previous content won't be recoverable.

Warning: invalid flag 0x0000 of partition table 4 will be corrected by w(rite)

Command (m for help): p

Disk /dev/sdc: 107.3 GB, 107374182400 bytes

255 heads, 63 sectors/track, 13054 cylinders

Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/sdc1             1           200     1606468+   83  Linux
/dev/sdc4            201        1000     6426000    5  Extended
/dev/sdc5            201           400     1606468+   8e  Linux
/dev/sdc6            401           600     1606468+   83  Linux

Command (m for help): t

Partition number (1-6): 5

Hex code (type L to list codes): 8e

Changed system type of partition 6 to 8e (Linux LVM)

Command (m for help): t

Partition number (1-6): 6

Hex code (type L to list codes): 8e

Changed system type of partition 6 to 8e (Linux LVM)

Command (m for help): p

Disk /dev/sdc: 107.3 GB, 107374182400 bytes

255 heads, 63 sectors/track, 13054 cylinders

Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/sdc1             1           200     1606468+   83  Linux
/dev/sdc4            201        1000     6426000    5  Extended
```

```
/dev/sdc5          201          400          1606468+  8e  Linux LVM
/dev/sdc6          401          600          1606468+  8e  Linux LVM
```

2. Run the **pvcreate** command to create a physical volume.

```
# pvcreate /dev/sdc5

Physical volume "/dev/sdc5" successfully created

# pvcreate /dev/sdc6

Physical volume "/dev/sdc6" successfully created
```

After creating the physical volume, run the **pvdisplay -v** command to check whether the physical volume is created successfully.

3. Run the **vgcreate** command to create a volume group.

```
# vgcreate vg0 /dev/sdc5 /dev/sdc6

Volume group "vg0" successfully created
```

4. Run the **lvcreate** command to create a logical volume.

```
# lvcreate -L 10m -n lv0 vg0

Rounding up size to full physical extent 12.00 MB

Logical volume "lv0" created
```

After creating the logical volume, run the **vgdisplay -v** command to confirm the logical volume information.

5. Run the **mkfs.xx** command to create a file system. The ext3 format is used as an example here.

```
# mkfs.ext3 /dev/vg0/lv0

mke2fs 1.39 (29-May-2006)

Filesystem label=
OS type: Linux
Block size=1024 (log=0)
Fragment size=1024 (log=0)
3072 inodes, 12288 blocks
614 blocks (5.00%) reserved for the super user
First data block=1
Maximum filesystem blocks=12582912
2 block groups
8192 blocks per group, 8192 fragments per group
1536 inodes per group
Superblock backups stored on blocks:

    8193

Writing inode tables: done
Creating journal (1024 blocks): done
Writing superblocks and filesystem accounting information: done
```

```
This filesystem will be automatically checked every 20 mounts or
180 days, whichever comes first. Use tune2fs -c or -i to override.
```

6. Create a mount point to mount the logical volume.

```
# mkdir /test/mnt1
# mount /dev/vg0/lv0 /test/mnt1/
```

### 3.14.4 Making Storage Space Available (Solaris)

This section describes how to enable a Solaris-based application server to use the space of a storage system.

#### Procedure

**Step 1** Log in to the Solaris-based application server as user **root**.

**Step 2** Run the **cfgadm -al** command to scan for the LUNs mapped to the application server.

The following output is displayed.

```
# cfgadm -al
Ap_Id                Type      Receptacle  Occupant  Condition
c1                   scsi-bus  connected   configured unknown
c1::dsk/c1t1d0       disk      connected   configured unknown
c2                   fc-private connected   unconfigured unknown
c2::2201123456789012 disk      connected   unconfigured unknown
c3                   fc-private connected   unconfigured unknown
c3::2210123456789012 disk      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-storage 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
```

 **NOTE**

If no new logical disk is detected, troubleshoot the fault and rescan for logical disks. Possible faults include:

- The application server is incorrectly connected to the storage system after the network cable has been removed and reinserted.
- The link between the application server and storage system is down.
- The rate of the Fibre Channel host port is inconsistent with that of the Fibre Channel HBA on the application server.
- The HBA driver has been uninstalled.
- The storage pool fails.
- Multipathing software is not installed or an incorrect version is installed.
- The device file on the application server is lost.

For details, see **Failure to Discover LUNs by an Application Server** in the *OceanStor V3 Series V300R006 Troubleshooting*.

### Step 3 Partition and format a disk.

1. Run the **format** command to query the information about all disks on the application server.

```
# format
Searching for disks...done
AVAILABLE DISK SELECTIONS:
0. clt0do <SUN146G cyl 14087 alt 2 hd 24 sec 848>
   /pci@0/pci@0/pci@2/scsi@0/sd@0, 0
1. clt1d0 <DEFAULT cyl 6398 alt 2 hd sec 256>
   /iscsi/disk@0000iqn.2006-08.com.huawei%3Aocceanstor
%3A2100001882afe72c%3Anotconfig%3A13.13.13.110003,
Specify disk (enter its number):
```

The output shows that the **clt1d0** logical disk (ID is **1**) is mapped to the host.

2. Enter the ID of the disk to be formatted after **Specify disk (enter its number)**.

```
Searching for disks...done
AVAILABLE DISK SELECTIONS:
0. clt0do <SUN146G cyl 14087 alt 2 hd 24 sec 848>
   /pci@0/pci@0/pci@2/scsi@0/sd@0, 0
1. clt1d0 <DEFAULT cyl 6398 alt 2 hd sec 256>
   /iscsi/disk@0000iqn.2006-08.com.huawei%3Aocceanstor
%3A2100001882afe72c%3Anotconfig%3A13.13.13.110003, 0
Specify disk (enter its number): 1
Selecting clt1d0
[disk formatted]
Disk not labeled. Label it now?
```

3. Enter **y** after **Label it now?**.

```
[disk formatted]
Disk not labeled. Label it now? y

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 the defective disk
label     - write label to the disk
analyze   - surface analysis
defect    - defect list management
back up   - search for backup labels
verify    - read and display labels
save      - save new disk/partition definitions
inquiry   - show vendor, product and revision
volname   - set 8-character volume name
!<cmd>    - execute <cmd>, then return
quit
```

#### NOTE

After the **format** command is executed, several partitions including **s0** and **s1** are automatically created.

4. View the partition table.

Run the **partition** command and then run the **print** command.

```
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 (original):
Total disk cylinders available: 6398 + 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 - 6397       49.98GB      104824832
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 - 6397     49.98GB      (6366/0/0) 262144
7        unassigned wm     0              0              (0/0/0) 0

```

 **NOTE**

In normal cases, the partition whose **Part** is **2** indicates the logical disk mapped to the host.

5. Enter **quit** to exit the **Partition** command output screen.
6. Enter **quit** to exit the **Format** command output screen.

**Step 4** Configure the multipathing software.

Solaris supports UltraPath and StorEdge Traffic Manager Software (STMS).

- UltraPath is developed by Huawei.
- STMS is delivered with the Solaris host system.

STMS is used as an example to describe how to configure the multipathing software. For details about how to install and configure UltraPath, see the user guide specific to your product.

- Solaris 10

The method used to enable the multipathing software on the host system varies according to different ALUA modes (enabled or disabled).

- ALUA is enabled.

After ALUA is enabled on the storage system, you do not need to configure the host system. Run the **stmsboot -D fp -e** command directly.

```

# stmsboot -D fp -e

WARNING: This operation will require a reboot.

Do you want to continue ? [y/n] (default: y) y

The changes will come into effect after rebooting the system.

Reboot the system now ? [y/n] (default: y) y

updating /platform/sun4u/boot_archive

```

 **NOTICE**

After the command is executed, the operating system will restart.

- ALUA is disabled.

If ALUA is disabled on the storage system, you must modify the configuration file on the host system. In this way, the multipathing software can take over the LUNs that are mapped by the storage system.

- i. Run the **format** command, select a mapped disk, and click **inquiry** to query **Vendor ID** and **Product ID** of the LUN.
- ii. Modify the **/kernel/drv/scsi\_vhci.conf** configuration file and add **Vendor ID** and **Product ID** of the LUN to the configuration file. For example, if **Vendor ID** is **HUAWEI** and **Product ID** is **XXXXXX**, configure the file as follows:

```
device-type-scsi-options-list =
"HUAWEI XXXXXX", "symmetric-option";
```

- iii. Run the **stmsboot -D fp -e** command to activate the STMS function. The STMS takes effect after the operating system restarts.

- Solaris 11

The method used to enable the multipathing software on the host system varies according to different ALUA modes (enabled or disabled).

- ALUA is enabled.

The configuration method is the same as that in Solaris 10.

- ALUA is disabled.

- i. Run the **format** command, select a mapped disk, and click **inquiry** to query **Vendor ID** and **Product ID** of the LUN.
- ii. Run the **cp /kernel/drv/scsi\_vhci.conf/etc/driver/drv/scsi\_vhci.conf** command to copy content of the **/kernel/drv/scsi\_vhci.conf** file to the **/etc/driver/drv/scsi\_vhci.conf** file.
- iii. Modify the **/etc/driver/drv/scsi\_vhci.conf** configuration file and add **Vendor ID** and **Product ID** of the LUN to the configuration file. For example, if **Vendor ID** is **HUAWEI** and **Product ID** is **XXXXXX**, configure the file as follows:

```
scsi-vhci-failover-override =
"HUAWEI XXXXXX", "f_sym";
```

- iv. Run the **stmsboot -D fp -e** command to activate the STMS function. The STMS takes effect after the operating system restarts.

**Step 5** Run the following **newfs** command to create a file system:

```
newfs /dev/dsk/ct1td0s2
```

In this example, the file system is created on **/dev/rdisk/ct1td0s2**, where **ct1td0** indicates the name of the logical disk mapped to the host, and **s2** indicates the second partition of the logical disk.

The following output is displayed.

```
newfs: construct a new file system /dev/rdisk/ct1td0s2: (y/n) y
/dev/rdisk/ct1td0s2 12566128 sectors in 3068 cylinders of 128 tracks, 32 sectors
6136.0 MB in 118 cyl groups (26 c/g, 52.00 MB/g, 6400 i/g)
super-block backups (for fsck -F ufs -o b=#) at:
32, 106560, 213088, 319616, 426144, 532672, 639200, 745728, 852256, 958784,
11505056, 11611584, 11718112, 11824640, 11931168, 12037696, 12144224,
12250725, 12357280, 12463830
```

**Step 6** Create a file directory.

Run the following command to create a file directory:

```
mkdir /directory
```

In this example, the `/directory` directory is created.

**Step 7** Mount the partitioned logical disk to the directory.

Run the following command to mount the logical disk:

```
mount /dev/dsk/clt1d0s2 /directory
```

In this example, the `/dev/dsk/clt1d0s2` logical disk is mounted to `/directory`.

----End

## Result

Successful mounting ensures that the application server can read and write the logical disk as a normal disk. Run the **mount** command to check whether the logical disk is properly mounted. If the following output is displayed, the mounting was successful:

```
# mount
/directory /dev/dsk/clt1d0s2 read/write/setuid/devices/intr/largefiles/logging/
xattr/oneerror=panic/dev=800302 on Fri Jun 10 14:25:12 2011
```

## 3.14.5 Making Storage Space Available (AIX)

This task guides you through enabling an AIX-based application server to use the storage space provided by a storage system.

### Context

An AIX-based application server manages its storage space using physical volumes and logical volumes. [Table 3-25](#) describes the commands used to manage physical and logical volumes.

**Table 3-25** Commands used to manage physical and logical volumes

Command	Use to
cfgmgr	Scans for LUNs.
lspv	Lists the information about physical volumes.
mkvg	Creates a physical volume group.
mklv	Creates a logical volume in a physical volume group.
crfs	Creates a file system.
rmdev	Deletes a physical volume.
rmlv	Deletes a logical volume.

### Precaution

If you need to configure SAN boot while UltraPath of a higher version is not installed for connecting an AIX host to a Huawei storage device, see "**Installing AIX ODM for MPIO**" of the *AIX ODM for MPIO User Guide* to install AIX ODM for MPIO before performing the following operations.

## Procedure

- Step 1** Log in to the AIX-based application server as user **root**.
- Step 2** Run the **cfgmgr** command to scan for the LUNs mapped to the application server.
- Step 3** Run the **lspv** command to query the **PVID** allocated to the newly mapped disk.

The following output is displayed.

```
# lspv
hdisk0          000c6ce67e98ce56          rootvg          active
updisk0        000c6ce66fc2cfc6          vg1
updisk1        000c6ce66fc2cfc6          vg1
updisk2        000c6ce67ed787c1          vg2
updisk3        None                       None
```

The output shows that **PVID** of the newly mapped disk is **updisk3** and the disk is inactive.

### NOTE

If no new logical disk is detected, troubleshoot the fault and rescan for logical disks. Possible faults include:

- The application server is incorrectly connected to the storage system after the network cable has been removed and reinserted.
- The link between the application server and storage system is down.
- The rate of the Fibre Channel host port is inconsistent with that of the Fibre Channel HBA on the application server.
- The HBA driver has been uninstalled.
- The storage pool fails.
- Multipathing software is not installed or an incorrect version is installed.
- The device file on the application server is lost.

For details, see **Failure to Discover LUNs by an Application Server** in the *OceanStor V3 Series V300R006 Troubleshooting*.

- Step 4** Create a physical volume group.

Run the following command to create a physical volume group:

```
# mkvg -y testvg updisk3
0516-1254 mkvg: Changing the PVID in the ODM.
testvg
```

In this example, the **testvg** physical volume group is created for the *updisk3* logical disk.

After the physical volume group is successfully created, run the **lspv** command to query the status. As shown in the following, the status of the physical volume group becomes **active**.

```
# lspv
hdisk0          000c6ce67e98ce56          rootvg          active
updisk0        000c6ce66fc2cfc6          vg1
updisk1        000c6ce66fc2cfc6          vg1
updisk2        000c6ce67ed787c1          vg2
updisk3        000c6ce67ee9fc27          testvg          active
```

- Step 5** Create a logical volume.

Run the following command to create a logical volume:

```
# mklv -y testlv -t jfs testvg 100
testlv
```

In this example, the *testlv* logical volume is created in the *testvg* physical volume group and is allocated 100 physical partitions.

- Step 6** Create the directory for mounting the logical volume.

Run the following command to create a directory for mounting the logical volume:

```
# mkdir /test
```

In this example, the *test* directory is created.

**Step 7** Run the following command to create a file system on the logical volume and mount the file system to the newly created directory:

```
# crfs -v jfs -d /dev/testlv -m /test -A yes -a size=1024
crfs: Warning: device name given, size parameter ignored.
Based on the parameters chosen, the new /test JFS file system
is limited to a maximum size of 134217728 (512 byte blocks)
```

In this example, a *jfs* file system containing 1024 data blocks (512 bytes each) is created on the *testlv* logical volume.

#### NOTE

The following describes the parameters in the **crfs** command:

- **-v jfs**: A JFS file system will be created.
- **-d**: name of the logical volume on which the file system is located.
- **-m**: directory to which the file system will be mounted.
- **-A yes**: file system auto mounting upon the application server re-startup will be enabled.
- **-a**: default values will be configured for the properties of the file system.
- **size=**: capacity of the file system, expressed in data blocks (512 bytes each).

After the file system has been created, run the **lsvg** command to view the file system created in the specified directory. For example, to view the file system created in the **testvg** directory, run the following command.

```
# lsvg -l testvg
testvg:
LV NAME          TYPE      LPs      PPs      PVs  LV STATE      MOUNT POINT
testlv           jfs       100      100      1    open/syncd    /test
loglv01          jfslog    1         1         1    open/syncd    N/A
```

----End

## Result

Successful mounting ensures that the application server can read and write the logical disk as a normal disk. Run the **mount** command to check whether the logical disk is properly mounted. If the following output is displayed, the mounting was successful:

```
# mount
node mounted      mounted over      vfs      date      options
-----
/dev/hd4          /                  jfs2     Aug 04 02:31 rw,log=/dev/hd8
/dev/hd2          /usr               jfs2     Aug 04 02:31 rw,log=/dev/hd8
/dev/hd9var       /var               jfs2     Aug 04 02:31 rw,log=/dev/hd8
/dev/hd3          /tmp               jfs2     Aug 04 02:31 rw,log=/dev/hd8
/dev/fwdump       /var/adm/ras/platform jfs2     Aug 04 02:32 rw,log=/dev/
hd8
/dev/hd1          /home              jfs2     Aug 04 02:32 rw,log=/dev/hd8
/dev/hd11admin    /admin             jfs2     Aug 04 02:32 rw,log=/dev/hd8
/proc             /proc              procfs    Aug 04 02:32 rw
/dev/hd10opt      /opt               jfs2     Aug 04 02:32 rw,log=/dev/hd8
/dev/livedump     /var/adm/ras/livedump jfs2     Aug 04 02:32 rw,log=/dev/
hd8
/dev/testlv       /test              jfs      Aug 05 04:07 rw,log=/dev/loglv01
```

### 3.14.6 Making Storage Space Available (HP-UX)

This section describes how to enable an HP-UX-based application server to use the space of a storage system.

#### Context

For versions earlier than HP-UX 11iv3, only the PV-Links multipathing software is supported. For HP-UX 11iv3, two multipathing software types are supported: PV-Links and NMP.

- PV-Links adds multiple paths of a LUN to the same volume group (VG) and uses the VG functions to manage the multiple paths. To use PV-Links, you must manually configure data for each LUN.
- NMP can be directly used without the need to set it. You can run the `scsimgr get_attr -a leg_mpath_enable` command to check the NMP service status.

#### Procedure

**Step 1** Log in to the HP-UX-based application server as user `root`.

**Step 2** View the information about disks identified by the operating system.

If the host operating system version is HP-UX 11iv3, you can run the `ioscan -funNC disk` command to view disks identified by the host operating system. If the host operating system version is HP-UX 11iv2 or 11iv1, you can run the `ioscan -funC disk` command to view disks identified by the host operating system.

```
# ioscan -funNC disk
Class      I  H/W Path          Driver S/W State  H/W Type      Description
=====
disk      162  0/3/1/0/4/0.8.0.2.0.0.0  sdisk CLAIMED DEVICE  ENGENIO INF-01-00
          /dev/dsk/c36t0d0      /dev/rdisk/c36t0d0
disk      164  0/3/1/0/4/0.8.0.2.0.0.1  sdisk CLAIMED DEVICE  ENGENIO INF-01-00
          /dev/dsk/c36t0d1      /dev/rdisk/c36t0d1
disk       0  0/4/1/0.0.0.0.0.0      sdisk CLAIMED DEVICE  HP      DG146BB976
          /dev/dsk/c2t0d0      /dev/rdisk/c2t0d0
disk       1  0/4/1/0.0.0.1.0        sdisk CLAIMED DEVICE  HP      DG146BB976
          /dev/dsk/c2t1d0      /dev/dsk/c2t1d0s2    /dev/rdisk/
c2t1d0    /dev/rdisk/c2t1d0s2    /dev/dsk/c2t1d0s1    /dev/dsk/c2t1d0s3    /dev/rdisk/
c2t1d0s1 /dev/rdisk/c2t1d0s3
disk      194  0/6/1/0/4/0.1.14.232.0.0.0  sdisk CLAIMED DEVICE  XXXX
          /dev/dsk/c45t0d0      /dev/rdisk/c45t0d0
disk      195  0/6/1/0/4/0.1.14.232.0.0.1  sdisk CLAIMED DEVICE  XXXX
          /dev/dsk/c45t0d1      /dev/rdisk/c45t0d1
disk      196  0/6/1/0/4/0.1.14.232.0.0.2  sdisk CLAIMED DEVICE  XXXX
          /dev/dsk/c45t0d2      /dev/rdisk/c45t0d2
disk      197  0/6/1/0/4/0.1.14.232.0.0.3  sdisk CLAIMED DEVICE  XXXX
          /dev/dsk/c45t0d3      /dev/rdisk/c45t0d3
disk      206  0/6/1/0/4/0.1.14.232.0.1.0  sdisk CLAIMED DEVICE  XXXX
          /dev/dsk/c45t1d0      /dev/rdisk/c45t1d0
disk       4  255/1/0.0.0          sdisk CLAIMED DEVICE  TEAC   DVD-ROM DW-224EV
          /dev/dsk/c3t0d0      /dev/rdisk/c3t0d0
```

#### NOTE

The host operating system creates a device file for a LUN that is mapped. If the host operating system does not create a device file, you must run the `insf -e` command to create or re-create device files for the existing LUNs.

In the command output, **XXXX** indicates a specific product model or brand.

**Step 3** Run the `ioscan -kfNnC disk` command to query the name of the logical disk mapped to the application server.

```
# ioscan -kfNnC disk
Class      I  H/W Path      Driver S/W State   H/W Type      Description
=====
disk       2  64000/0xfa00/0x0  esdisk CLAIMED DEVICE  HP      DG146BB976
           /dev/disk/disk2  /dev/disk/disk2_p2  /dev/rdisk/
disk2      /dev/rdisk/disk2_p2
           /dev/disk/disk2_p1  /dev/disk/disk2_p3  /dev/rdisk/
disk2_p1   /dev/rdisk/disk2_p3
disk       3  64000/0xfa00/0x1  esdisk CLAIMED DEVICE  HP      DG146BB976
           /dev/disk/disk3  /dev/rdisk/disk3
disk       5  64000/0xfa00/0x2  esdisk CLAIMED DEVICE  TEAC   DVD-ROM DW-224EV
           /dev/disk/disk5  /dev/rdisk/disk5
disk      172  64000/0xfa00/0x58  esdisk CLAIMED DEVICE  ENGENIO INF-01-00
           /dev/disk/disk172 /dev/rdisk/disk172
disk      173  64000/0xfa00/0x59  esdisk CLAIMED DEVICE  ENGENIO INF-01-00
           /dev/disk/disk173 /dev/rdisk/disk173
disk      202  64000/0xfa00/0x5b  esdisk CLAIMED DEVICE  XXXX
           /dev/disk/disk202 /dev/rdisk/disk202
disk      203  64000/0xfa00/0x5c  esdisk CLAIMED DEVICE  XXXX
           /dev/disk/disk203 /dev/rdisk/disk203
disk      204  64000/0xfa00/0x5d  esdisk CLAIMED DEVICE  XXXX
           /dev/disk/disk204 /dev/rdisk/disk204
disk      205  64000/0xfa00/0x5e  esdisk CLAIMED DEVICE  XXXX
           /dev/disk/disk205 /dev/rdisk/disk205
disk      208  64000/0xfa00/0x5f  esdisk CLAIMED DEVICE  XXXX
           /dev/disk/disk208 /dev/rdisk/disk208
```

In the command output, **XXXX** indicates a specific product model or brand.

 **NOTE**

- The disk displayed in the last line is newly mapped to the application server.
- If no new logical disk is detected, troubleshoot the fault and rescan for logical disks. Possible faults include:
  - The application server is incorrectly connected to the storage system after the network cable has been removed and reinserted.
  - The link between the application server and storage system is down.
  - The rate of the Fibre Channel host port is inconsistent with that of the Fibre Channel HBA on the application server.
  - The HBA driver has been uninstalled.
  - The storage pool fails.
  - Multipathing software is not installed or an incorrect version is installed.
  - The device file on the application server is lost.

For details, see **Failure to Discover LUNs by an Application Server** in the *OceanStor V3 Series V300R006 Troubleshooting*.

**Step 4** Create a physical volume.

 **NOTE**

If the PV-Links multipathing software is used, you must create physical volumes for the block devices corresponding to the paths of the LUN.

Run the following command to create a physical volume:

```
# pvcreate /dev/rdisk/disk208
Physical volume "/dev/rdisk/disk208" has been successfully created.
```

In this example, a physical volume is created for the newly mapped `/dev/rdisk/disk208` disk.

**Step 5** Create a physical volume group.

 **NOTE**

If the PV-Links multipathing software is used, you must create a volume group for the LUN. The volume group contains the physical volumes corresponding to the LUN's paths.

1. Create a directory for the physical volume group.

Run the following command to create a directory for the physical volume group:

```
# mkdir /dev/vgmn
```

In this example, the `/dev/vgmn` directory is created for the physical volume group.

2. Create a device file in the newly created directory.

Run the following command to create a device file:

```
# mknod /dev/vgmn/group c 64 0x110000
```

In this example, the name, type, major number, and minor number of the device file are `group`, `c` (*character device*), `64`, and `0x110000` respectively.

 **NOTE**

- The major number of a device file is **64**.
- The minor number is a hexadecimal string in the format of **0xNN0000**, where *NN* indicates the volume group number. The value of *NN* must be unique.

3. Create a physical volume group and allocate physical volumes to it.

Run the following command to create a physical volume group and add physical volumes to it:

```
# vgcreate /dev/vgmn /dev/disk/disk208
```

In this example, the `/dev/vgmn` physical volume group is created and is allocated the `/dev/disk/disk208` physical volume.

The following output is displayed:

```
Increased the number of physical extents per physical volume to 1279.  
Volume group "/dev/vgmn" has been successfully created.  
Volume Group configuration for /dev/vgmn has been saved in /etc/lvmconf/  
vgmn.conf
```

 **NOTE**

This physical volume group contains 1279 partitions.

### Step 6 Create a logical volume.

Run the **lvcreate** command to create a logical volume:

```
# lvcreate -l 279 /dev/vgmn  
Logical volume "/dev/vgmn/lvol1" has been successfully created with  
character device "/dev/vgmn/rlvol1".  
Logical volume "/dev/vgmn/lvol1" has been successfully extended.  
Volume Group configuration for /dev/vgmn has been saved in /etc/lvmconf/vgmn.conf
```

In this example, the `/dev/vgmn/lvoln` logical volume contains 279 partitions. **n** in `lvoln` is automatically assigned by the LVM.

 **NOTE**

When the logical volume is being created, a block device file and a character device file are also created and saved in the `/dev/vgmn` directory.

### Step 7 Create a file system on the logical volume.

Run the **newfs** command to create a file system.

```
# newfs /dev/vgmn/rlvol1  
newfs: /etc/default/fs is used for determining the file system type
```



```
version 6 layout
5238784 sectors, 5238784 blocks of size 1024, log size 16384 blocks
largefiles supported
```

In this example, a file system of the default type is created. To create other types of file system, see the corresponding manual of the HP-UX operating system.

**Step 8** Create a file directory.

Run the following command to create a file directory:

```
# mkdir /directory
```

In this example, the */directory* directory is created.

**Step 9** Mount the logical volume to the file directory.

Run the following command to mount the logical volume to the file directory:

```
# mount /dev/vgmn/lvol1 /directory
```

In this example, the */dev/vgmn/lvol1* logical volume is mounted to */directory*.

----End

## Result

Successful mounting ensures that the application server can read and write the logical disk as a normal disk. Run the **mount** command to check whether the logical disk is properly mounted.

## 3.14.7 Making Storage Space Available (VMware)

This section uses a VMware ESXi.5.1.0 application server and datastores based on VMFS-5 file system configuration as an example to introduce how to make the storage space available to a VMware-based application server. For application servers running other versions of VMware operating systems, adjust the operations based on actual conditions.

### Context

You can use any of the following methods to make the storage space available to a VMware-based application server:

- Device-based method  
After a mapped device is detected on the application server, use the device to configure disks for a VM.
- Datastore-based method  
After a mapped device is detected on the application server, create a corresponding file system and use the storage space. Datastore is a common method to help you use the storage space.

### Procedure

**Step 1 Optional:** Configure the multipathing software information.

The VMware system has its own multipathing software NMP. You can directly use this software without the need to configure it. If you use UltraPath, see your UltraPath document.

If you use NMP, the recommended configuration is as follows:

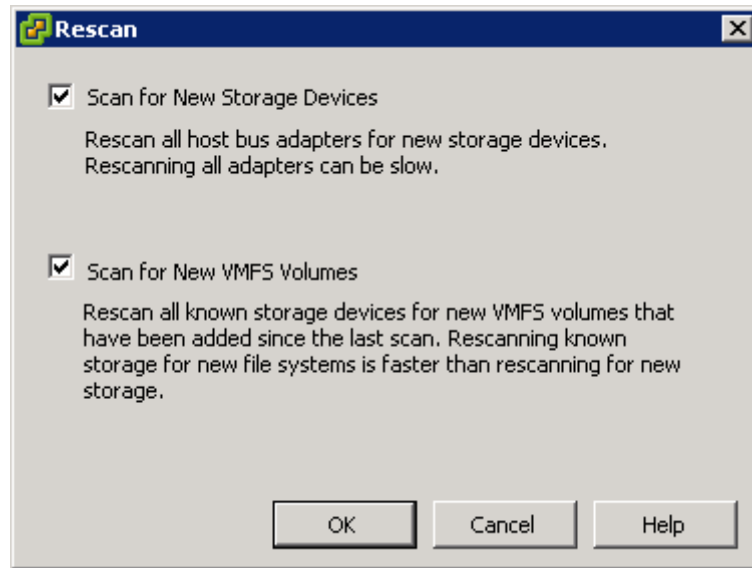
Storage Type	Number of Existing and Planned Controllers	ALUA Enabled or Not (Y/N)	Storage VM Cluster or Not	Recommended SATP Type	Recommended PSP Type
ESXi 5.0 & 5.0 updated version					
2000, 5000, 6000 and 18000 series storage systems	≤ 2 controllers	Y	N/A	VMW_SATP_ALUA	VMW_PSP_FIXED
	≥ 4 controllers	N	N/A	VMW_SATP_DEFAULT_AA	VMW_PSP_FIXED
ESXi 5.1 & 5.1 updated version					
2000, 5000, 6000 and 18000 series storage systems	≤ 2 controllers	Y	Y	VMW_SATP_ALUA	VMW_PSP_FIXED
			N	VMW_SATP_ALUA	VMW_PSP_FIXED
	≥ 4 controllers	N	N/A	VMW_SATP_ALUA	VMW_PSP_RR
				VMW_SATP_DEFAULT_AA	VMW_PSP_FIXED
ESXi 5.5 & 5.5 updated & 6.0 & 6.0 updated version					
2000, 5000, 6000 and 18000 series storage systems	≤ 2 controllers	Y	N/A	VMW_SATP_ALUA	VMW_PSP_FIXED
				VMW_SATP_ALUA	VMW_PSP_RR
	≥ 4 controllers	N	N/A	VMW_SATP_DEFAULT_AA	VMW_PSP_FIXED

**Step 2** Go to the **Add Storage** dialog box.

1. On the vSphere Client, click the **Configuration** tab.
2. On the navigation bar, click **Storage**.
3. On the **Storage** page, click the **Devices** tab and click **Rescan All**.

The **Rescan** dialog box is displayed, as shown in [Figure 3-66](#).

Figure 3-66 Rescan dialog box



- 4. Click **OK**.

It takes 2 to 4 minutes to scan for new storage devices and virtual machine file system (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 3-67](#), the scanning is ongoing.

Figure 3-67 Scanning ongoing

Name	Target	Status	Details	Initiated by	vCenter Server	Requested Start Time	Start Time	Completed Time
Rescan VMFS		In Progress		Administrator	win232.zcyunhws...	8/19/2013 6:47:46 PM	8/19/2013 6:47...	
Rescan all HBAs		In Progress		Administrator	win232.zcyunhws...	8/19/2013 6:46:58 PM	8/19/2013 6:46...	

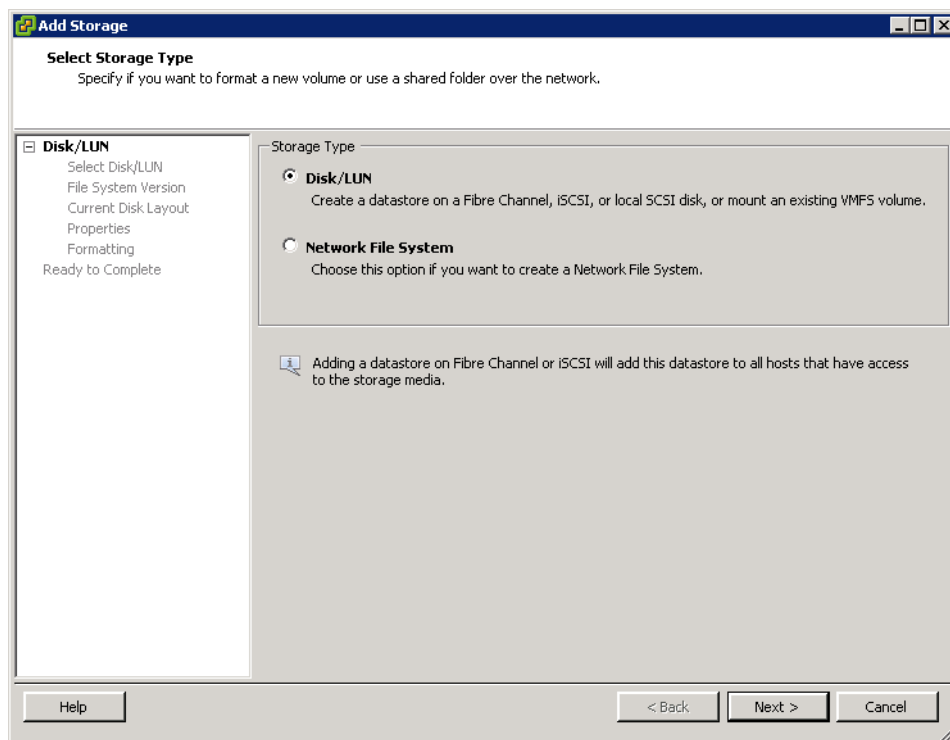
- If the task status is **Completed** as shown in [Figure 3-68](#), the scanning is completed.

Figure 3-68 Scanning completed

Name	Target	Status	Details	Initiated by	vCenter Server	Requested Start Time	Start Time	Completed Time
Rescan VMFS		Completed		Administrator	win232.zcyunhws...	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.zcyunhws...	8/19/2013 6:46:58 PM	8/19/2013 6:46...	8/19/2013 6:47:46 PM

- 5. On the **Storage** page, click the **Datastores** tab and click **Add Storage**. The **Add Storage** dialog box is displayed, as shown in [Figure 3-69](#).

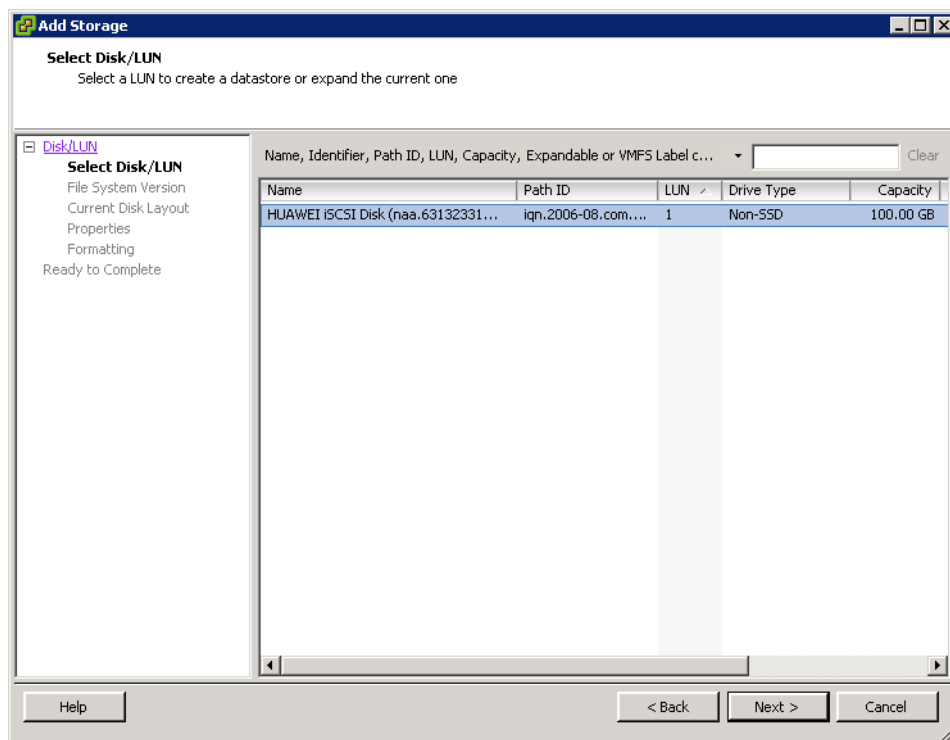
**Figure 3-69** Add Storage dialog box



**Step 3** Configure datastore parameters.

1. Select **Disk/LUN** for **Storage Type** and click **Next**.
2. Select the LUN mapped from the storage system and click **Next**, as shown in [Figure 3-70](#).

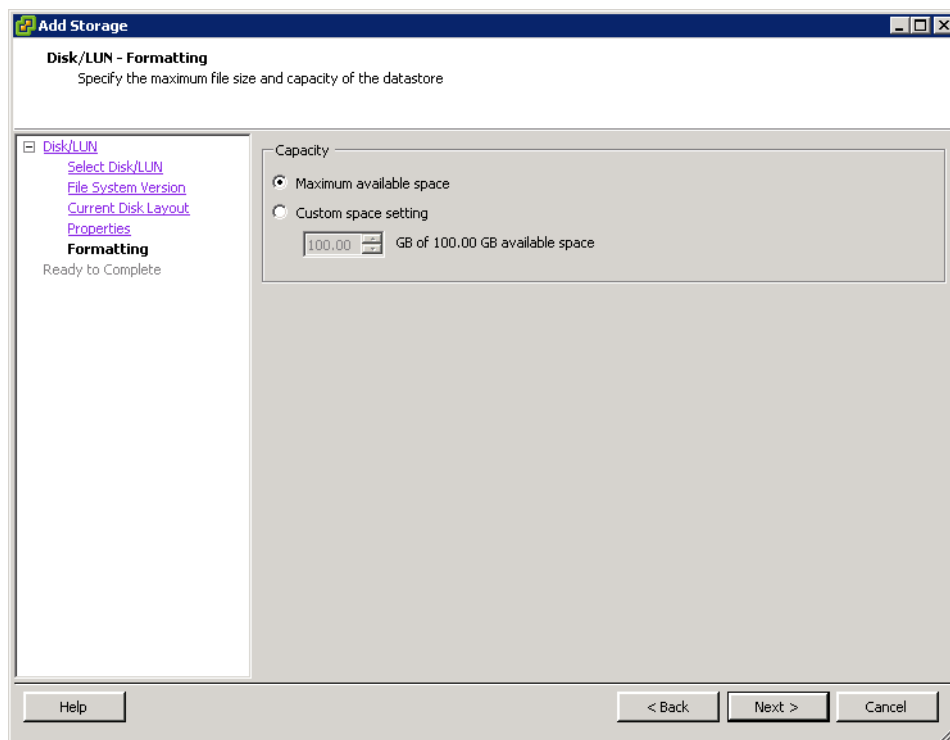
Figure 3-70 Select Disk/LUN page



 **NOTE**

- If multiple LUNs appear on the interface, you can distinguish them from each other by WWN.
  - To query the WWN of a LUN on the DeviceManager, choose **Resource Allocation > View and Management > LUNs**.
3. Select **VMFS-5** for **File System Version** and click **Next**.
  4. Confirm the disk layout and click **Next**.
  5. Enter a name for the datastore and click **Next**.
  6. Configure the disk capacity and click **Next**, as shown in [Figure 3-71](#). In normal cases, configure the maximum available space.

**Figure 3-71** Configuring disk capacity



**Step 4** Confirm the configurations and click **OK**.

It takes 3 to 5 minutes to create a datastore. You can check the task status in the **Recent Tasks** area at the lower part of the main window.

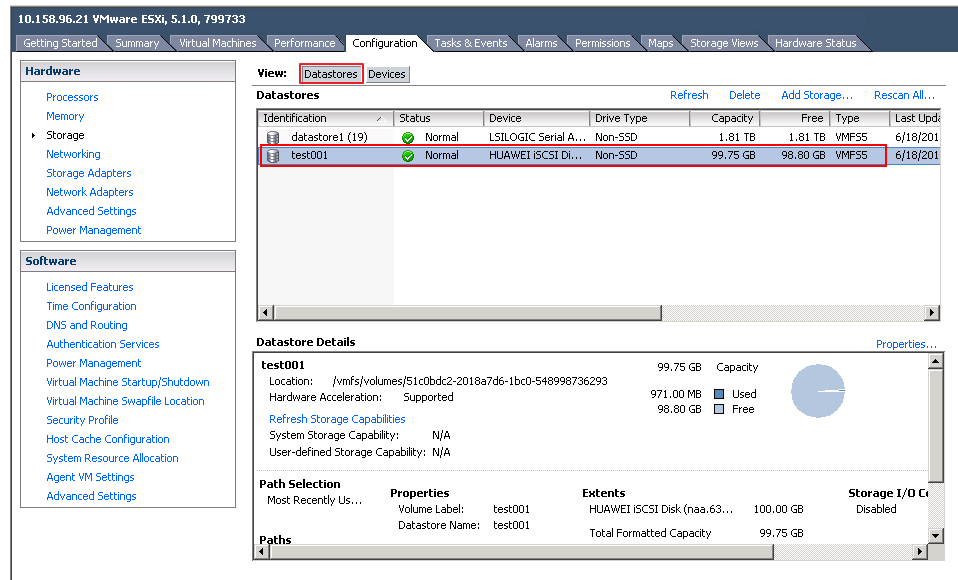
- If the task status is **In Progress**, the datastore is being created.
- If the task status is **Completed**, the datastore has been created.

----End

## Result

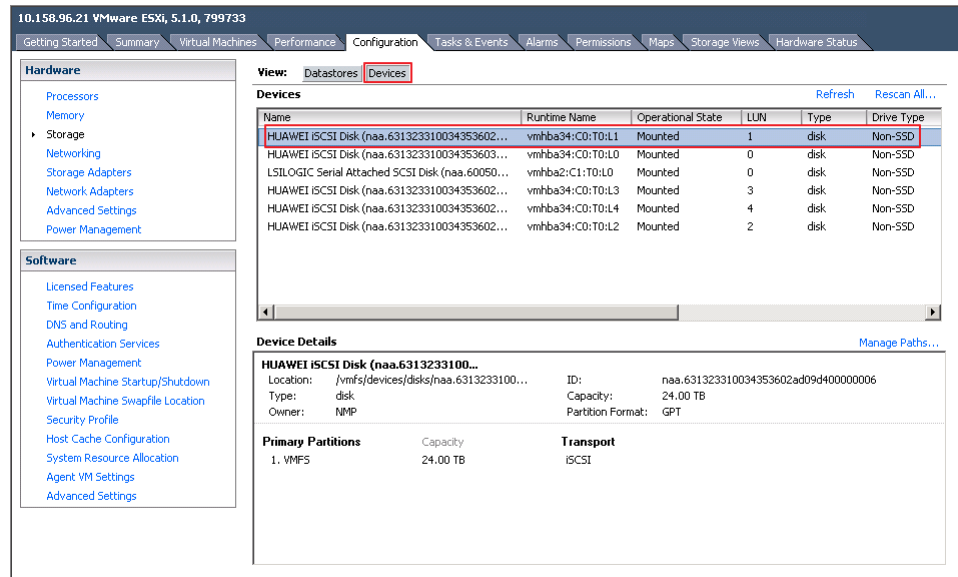
- On the **Datastores** tab page, you can view the newly configured datastores, as shown in [Figure 3-72](#).

Figure 3-72 Viewing datastore



- On the **Devices** tab page, you can view the newly scanned devices, as shown in [Figure 3-73](#).

Figure 3-73 Viewing devices



### 3.14.8 Making Storage Space Available (Hyper-V)

This section describes how to enable a Hyper-V application server to use the space of a storage system.

## Prerequisites

- The Hyper-V role has been installed on the Windows Server.
- Hyper-V VMs have been created in the Hyper-V manager.
- Guest operating systems have been installed in Hyper-V VMs. Windows Server 2008 is used as an example.

## Context

Hyper-V is a Microsoft VM and is deployed in Windows 8.0 (64-bit) Pro or later versions and Windows Server 2008 or later versions.

Hyper-V VMs can be connected to storage using the following methods: virtual hard disks, pass-through disks, direct iSCSI disks, and direct connection to the storage through virtual Fibre Channel. This section only introduces the two common methods: connection through virtual hard disks and pass-through disks. In these two methods, VMs can directly access physical disks connected to a Hyper-V host machine, namely LUNs of the storage must be visible to the host machine. After a storage system creates and maps LUNs to a Hyper-V host machine, Hyper-V VMs run on these LUNs.

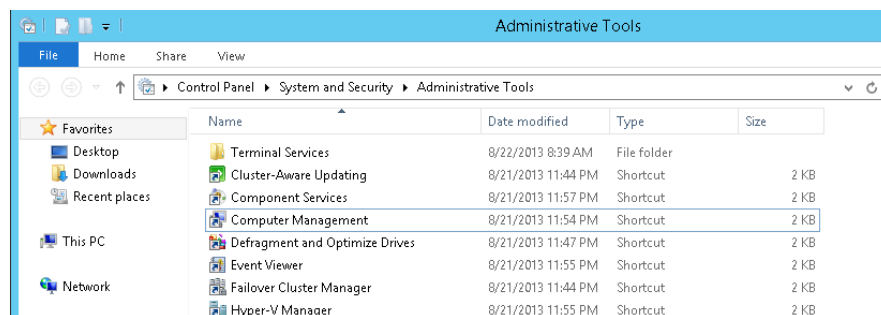
## Procedure

**Step 1** Map LUNs created on the storage system to a physical server running Windows Server 2012.

1. Go to **Disk Management**.

In **Start**, click **Administrative Tools**. In the dialog box that is displayed, double-click **Computer Management**, as shown in [Figure 3-74](#).

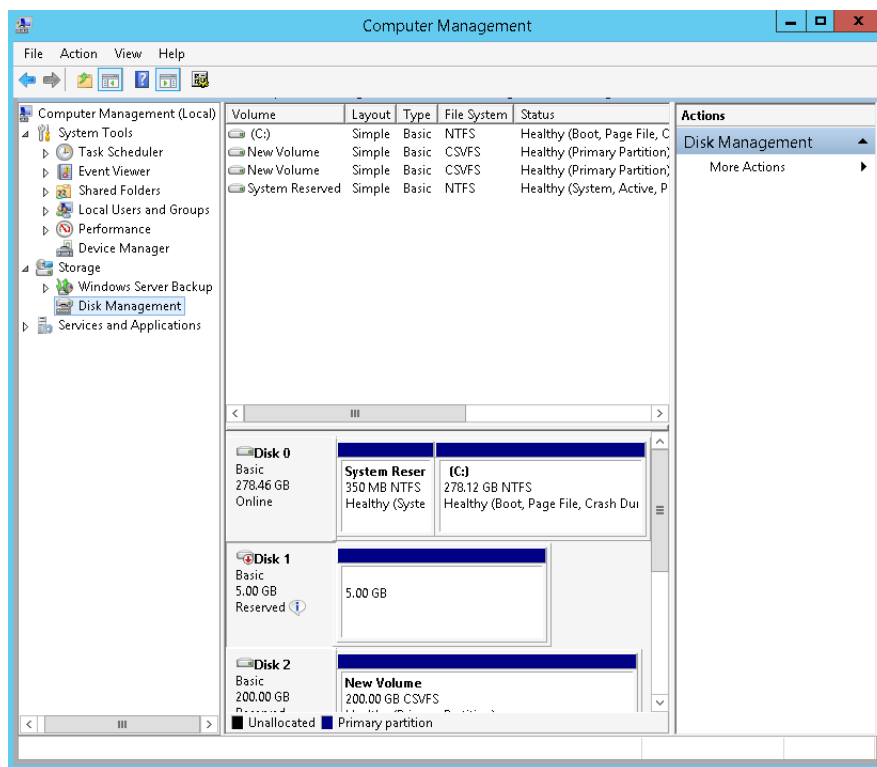
**Figure 3-74** Administrative Tools dialog box



2. Scan for new logical disks on the application server.
  - a. In the navigation tree of the **Computer Management** dialog box, choose **Storage > Disk Management**.
  - b. Right-click **Disk Management**. In the shortcut menu that is displayed, choose **Rescan Disks**. The results are shown in [Figure 3-75](#).



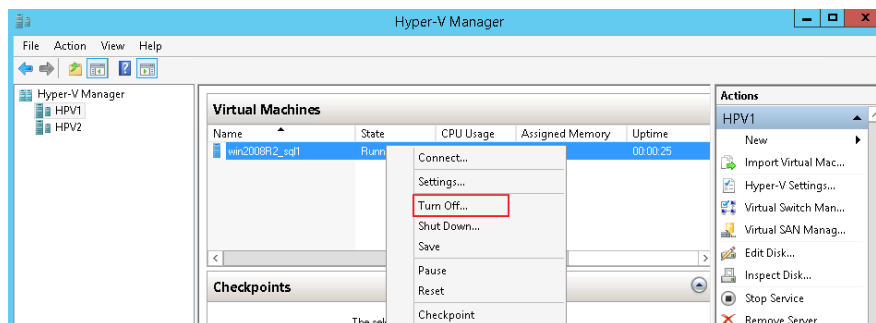
Figure 3-75 Scanning for new logical disks on the application server



**Step 2** Disable a Hyper-V VM.

1. On the Windows 2012 server, choose **Start > Administrative Tools > Hyper-V Manager** to open the **Hyper-V Manager** dialog box.
2. In the **Hyper-V Manager** dialog box, right-click the name of the VM and choose **Turn Off** to disable the VM, as shown in [Figure 3-76](#).

Figure 3-76 Disabling a Hyper-V VM

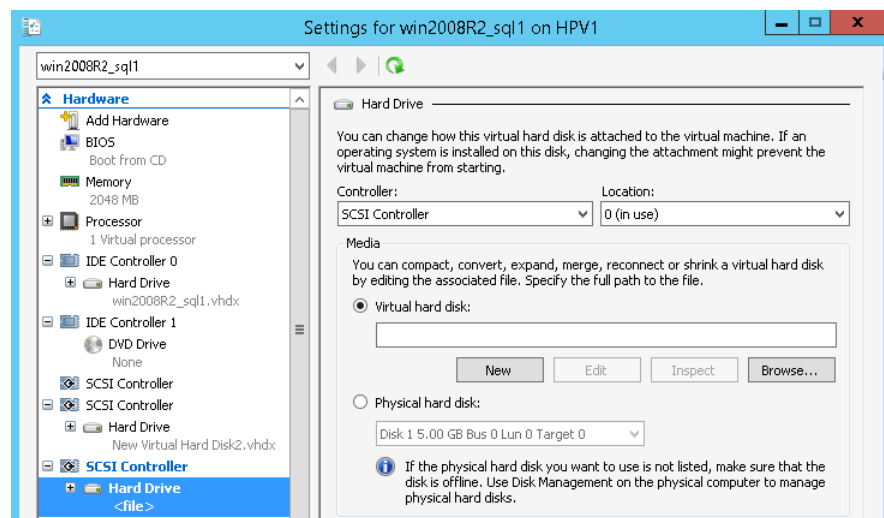


**Step 3** Allocate storage space to the VM.

You can use one of the following methods to allocate storage space to a Hyper-V VM based on your service requirements.

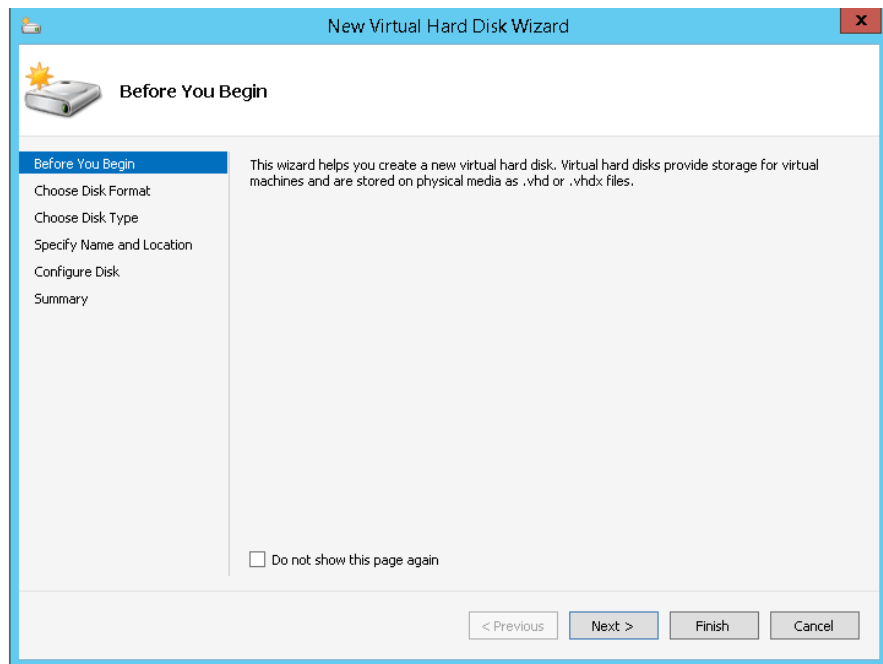
- Add virtual disks to a Hyper-V VM.
  - a. Initialize and format disks that are newly mapped to the host machine. For details, see [3.14.1 Making Storage Space Available \(Windows\)](#).
  - b. Right-click the name of the VM and choose **Setting > Add Hardware > SCSI Controller**. Click **Add**.
  - c. Select **Hard Drive** and click **Add** to go to the **Hard Drive** tab page.
  - d. Choose **Virtual hard disk > New** to go to the **New Virtual Hard Disk Wizard** dialog box, as shown in [Figure 3-77](#).

**Figure 3-77** Creating a Virtual hard disk



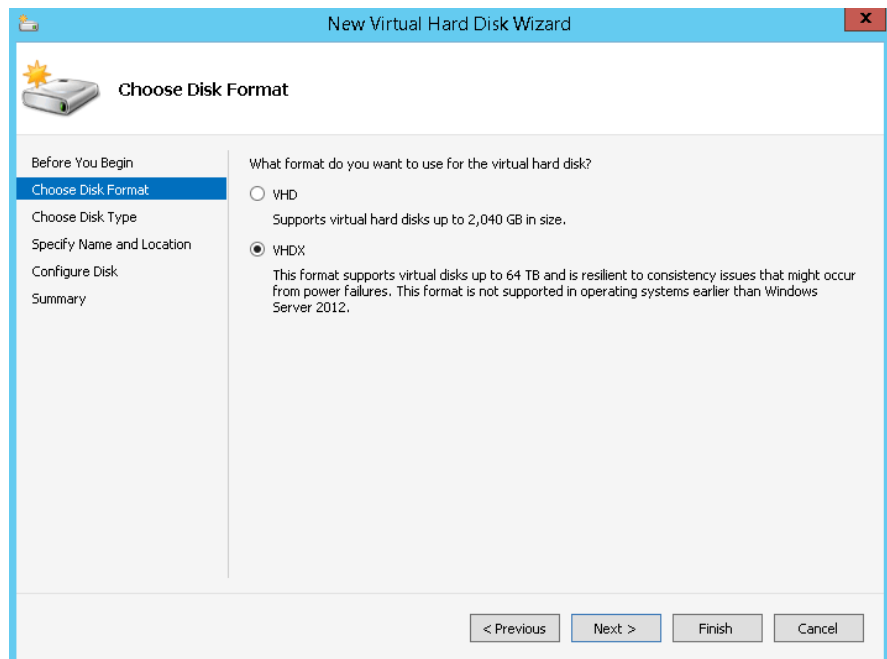
- e. In the **New Virtual Hard Disk Wizard** dialog box, set the properties of a virtual disk.

**Figure 3-78** Setting the properties of the virtual disk



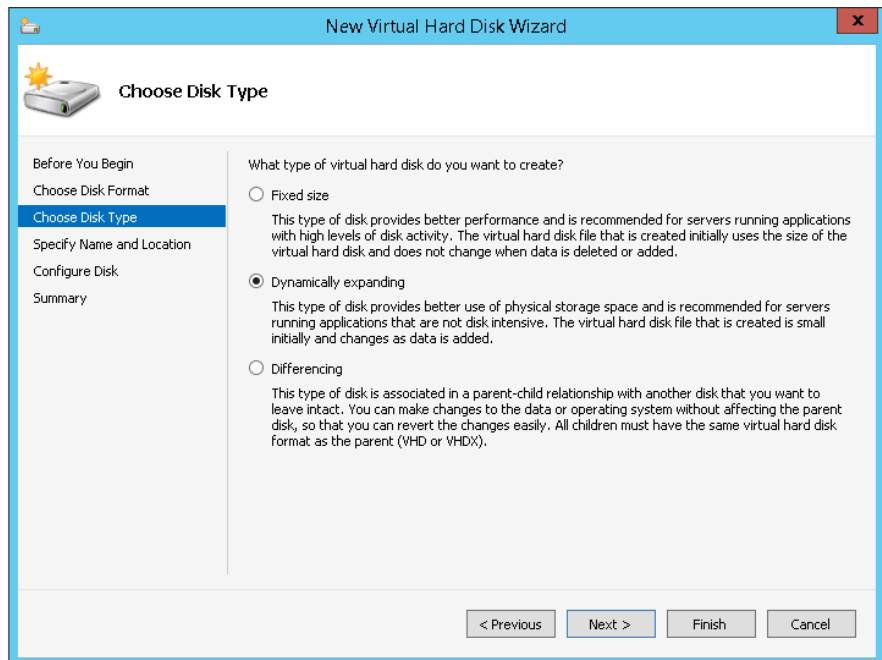
- i. On the **Before You Begin** page, click **Next**.
- ii. On the **Choose Disk Format** page, set the format of the virtual disk. Click **Next**. **Table 3-26** describes the related parameters.

**Figure 3-79** Format of a virtual disk



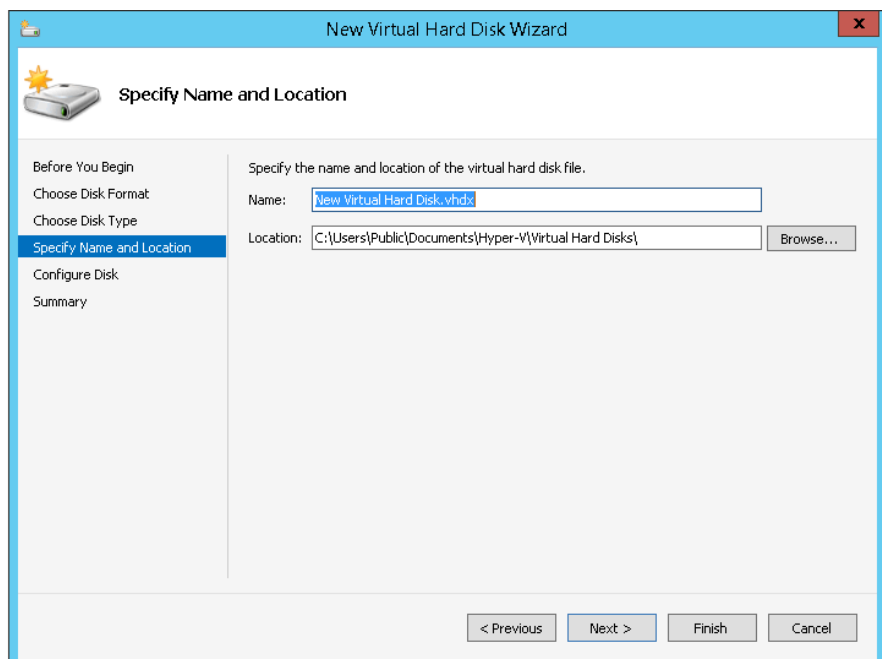
- iii. On the **Choose Disk Type** page, select the type of the virtual disk. Click **Next**. [Table 3-26](#) describes the related parameters.

**Figure 3-80** Type of a virtual disk



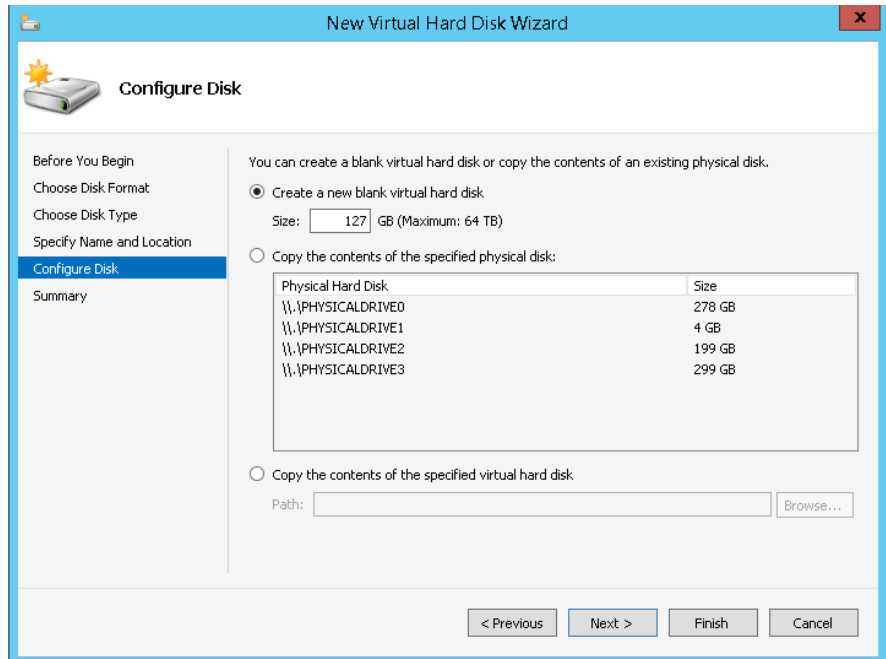
- iv. On the **Specify Name and Location** page, set the name and saving path of the new virtual disk. Click **Next**.

**Figure 3-81** Specifying the name and saving path



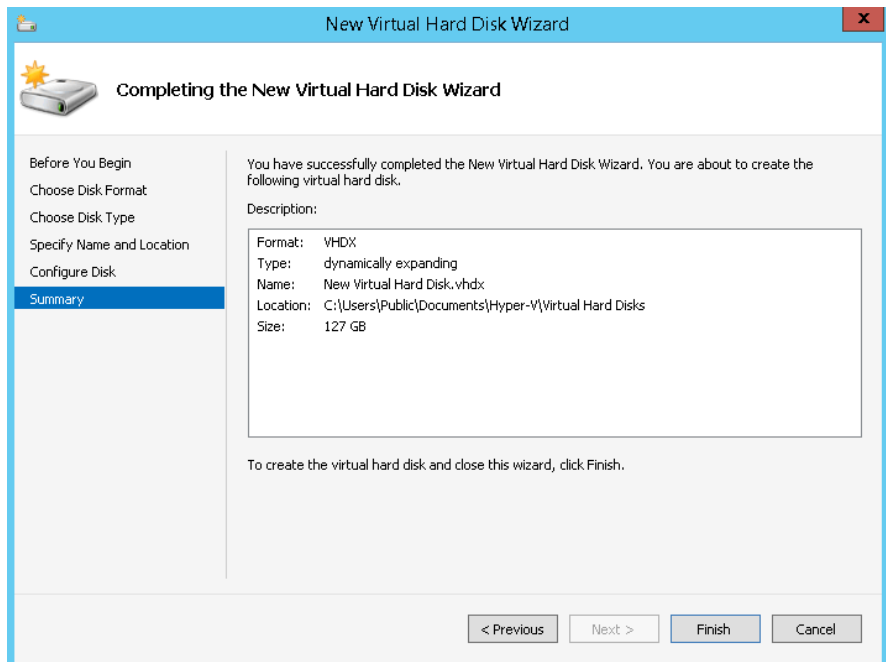
- v. On the **Configure Disk** page, create a blank virtual disk and set its size or copy the contents of a physical or virtual disk. Then, create a virtual disk based on the contents of the disk. Click **Next**.

**Figure 3-82** Configuring a disk



- vi. View details about the created virtual disk. Click **Finish** to finish adding the virtual disk file.

**Figure 3-83** Viewing the created virtual disk



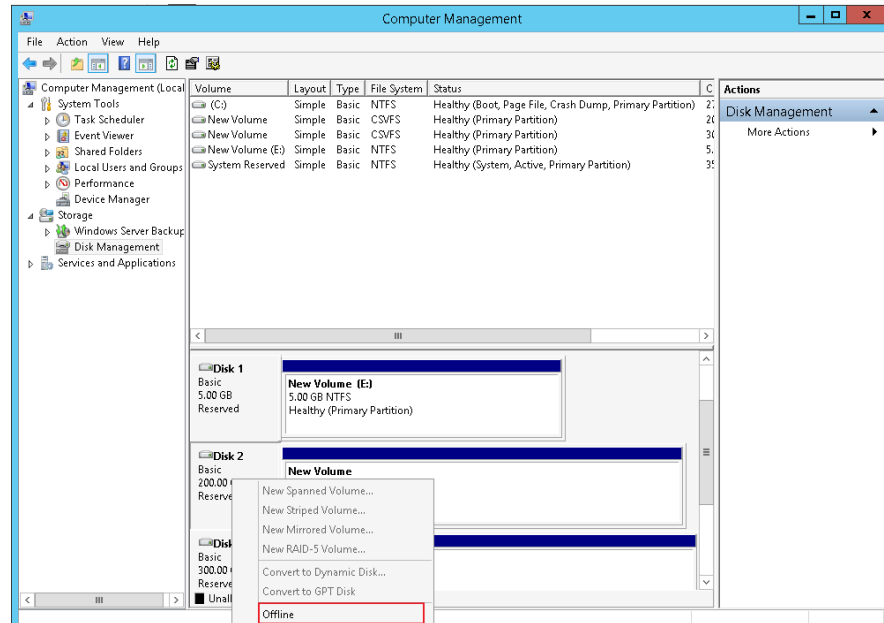
**Table 3-26** Description about parameters used for configuring a virtual disk

Parameter	Description	Value
Virtual disk format	<ul style="list-style-type: none"> <li>■ VHD: Microsoft virtual disk file. Maximum virtual disk capacity: 2040 GB</li> <li>■ VHDX: A new VHD version used for Windows Server 2012 Hyper-V. Maximum virtual disk capacity: 64 TB.</li> </ul>	[Default value] <b>VHDX</b> <b>NOTE</b> Compared with VHD, VHDX has a larger capacity. VHDX provides data protection upon a power failure and optimizes the structure alignment mode of dynamic and differentiated disks to prevent performance degradation in new physical disks with large sectors.
Type of a virtual disk	<ul style="list-style-type: none"> <li>■ Fixed size: VHD storage space allocated to the VHD file system at a time no matter whether data is stored in the created VHD.</li> <li>■ Dynamically expanding: The storage system does not allocate space to the LUNs at a time. Instead, it gradually increases the capacity for the LUNs as more data is written in to the LUNs.</li> <li>■ Differencing: Similar to an expandable VHD, a differencing VHD needs to designate a parent VHD. Differencing VHDs only contain the modified data of all related parent VHDs.</li> </ul>	[Default value] <b>Dynamically expanding</b>

- f. Click **Finish** to finish creating a virtual disk.
- Add physical disks to a Hyper-V VM.

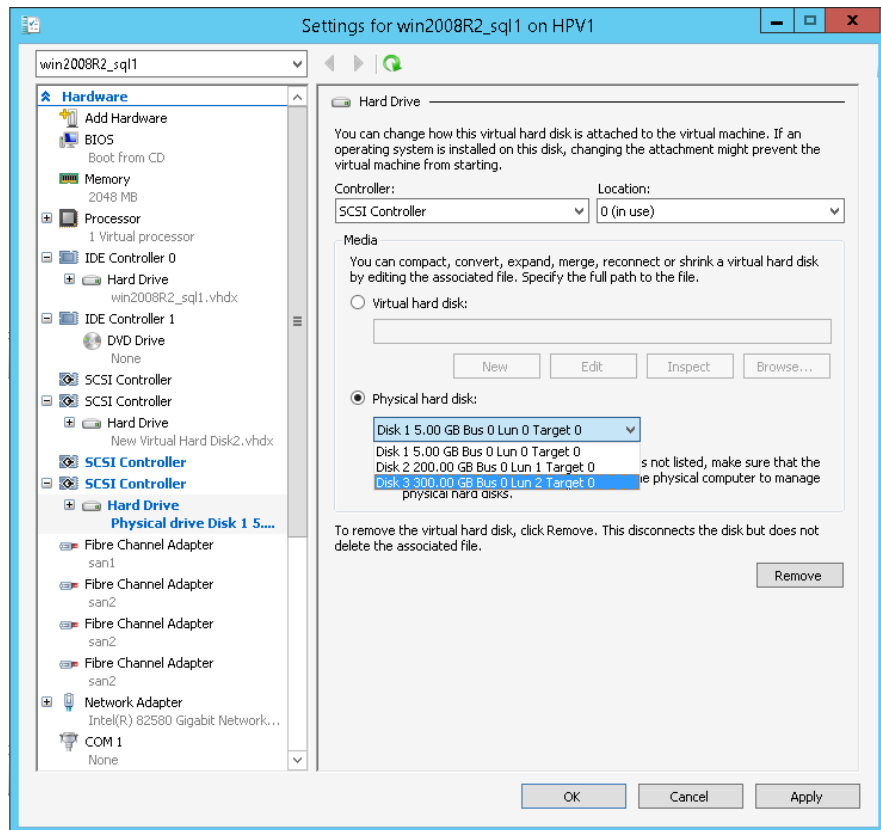
- a. In **Disk Management**, right-click the disk that you want to add to the Hyper-V VM, and select **Offline**.

**Figure 3-84** Taking a VM disk offline



- b. In the **Hyper-V Manager** dialog box, right-click the name of a VM and choose **setting > Add Hardware > SCSI Controller**. Then click **Add**.
- c. Select **Hard Drive** and click **Add**.
- d. Click **Physical hard disk** and select the disk that you want to add, as shown in [Figure 3-85](#).

Figure 3-85 Adding a physical disk



**NOTE**

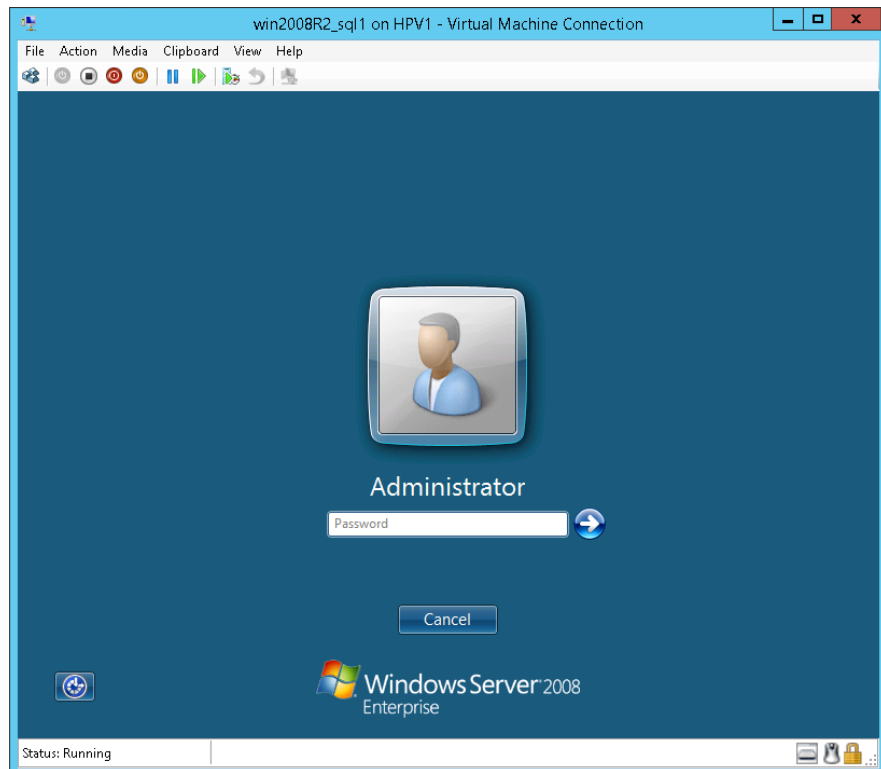
A VM must have exclusive access permission to a physical disk. If two VMs can access one physical disk at the same time, the VM may fail to be started.

**Step 4** Log in to the VM and scan for disks.

1. Log in to the VM.
  - a. In the **Hyper-V Manager** dialog box, right-click the name of the VM and choose **Start** to power on the VM.
  - b. Double-click the name of the VM to enable the VM.
  - c. Log in to the Hyper-V VM as **Administrator** and enter the password, as shown in [Figure 3-86](#).

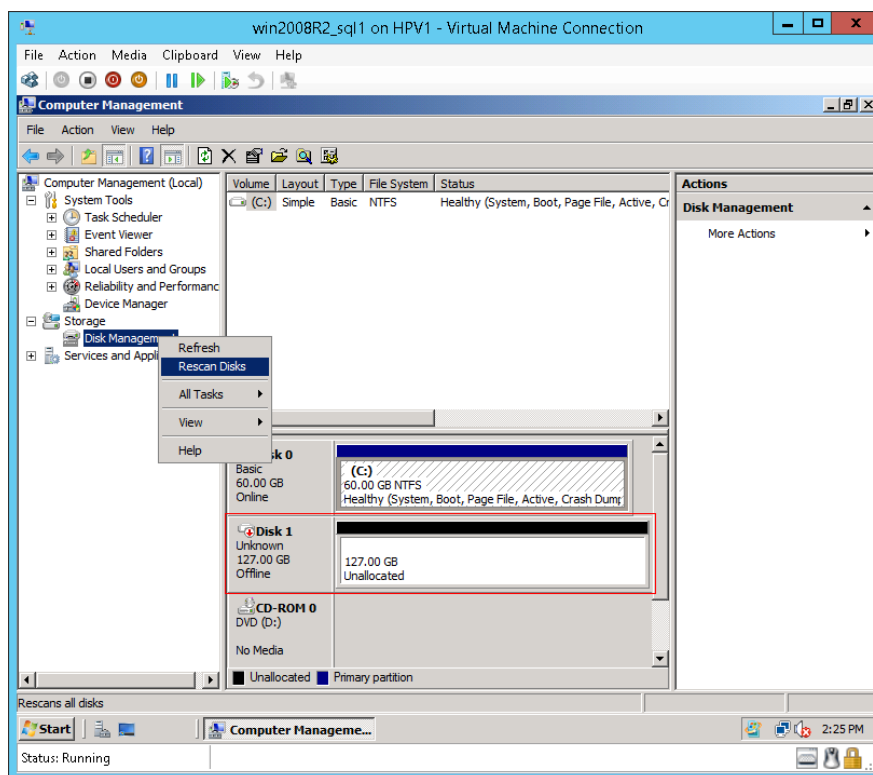


**Figure 3-86** Logging in to a Hyper-V application server



2. Scan for disks on the VM.
  - a. Choose **Start > Administrative Tools > Computer Management** to go to the **Computer Management** dialog box.
  - b. In the navigation tree of the **Computer Management** dialog box, choose **Storage > Disk Management**.
  - c. Right-click **Disk Management**. In the shortcut menu that is displayed, choose **Rescan Disks**. The results are shown in [Figure 3-87](#).

**Figure 3-87** Viewing newly added logical disks



- d. For details about how to initialize detected disks, see [3.14.1 Making Storage Space Available \(Windows\)](#).

----End

### 3.15 Performing an Emergency Rollback

If a newly created storage resource does not meet service requirements, you must roll it back. Rollback operations vary depending on different configuration operations. For details, see [Table 3-27](#).

**Table 3-27** Emergency rollback procedure

Configuration Process	Completed Operation	Rollback Operation
Preparing for configuration	Checking software installation	N/A
	Checking initial configuration	
	Logging in to the DeviceManager	

Configuration Process	Completed Operation	Rollback Operation
Creating storage space	<ul style="list-style-type: none"> <li>● Creating a disk domain</li> <li>● Creating a storage pool</li> <li>● Creating a LUN</li> <li>● Creating a LUN group</li> </ul>	<ol style="list-style-type: none"> <li>1. Delete a LUN group. For details, see <a href="#">6.7.6 Deleting a LUN Group</a>.</li> <li>2. Delete a LUN. For details, see <a href="#">6.6.7 Deleting a LUN</a>.</li> <li>3. Delete a storage pool. For details, see <a href="#">6.5.8 Deleting a Storage Pool</a>.</li> </ol>
Configuring host connectivity and establishing a connection	<ul style="list-style-type: none"> <li>● Configuring host connectivity</li> <li>● Creating a host</li> <li>● Creating a host group</li> <li>● <b>Optional:</b> Creating a port group</li> <li>● Creating a mapping view</li> </ul>	<ol style="list-style-type: none"> <li>1. Delete a mapping view. For details, see <a href="#">6.11.3 Deleting a Mapping View</a>.</li> <li>2. <b>Optional:</b> Delete a port group. For details, see <a href="#">6.10.4 Deleting a Port Group</a>.</li> <li>3. Delete a host group. For details, see <a href="#">6.9.5 Deleting a Host Group</a>.</li> <li>4. Delete a host. For details, see <a href="#">6.8.7 Deleting a Host</a>.</li> <li>5. Disconnect the connection of the storage system, application server, and switch, and delete the VLAN or zone configuration.</li> </ol>

# 4 Configuring Basic Storage Services (for VMware VVol Scenarios Only)

---

## About This Chapter

VVol is a new function in VMware ESXi 6.0. VVol can be used to provide storage resources in the VM unit. The operations of more VMs are delivered to storage systems. In this way, storage resources are fully utilized. The VVol technology lays a foundation for VM I/O isolation and storage's VM awareness.

### Problems Faced with VMware If VMware Uses Traditional Storage

In an environment where VMware uses traditional storage, three parts are involved: VMware Virtual Machine Disk Format (VMDK), VMware VMFS, and storage devices.

VMs appear as independent VMDK files on a storage device. VMs execute clone, snapshot, and recovery in the VMDK form. The operations of the virtual software are performed on VMDK files of the storage device. The execution efficiency of the operations is lower than that of clone, snapshot, and recovery on the storage device. For storage, the operations of VMs are LUN-based. The operations such as clone and snapshot are also related to LUNs. The configuration of a LUN on a VM is difficult to adapt to the VMDK of all storage devices. As a result, the VMDK does not match the LUN.

VMDK and storage do not sense each other. VVol combines storage and VMDK to meet user requirements for storage configuration on each VM, achieving flexible and efficient VM-based management at the storage level.

### Advantages of VM-Level Granularity

VVol can be used to provide storage resources in the VM unit. The operations of more VMs are delivered to storage systems. In this way, storage resources are fully utilized. Advantages of VM-level granularity are listed as follows:

- Simple management and rapid deployment

When VVol is used to create VMs, VMware directly obtains storage resources from the storage system, resolving the issues of managing multiple VMs in a single LUN through VMDK. Each VVol LUN corresponds to a VM, while a VM can correspond to multiple VVol LUNs.

- High storage utilization  
When VVol is used to create VMs, VMs dynamically obtain storage resources on demand, delivering better storage utilization than the VMDK mode.
- Reduced required computing and network resources  
When VVol is used to create VMs, VMware delivers VM clone, snapshot, recovery, and other operations to the storage system, quickly releasing VMware resources while substantially reducing required computing and network resources.

## Basic Concepts

VVol involves the following concepts:

- Virtual volume  
A virtual volume is an object that is exported from a storage system. The virtual volume is managed in the storage system, identified by a unique GUID, and used to encapsulate VM files, VM disks, and derivative files. Using a specialized API such as vSphere APIs for Storage Awareness (VASA), the storage system can sense the contents related to the virtual volume. VVol is a basic storage unit provided by a storage system to the virtualization layer. VVols and VM files are in a one-to-one relationship. Generally, a VM contains multiple files such as the configuration file, data file, and memory file.
- Storage container  
A storage container is an original storage pool or storage function set provided by a storage system. As the container of virtual volumes, the storage container allocates storage space to the virtual volumes. The storage container is defined by storage system administrators.
- PE  
ESXi hosts cannot directly access virtual volumes. The ESXi hosts must use PEs as logical I/O proxies. A PE is a hybrid read and write channel used to connect the ESX and storage array. A PE simplifies the I/O connections between hosts and storage devices. The meshed connection mode becomes many-to-one connection mode. In this way, the heterogeneity problem is eliminated between different storage devices.
- Virtual DataStore  
A storage container is expressed as a Virtual DataStore on the vCenter Server and vSphere Web Client. For a vSphere administrator, a Virtual DataStore is similar to a traditional datastore. When creating a Virtual DataStore, you must select the VVol type.

## VASA Provider

VASA Provider 2.0 (VASA Provider for short) is developed by Huawei and meets the VASA standard. It enables vCenter Server to manage Huawei storage devices. VASA Provider supports VVol.

### [4.1 Configuration Process](#)

The configuration process describes the overall procedures for configuring the storage space in the VVol scenario.

### [4.2 Logging In to the DeviceManager](#)

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

### [4.3 Creating a Disk Domain](#)

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

#### 4.4 Creating a Storage Pool

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

#### 4.5 Creating a PE LUN

When using VVol, you must set LUNs to the PE type.

#### 4.6 Creating a LUN Group

To allow hosts to use PE LUNs, you must add the PE LUNs into LUN groups. Then, establish mapping views between the LUN groups and host groups. In doing so, the hosts in the host groups can use the PE LUNs in the LUN groups. A LUN group can contain one to multiple PE LUNs.

#### 4.7 Configuring Connectivity between Host and Storage System

This section describes how to configure the connectivity between host and storage system through iSCSI networking or FC networking.

#### 4.8 Creating a Host

Create a host to establish a connection between a storage system and an application server, and add an initiator for the host to establish a mapping relationship between the host and application server.

#### 4.9 Creating a Host Group

To allow hosts to use LUNs, you must add hosts into host groups. Then, establish mapping views between the LUN groups and host groups. By doing so, the hosts in the host groups can use the LUNs in the LUN groups. A host group can contain one or multiple hosts.

#### 4.10 (Optional) Creating a Port Group

A port group is a logical combination of multiple physical ports. The storage system specifies ports to set up mappings between storage resources (LUNs) and servers. This operation enables you to create a port group and add it to a mapping view. After that, LUNs of a specified LUN group use the ports of the port group to communicate with the corresponding hosts of the host group. If no port group is added to the mapping view, available ports are randomly used. A port group can be added to a maximum of 64 mapping views. A port can be added to a maximum of 64 port groups.

#### 4.11 Creating a Mapping View

This operation enables you to create a mapping view and manage the mapping relationship between multiple host groups and LUN groups by adding them to the mapping view.

#### 4.12 Configuring the VVols Function

Install VASA Provider to provide the Virtual Volumes (VVols) function.

#### 4.13 Using a VVOL Datastore to Create a VM

This section describes how to use a virtual datastore to create a VM.

## 4.1 Configuration Process

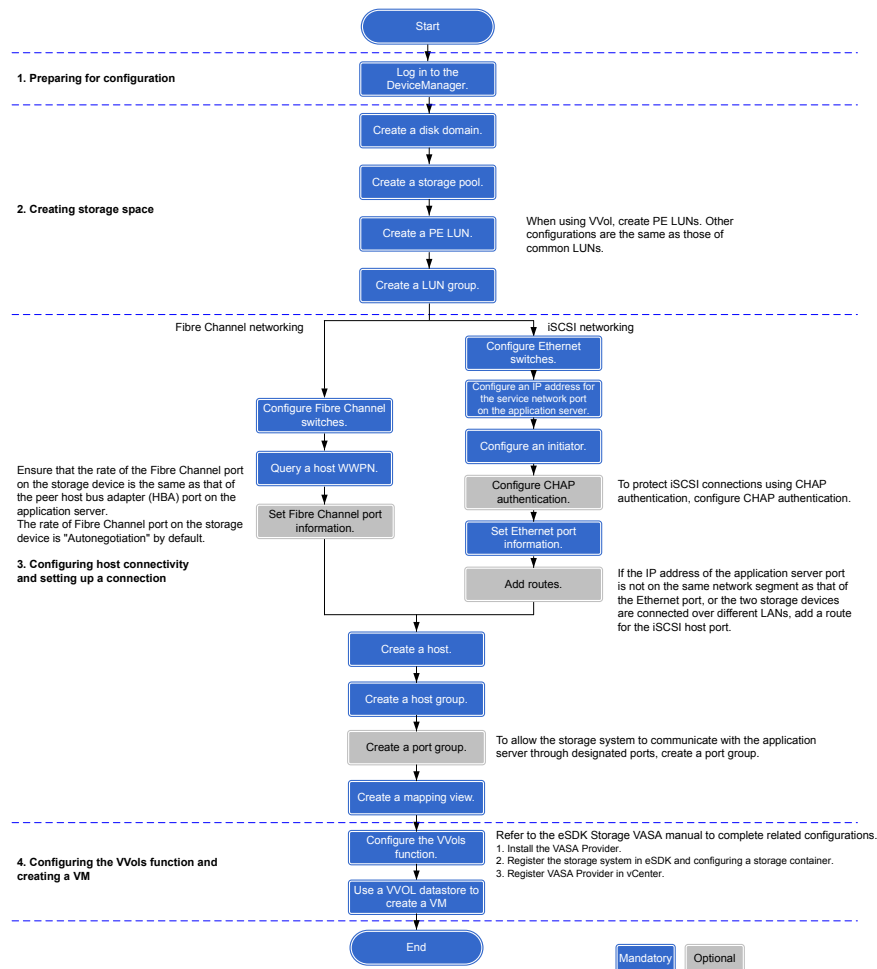
The configuration process describes the overall procedures for configuring the storage space in the VVol scenario.

**NOTE**

If the storage system requires the VVol function, you must purchase licenses for SmartThin, SmartQoS, HyperCopy, and HyperSnap.

Figure 4-1 shows the process for configuring VVol.

**Figure 4-1** Process for configuring VVol



**Table 4-1** Process for configuring VVol

Procedure	Operation	Reference
1. Preparing for configuration	Logging in to the DeviceManager	<a href="#">4.2 Logging In to the DeviceManager</a>
2. Creating storage space	Creating a disk domain	<a href="#">4.3 Creating a Disk Domain</a>
	Creating a storage pool	<a href="#">4.4 Creating a Storage Pool</a>
	Creating a PE LUN	<a href="#">4.5 Creating a PE LUN</a>

Procedure	Operation	Reference
	Creating a LUN group	<a href="#">4.6 Creating a LUN Group</a>
3. Configuring host connectivity and setting up a connection	Configuring connectivity between host and storage system	<a href="#">4.7 Configuring Connectivity between Host and Storage System</a>
	Creating a host	<a href="#">4.8 Creating a Host</a>
	Creating a host group	<a href="#">4.9 Creating a Host Group</a>
	(Optional) Creating a port group	<a href="#">4.10 (Optional) Creating a Port Group</a>
	Creating a mapping view	<a href="#">4.11 Creating a Mapping View</a>
4. Configuring the VVols function and creating a VM	<p>Configuring the VVols function</p> <p>Refer to the eSDK Storage VASA manual to complete related configurations.</p> <ol style="list-style-type: none"> <li>1. Installing the VASA Provider</li> <li>2. Registering the storage system in eSDK and configuring a storage container</li> <li>3. Registering VASA Provider in vCenter</li> </ol> <p><b>NOTE</b></p> <p>Log in to <a href="http://support.huawei.com/enterprise/">http://support.huawei.com/enterprise/</a>, and apply for an account and password. Log in to the system using the user name and password that you have applied for. In the search field, enter <b>eSDK Storage Plugins</b>. Select the path that is automatically associated with this parameter. Go to the documentation page to download the <i>Quick Guide (VASA2.0)</i> of the required version.</p>	<a href="#">4.12 Configuring the VVols Function</a>
	Using a VVOL datastore to create a VM	<a href="#">4.13 Using a VVOL Datastore to Create a VM</a>

## 4.2 Logging In to the DeviceManager

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



## 4.2.1 Logging In to the DeviceManager Through Web

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

### Prerequisites

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

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

### Context

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

### Procedure

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

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

 **NOTE**

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

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

1. Click **Advanced**.
2. From the **Authentication Mode** list, select an authentication mode.
  - Local user: You will log in to the storage system in local authentication mode.  
The super administrator can log in to the storage system using the local user authentication mode only.
  - LDAP user: You will log in to the storage system in LDAP domain authentication mode.  
You can log in to the storage system in LDAP domain authentication mode only after the LDAP server is properly configured.
3. Choose a language from the **Language** list.

 **NOTE**

DeviceManager supports two languages: simplified Chinese and English.

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

 **NOTE**

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

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

The DeviceManager home page is displayed.

**Figure 4-2** shows the home page of the DeviceManager.

Figure 4-2 Home page of the DeviceManager

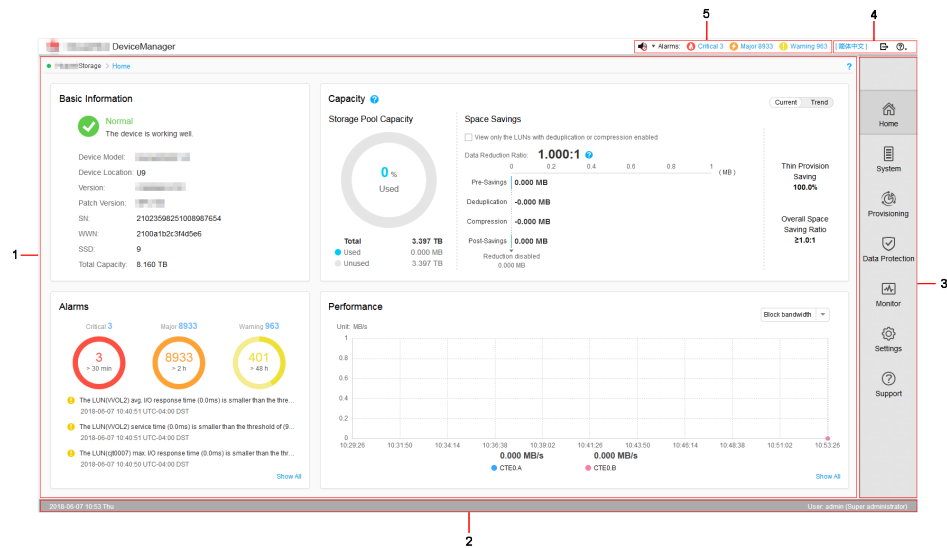


Table 4-2 describes DeviceManager components.


Table 4-2 DeviceManager components

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

----End

## Follow-up Procedure

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

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

The **Confirm** dialog box is displayed.

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

## 4.2.2 Logging In to the DeviceManager Using a Tablet

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

### Prerequisites

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

### Context

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

### Procedure

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

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

The **WLAN** page is displayed.

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

The **Enter Password** page is displayed.

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

4. Click **Join**.

The iPad is connected to the Wi-Fi network.

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

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

The login page of the management software is displayed.

For 2000, 5000 and 6000 series storage systems, **xxx.xxx.xxx.xxx** indicates the IP address of the management network port on the storage system. For 18000 series storage systems, **xxx.xxx.xxx.xxx** indicates the IP address of the SVP management network port.

3. **Optional:** In **Language**, select a language.

 **NOTE**

DeviceManager supports two languages: simplified Chinese and English.

4. Set **User Name** and **Password** to the user name and password for logging in to the management software. Set **Verification Code** to a four-digit verification code.

 **NOTE**

- The default user name and password are **admin** and **Admin@storage** respectively.
- You are advised to change the default login password immediately after you have logged in to the storage system for the first time. In addition, periodically change your login password to reduce password leakage risks. For details about how to change a password, see the *Administrator Guide* of the corresponding product model.

5. Click **Login**.

The home page of the management software is displayed.

----End

## 4.2.3 Logging In to the DeviceManager Through SVP (18000 Series)

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

### Prerequisites

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

### Context

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

## Procedure

### Step 1 Log in to the SVP server.

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

#### NOTE

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

- a. Choose **Start > All Programs > Accessories > Remote Desktop Connection**. The **Remote Desktop Connection** dialog box is displayed.
- b. Type the IP address of the management network port in the **Computer** text box and press **Enter** (the default IP address is **192.168.0.136**).
- c. Type the correct user name and password to log in.

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

#### NOTE

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

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

#### NOTE

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

The DeviceManager login page is displayed.

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

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

#### NOTE

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

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

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



DeviceManager supports two languages: simplified Chinese and English.

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



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

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

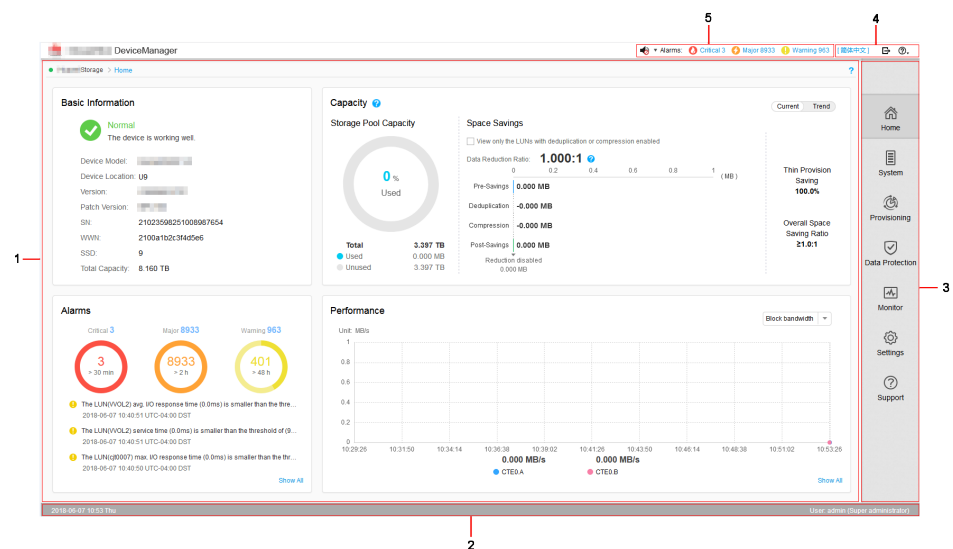


- To log out of the DeviceManager, click in the upper right corner.
- To view online help, click in the upper right corner. The online help provides details about each step and operation.

The DeviceManager main window is displayed.

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

**Figure 4-3** Main window of the DeviceManager



**Table 4-3** describes DeviceManager components.

**Table 4-3** DeviceManager components

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

---End

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

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

### Prerequisites

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

### Context

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



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

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

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

## Procedure

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

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

The DeviceManager login page is displayed.

### NOTE

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

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

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

### NOTE

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

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

### NOTE

DeviceManager supports two languages: simplified Chinese and English.



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

**NOTE**

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

**Step 5 Click Log In.**

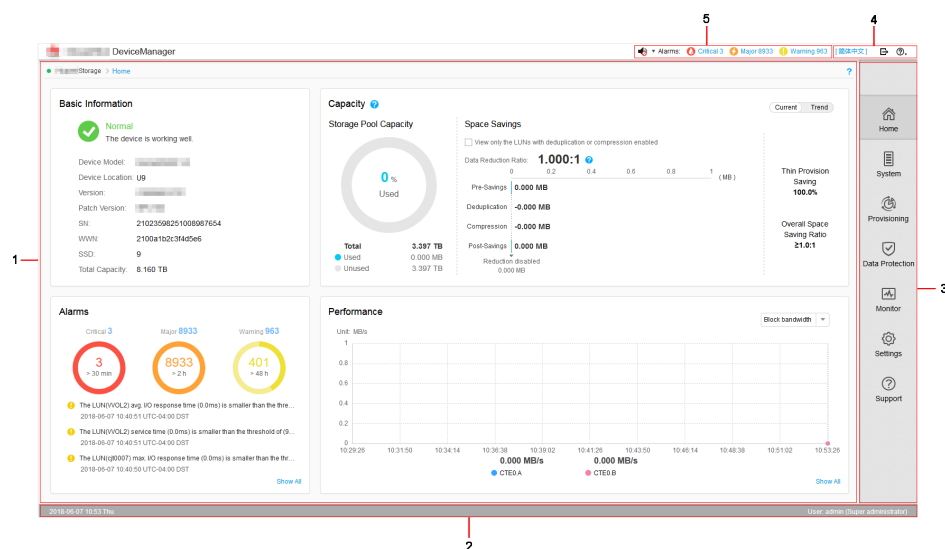
**NOTE**

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

The DeviceManager main window is displayed.

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

**Figure 4-4** Main window of the DeviceManager



**Table 4-4** describes DeviceManager components.

**Table 4-4** DeviceManager components

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

---End

## 4.3 Creating a Disk Domain

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

### Context

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

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

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

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

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

- - High
 

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

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

The system does not provide hot spare space.

**Table 4-5** describes how hot spare space changes with the number of disks. The hot spare space changes at a storage tier are used as an example here. The hot spare space changes at different types of storage tiers are the same.

**Table 4-5** Changes of hot spare space

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

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

 **NOTE**

- For 18000 and 18000F series storage systems, the high hot spare policy is used by default. You can only run the **change disk\_domain general** command on the CLI to modify the hot spare policy.
- When you are creating a disk domain, ensure that the disks used to provide hot spare space are sufficient.
- Hot spare space can be used for the current disk domain only.
- [Table 4-5](#) lists common capacity changes of the hot spare space. The number of disks supported by a storage system and the capacity of their hot spare space are based on actual specifications.

## Procedure

**Step 1** Log in to DeviceManager.

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

**Step 3** Click **Create**.

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

**Step 4** Name and describe the disk domain.

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

 **NOTE**

- The name must be unique.
- The name can contain only letters, digits, periods (.), underscores (\_), and hyphens (-).
- The value contains 1 to 31 characters.

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

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

Encryption types include:

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

 **NOTE**

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

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

- Select **All available disks**.

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

 **NOTE**

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


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

 **NOTE**

For 18000 series storage systems, the high hot spare policy is used by default. You can only run the **change disk\_domain general** command on the CLI to modify the hot spare policy.

- Select **Specify the number of disks** (2000F, 5000F, 6000F, 18000F series storage systems).

The number of disks composing the storage tier will be configured.

- Select **Manually select**.
  - a. Click **Select**.
  - b. In the **Select Disk** dialog box, select the disks you need and click .
  - c. Click **OK** to finish selecting disks.
  - d. Configure the hot spare policy for each storage tier.

 **NOTE**

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

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

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

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

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


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

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

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

**Step 7** Click **OK**.

A message is displayed, indicating that the operation succeeded.

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

----End

## 4.4 Creating a Storage Pool

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

### Context

- You are advised to use different disk domains to create storage pools for the block storage service and file storage service.
- For 2000, 5000, 6000, 18000 series storage systems, a storage pool is a logical combination of one or multiple storage tiers in a disk domain. Different storage tiers may have different RAID policies.
- A RAID policy includes a RAID level and the number of disk blocks and parity blocks and parity blocks of this RAID level.
- The RAID level is classified into typical configuration and flexible configuration based on the number of data blocks and parity blocks. The detailed configuration is shown in [Table 4-6](#).

**Table 4-6** RAID level configuration

RAID Level	Typical Configuration	Flexible Configuration
RAID 0	-	-
RAID 1	<ul style="list-style-type: none"> <li>● 2D<sup>a</sup></li> <li>● 4D</li> </ul>	-
RAID 10	-	-
RAID 3	<ul style="list-style-type: none"> <li>● 2D+1P<sup>b</sup></li> <li>● 4D+1P</li> <li>● 8D+1P</li> </ul>	2D+1P to 13D+1P
RAID 5	<ul style="list-style-type: none"> <li>● 2D+1P</li> <li>● 4D+1P</li> <li>● 8D+1P</li> </ul>	2D+1P to 13D+1P
RAID 50	<ul style="list-style-type: none"> <li>● (2D+1P)x2</li> <li>● (4D+1P)x2</li> <li>● (8D+1P)x2</li> </ul>	-



RAID Level	Typical Configuration	Flexible Configuration
RAID 6	<ul style="list-style-type: none"> <li>● 2D+2P</li> <li>● 4D+2P</li> <li>● 8D+2P</li> <li>● 16D+2P</li> </ul>	2D+2P to 26D+2P
<p>a: <b>D</b> indicates the data block.</p> <p>b: <b>P</b> indicates the parity block.</p> <p><b>NOTE</b></p> <p>For 2000, 5000, 6000, 18000 series storage systems, if the RAID level of one storage tier is configured with flexible configuration first, this tier is the primary control tier that controls other tiers' RAID policies. The number of RAID data disks of the primary control tier and the number of RAID data disks of other tiers must be a multiple of 1, 2, 4, or 8. For example, if the performance tier is the primary control tier and its RAID policy is 3D+1P, the RAID policy of other tiers must be 3D+1P, 6D+2P, or so on, and cannot be 4D+1P. If you want to change the current primary control tier, deselect this tier and select it again.</p>		

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

## Procedure

**Step 1** Log in to DeviceManager.

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

**Step 3** Click **Create**.

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

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

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

 **NOTE**

- The name must be unique.
- The name can contain only letters, digits, periods (.), underscores (\_), and hyphens (-).
- The value contains 1 to 31 characters.

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

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

 **NOTE**

**Usage** is unchangeable after it is configured.

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

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

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

1. Select storage tiers that meet service requirements.
2. Set basic properties for the storage tiers. [Table 4-7](#) describes related parameters.

**Table 4-7** Storage tier parameters

Parameter	Description	Setting
RAID Policy	<p>RAID level. The system supports RAID 0, RAID 1, RAID 10, RAID 3, RAID 5, RAID 50, and RAID 6.</p> <p><b>NOTE</b>                      RAID 0 only supports configuration in CLI mode. For details, see the <i>Command Reference</i> of the corresponding product model.</p>	<p>Select a RAID policy based on the planned solution.</p> <p>The default RAID policy of a storage tier varies with the number of disks allocated to the storage tier.</p> <ul style="list-style-type: none"> <li>- If the number of disks allocated to a storage tier is smaller than 10:                             <ul style="list-style-type: none"> <li>■ Default RAID policy of the high performance tier: RAID 10</li> <li>■ Default RAID policy of the performance tier: RAID 5 (4D+1P)</li> <li>■ Default RAID policy of the capacity tier: RAID 6 (4D+2P)</li> </ul> </li> <li>- If the number of disks allocated to a storage tier is equal to 10:                             <ul style="list-style-type: none"> <li>■ Default RAID policy of the high performance tier: RAID 10</li> <li>■ Default RAID policy of the performance tier: RAID 5 (8D+1P)</li> <li>■ Default RAID policy of the capacity tier: RAID 6 (4D+2P)</li> </ul> </li> <li>- If the number of disks allocated to a storage tier is greater than 10:                             <ul style="list-style-type: none"> <li>■ Default RAID policy of the high performance tier: RAID 10</li> </ul> </li> </ul>

Parameter	Description	Setting
		<ul style="list-style-type: none"> <li>■ Default RAID policy of the performance tier: RAID 5 (8D+1P)</li> <li>■ Default RAID policy of the capacity tier: RAID 6 (8D+2P)</li> </ul> <p><b>NOTE</b>                      If the number of SSDs in a disk domain is two or three, you are advised to configure the corresponding high-performance tier to RAID 1 (2D).</p>
Capacity	The capacity that the storage tier provides for the storage pool. Three capacity levels are provided: TB, GB, and PB. <b>NOTE</b> Select <b>Use all available capacity</b> , and then you can allocate all available capacity in this storage layer to the new storage pool.	The capacity must be not larger than the available capacity of the storage tier.

 **NOTE**

- If the storage pool consists of multiple storage tiers, you are advised to set a SmartTier policy. The policy enables data to migrate among different types of storage tiers, optimizing storage performance distribution.
- You are advised to create RAID 6 groups on the capacity tier to ensure data security.

**Step 8** Configure SmartTier policy for the storage pool being created.

1. Click **Set SmartTier Policy**.

The **Set SmartTier Policy** dialog box is displayed. [Table 4-8](#) lists related parameters.

**Table 4-8** SmartTier policy of the storage pool

Parameter	Description	Setting
Service Monitoring Period	<p>Period of time during which the service is monitored and hotspot statistics is collected after you select <b>Enable I/O monitoring</b>. The statistics serves as guidance for data to migrate among different storage tiers.</p> <p>You can specify the period by setting days, <b>Start Time</b>, and <b>Duration</b>.</p>	<p>[Default value]                      I/O monitoring disabled</p>
Data Migration Plan	<p>The trigger policy of data relocation between the storage layers in a storage pool. The policies include:</p> <ul style="list-style-type: none"> <li>- Manual: You must manually trigger the data relocation among storage tiers. The data relocation process is transparent to application servers. Manual data relocation can be performed anytime.</li> <li>- Periodical: You must specify the start time and duration of data relocation for the storage system to perform data relocation automatically at the specified time. This reduces the management cost and complexity. The data relocation process is transparent to application servers. Automatic data relocation is performed only at the specified time.</li> </ul>	<p>[Default value]                      Manual</p>

 **NOTE**

- SmartTier policy is only applicable when **Usage** of a storage pool is configured as **Block Storage Service**.
- SmartTier is not supported by 2000F, 5000F, 6000F, 18000F series storage systems.
- The dynamic storage tier function can be used when multiple tiers are created. This requires an valid SmartTier license.
- If **Data Migration Plan** is set to **Periodical**, I/Os are monitored on a 7 x 24 basis by default. If **Data Migration Plan** is set to **Manual**, select a path to start migration.
- A storage pool configured with SmartTier needs to reserve free space because SmartTier requires extra data exchange space to dynamically migrate data.

2. Click **OK**. The **Create Storage Pool** dialog box is displayed.

**Step 9** Set advanced properties for the storage pool.

1. Click **Advanced**.

The **Advanced Property Settings** dialog box is displayed. [Table 4-9](#) describes the related parameters.

**Table 4-9** Storage pool advanced parameters

Parameter	Description	Setting
Data Protection Capacity Alarm Threshold (%)	When ratio the data protection capacity of the storage pool to the total capacity of the storage pool exceeds the capacity alarm threshold, the system generates an alarm.	[Value range] 1 to 100 [Default value] 100

Parameter	Description	Setting
Used Capacity Alarm Threshold (%)	<p>If a storage pool contains a LUN or a thin LUN and both LUNs are equipped with value-added services, an alarm will be generated when the percentage of the storage pool's used capacity to its total capacity reaches the alarm threshold of the used capacity. The alarm is generated in 3 circumstances:</p> <ul style="list-style-type: none"> <li>- When the used capacity reaches the used capacity alarm threshold, the system generates an alarm informing that the capacity of storage pool is insufficient.</li> <li>- When the used capacity alarm threshold is no greater than 88 and the used capacity reaches 90%, the system generates an alarm informing that the storage pool is running out.</li> <li>- When the used capacity alarm threshold is no greater than 88 and the used capacity reaches (used capacity alarm threshold +2)%, the system generates an alarm informing that the storage pool is running out.</li> </ul> <p><b>NOTE</b>                      If the used capacity alarm threshold is set as 85, when the used capacity reaches 85%, the system generates an alarm informing that the capacity of storage pool is insufficient, and when the used capacity reaches 90%, the system generates an alarm informing that the storage pool is running out. If the used capacity alarm threshold is set as 91, when the used capacity reaches 93%, the system generates an alarm informing that the storage pool is running out.</p> <p>A proper used capacity alarm threshold helps you monitor the capacity usage of a storage pool.</p>	<p>[Value range]                      1 to 95                      [Default value]                      80</p>

Parameter	Description	Setting
Data Migration Granularity	<p>A logical storage space with a fixed size divided from a CKG. It is the smallest unit (granularity) for data migration and hotspot data statistics collection. It is also the smallest unit for space application and release in a storage pool. The default value <b>4 MB</b> is recommended. The value cannot be changed after being set.</p> <p><b>NOTE</b> You can configure this parameter only when RAID levels of storage tiers are typical configuration.</p>	<p>[Value range] 512 KB to 64 MB</p> <p>[Default value] 4 MB</p>



Parameter	Description	Setting
Strip Depth	<p>Strip refers to that continuous data is divided into data blocks of the same size and data blocks are distributed on different disks of storage devices. In this way, I/O loads are balanced among disks, improving read/write performance.</p> <p>Strip depth refers to strip size, indicating the size of data blocks on each disk. Smaller strip size indicates smaller data blocks. These data blocks are distributed on more disks, improving transmission performance. However, more time is required to find different data blocks, decreasing disk locating performance. On the contrary, fewer data blocks indicate lower transmission performance but higher disk locating performance.</p> <p>The value of this parameter can be:</p> <ul style="list-style-type: none"> <li>- System auto select The system selects the optimal strip depth based on the RAID policy of the storage tier and data migration granularity.</li> <li>- 32 KB</li> <li>- 64 KB</li> <li>- 128 KB 128 KB is recommended for random read/write services (such as in database scenarios).</li> <li>- 256 KB</li> <li>- 512KB 512 KB is recommended for sequential read/write services (such as media asset scenarios)</li> </ul> <p><b>NOTE</b> The parameter value cannot be changed after being determined.</p>	<p>[Default value] System auto select</p>

2. Click **OK**.

**Step 10** In the **Create Storage Pool** dialog box, Click **OK**.

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

**Step 11** Click **Close**.

----End

## 4.5 Creating a PE LUN

When using VVol, you must set LUNs to the PE type.

### Prerequisites

- At least one storage pool has been created. If the storage system has no storage pool, create one first.
- Only administrators and super administrators are allowed to create PE LUNs.

### Context

- A PE LUN does not provide storage space. Therefore, it cannot be allocated any capacity.
- In the advanced properties of a PE LUN, you can only configure its owning controller.

### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **LUN**.

**Step 3** Click **Create**.

The **Create LUN** dialog box is displayed.

**Step 4** Set basic properties for the PE LUN.  
[Table 4-10](#) describes related parameters.

**Table 4-10** LUN parameters

Parameter	Description	Setting
Name	Name of a newly created LUN.	<p>[Value range]</p> <ul style="list-style-type: none"> <li>● The name must be unique.</li> <li>● The name can contain only letters, digits, periods (.), underscores (_), and hyphens (-).</li> <li>● The value contains 1 to 31 characters.</li> </ul> <p>[Example] <b>LUN001</b></p>
Description	Description of a LUN.	<p>[Example] -</p>

Parameter	Description	Setting
Start ID	<p>The ID of a LUN.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>● The system automatically allocates an ID to a newly created LUN by default.</li> <li>● If you want to manually set a LUN ID, do not select <b>Automatic allocate</b>. Instead, enter an ID manually.</li> <li>● When creating a single LUN, the value you enter is the ID of the LUN.</li> <li>● When creating LUNs in a batch, the system automatically allocates an ID starting from the value you have entered to each LUN.</li> </ul>	<p>[Example]</p> <p><b>2</b></p>
Use Type	<p>Use type of a LUN.</p> <ul style="list-style-type: none"> <li>● <b>Common LUN</b> A logical disk accessible to the host, including thin LUN and thick LUN.</li> <li>● <b>PE LUN</b> PE LUNs are only applied for VVol LUNs in VMware software defined storage. VVol provides storage space for VMs. A PE LUN is used as an I/O demultiplexer to simplify the connection between a VM and a VVol LUN. VM I/Os are sent to the corresponding VVol LUN through a PE LUN.</li> </ul>	<p>[Example]</p> <p><b>PE LUN</b></p>
Quantity	<p>Number of LUNs created in a batch. Set this parameter based on your need.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>● LUNs created in a batch have the same capacity.</li> <li>● The total capacity of LUNs created in a batch must be less than or equal to the available capacity of the storage pool.</li> <li>● The number of PE LUNs must be equal to or greater than that of controllers.</li> </ul>	<p>[Value range]</p> <p>1 to 500</p> <p>[Example]</p> <p><b>2</b></p>

Parameter	Description	Setting
Manually specify the suffix	When creating multiple LUNs, the system automatically appends a suffix number to each LUN name for LUN distinction. You can manually set the start suffix number after selecting this option. <b>NOTE</b> If this option is not selected, the suffix number starts at 0000 by default.	[Example] -
Owning Storage Pool	Storage pool to which the LUN you are creating belongs. <b>NOTE</b> If the storage system has no storage pool, click <b>Create</b> to create one.	[Example] <b>storagepool001</b>

 **NOTE**

**Start ID** and **Use Type** are hidden options. If you want to display these options, click **All options**.

**Step 5 Optional:** Set advanced properties for the PE LUN.

1. Click **Advanced**. The **Advanced** dialog box is displayed.
2. Select the owning controller of the PE LUN. **Table 4-11** describes the related parameter.

**Table 4-11** Advanced properties of a PE LUN

Parameter	Description	Setting
Owning Controller	Owning controller of a LUN. You are advised to allocate LUNs to different controllers for load balancing.	If you are not sure about the owning controller, select <b>Auto select</b> . The storage system will automatically select the owning controller for the LUN. [Example] <b>Auto select</b>

3. Click **OK**. The **Create LUN** dialog box is displayed.

**Step 6** Confirm the creation of the PE LUN.

1. Click **OK**.  
The **Execution Result** dialog box is displayed, indicating that the operation succeeded.
2. Click **Close**.

----End

## 4.6 Creating a LUN Group

To allow hosts to use PE LUNs, you must add the PE LUNs into LUN groups. Then, establish mapping views between the LUN groups and host groups. In doing so, the hosts in the host groups can use the PE LUNs in the LUN groups. A LUN group can contain one to multiple PE LUNs.

### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **LUN** > **LUN Group**.

**Step 3** Click **Create**.

The **Create LUN Group** dialog box is displayed.

**Step 4** Set basic properties for the LUN group. [Table 4-12](#) describes related parameters.

**Table 4-12** LUN group parameters

Parameter	Description	Setting
Name	Name of a newly created LUN group.	[Value range] <ul style="list-style-type: none"> <li>The name must be unique.</li> <li>The name can contain only letters, digits, periods (.), underscores (_), and hyphens (-).</li> <li>The name contains 1 to 31 characters.</li> </ul> [Example] LUNgroup001
Description	Description of a LUN group.	[Example] -

**Step 5** Select the PE LUNs you want to add to the LUN group.

- In the **Available LUNs** area, select one or multiple PE LUNs based on your service need.

 **NOTE**

By default, the **Show only the LUNs that do not belong to any LUN group** checkbox in the bottom left corner of the dialog box is selected to facilitate LUN locating.

- Click  to add the PE LUNs to the **Selected LUNs** area.

**Step 6** Confirm the creation of the LUN group.

- Click **OK**.

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

2. Click **Close**.

----End

## 4.7 Configuring Connectivity between Host and Storage System

This section describes how to configure the connectivity between host and storage system through iSCSI networking or FC networking.

### 4.7.1 iSCSI Networking

This section describes how to configure the connectivity between host and storage system through iSCSI networking.

#### 4.7.1.1 Configuring Ethernet Switches

Configuring VLANs for Ethernet switches can avoid conflicts and improve flexibility of the service systems.

#### Context

On an Ethernet network to which many hosts are connected, a large number of broadcast packets are generated during the host communication. Broadcast packets sent from one host will be received by all other hosts on the network, consuming more bandwidth. Moreover, all hosts on the network can access each other, resulting in data security risks. To save bandwidth and prevent security risks, hosts on an Ethernet network are divided into multiple logical groups. Each logical group is a VLAN.

The following uses HUAWEI Quidway 2700 Ethernet switch as an example to explain how to configure VLANs. In the following example, two VLANs (VLAN 1000 and VLAN 2000) are created. VLAN 1000 contains ports GE 1/0/1 to 1/0/16. VLAN 2000 contains ports GE 1/0/20 to 1/0/24.

#### Procedure

- Step 1** Go to the system view.

```
<Quidway> system-view  
System View: return to User View with Ctrl+Z.
```

- Step 2** Create VLAN 1000 and add ports to it.

```
[Quidway]VLAN 1000  
[Quidway-vlan1000]port GigabitEthernet 1/0/1 to GigabitEthernet 1/0/16
```

- Step 3** Configure the IP address of VLAN 1000.

```
[Quidway-vlan1000]interface VLAN 1000  
[Quidway-Vlan-interface1000]ip address 192.168.1.0 255.255.0.0
```

- Step 4** Create VLAN 2000, add ports, and configure the IP address.

```
[Quidway]VLAN 2000  
[Quidway-vlan2000]port GigabitEthernet 1/0/20 to GigabitEthernet 1/0/24
```

```
[Quidway-vlan2000]interface VLAN 2000  
[Quidway-Vlan-interface2000]ip address 192.168.2.0 255.255.0.0
```

**Step 5** Run the **commit** command to submit the configuration file.

**Step 6** Run the **quit** command to exit the system view.

**Step 7** Run the **save** command to save the configuration file.

----End

### 4.7.1.2 Configuring an IP Address for the Service Network Port on the Application Server


When the application server connects to a storage system through iSCSI, you must configure the IP address of the service network port on the application server and the IP address of the iSCSI host port on the storage system on the same network segment. You can add a virtual network to the VMware host system to configure the service IP address. This section describes how to configure the IP address for a VMware service network port.

#### Procedure

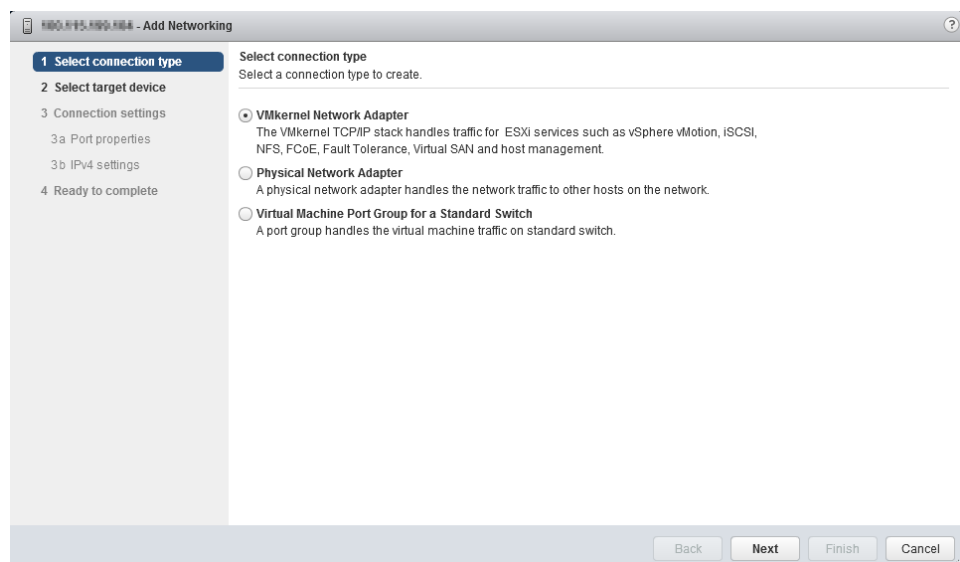
**Step 1** Log in to vSphere Web Client (vCenter 6.0 as an example).

**Step 2** Select the host that you want to manage.

**Step 3** Create a virtual switch.

1. Choose **Manage > Networking > Virtual switches** and click .  
The **Add Networking** dialog box is displayed, as shown in [Figure 4-5](#).

**Figure 4-5** Add Networking dialog box

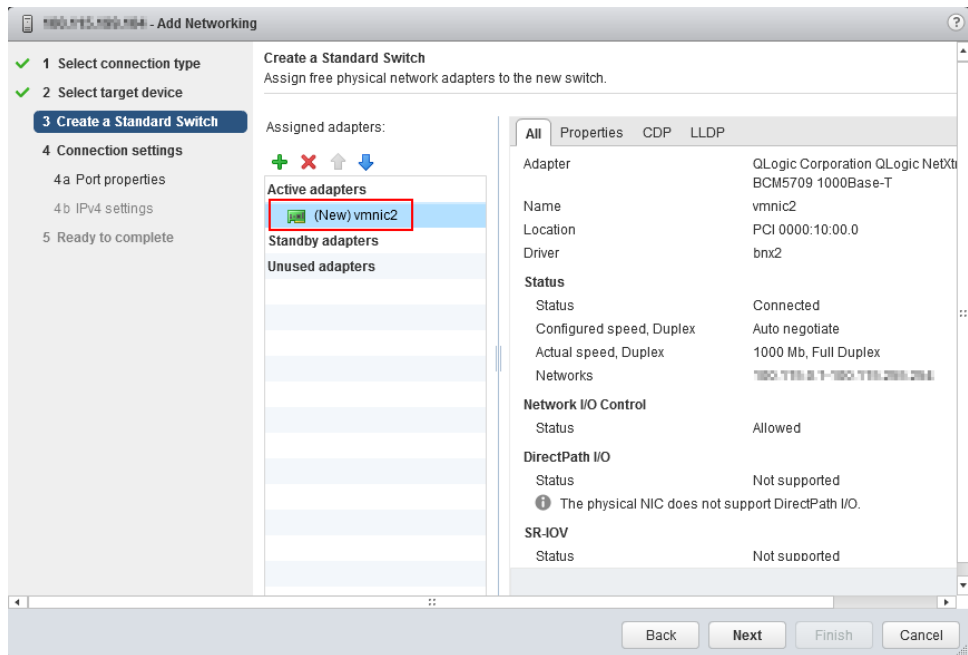


2. In **1 Select connection type**, select **VMkernel Network Adapter** and click **Next**.
3. In **2 Select target device**, select **New standard switch** and click **Next**.



4. In **3 Create a Standard Switch**, click **+**. Select a standard switch that you want to connect to the storage system
5. Click **OK**. The **3 Create a Standard Switch** page is displayed. In the list, you can see the network adapter selected in [Step 3.4](#), as shown in [Figure 4-6](#). Click **Next**.

**Figure 4-6 Create a Standard Switch page**



6. In **4a Port properties**, configure the network label based on actual requirements. Keep the default settings for other parameters and click **Next**.
7. In **4b IPv4 setting**, select **Use static IPv4 setting**. In **IPv4 address** and **Subnet mask**, enter the IP address of the service network port and subnet mask of the ESXi host and the storage system. Click **Next**.

You must configure the service network port IP address and the iSCSI host port IP address on the same network segment. In this way, the storage system can properly communicate with the application server.

8. Click **Next** to confirm the configuration.
9. Click **Finish**. The virtual switch is created.

**NOTE**

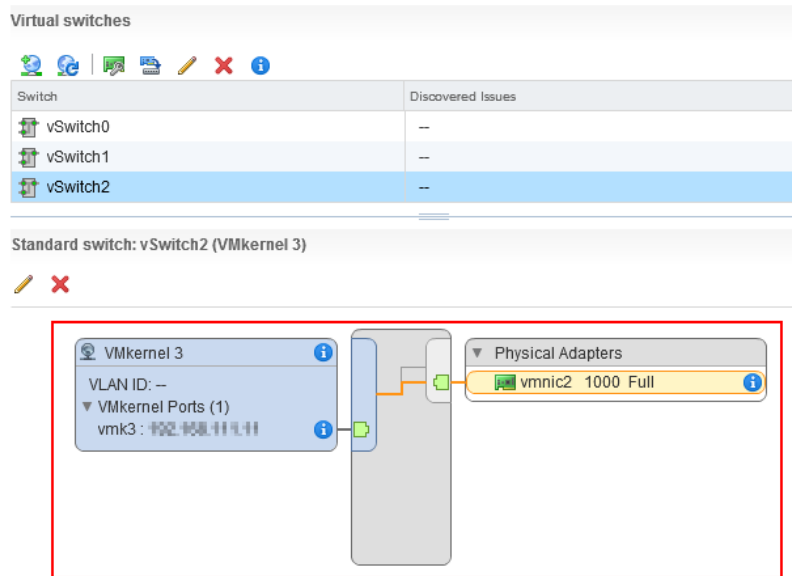
- After completing the configuration, you can run **ifconfig** to check whether the IP address of the application server is correct.
- If you want to create multiple virtual networks, repeat the preceding operations.

---End

## Follow-up Procedure

Choose **Manage > Networking > Virtual switches**. In the **Standard switch** area, check the virtual network that has been configured, as shown in [Figure 4-7](#).

**Figure 4-7** Checking the virtual network configuration



### 4.7.1.3 Configuring an Initiator

This section describes how to configure an initiator on an application server running VMware.

#### Prerequisites

The service network port on the application server is communicating properly with the iSCSI host port on the storage system. On the application server, run the **ping ip** command, where *ip* indicates the IP address of the iSCSI host port connected to the application server. If the application server receives the data packets sent from the iSCSI host port, the communication between the application server and storage system is normal. If the application server fails to receive the data packets, use either of the following methods to ensure normal communication.

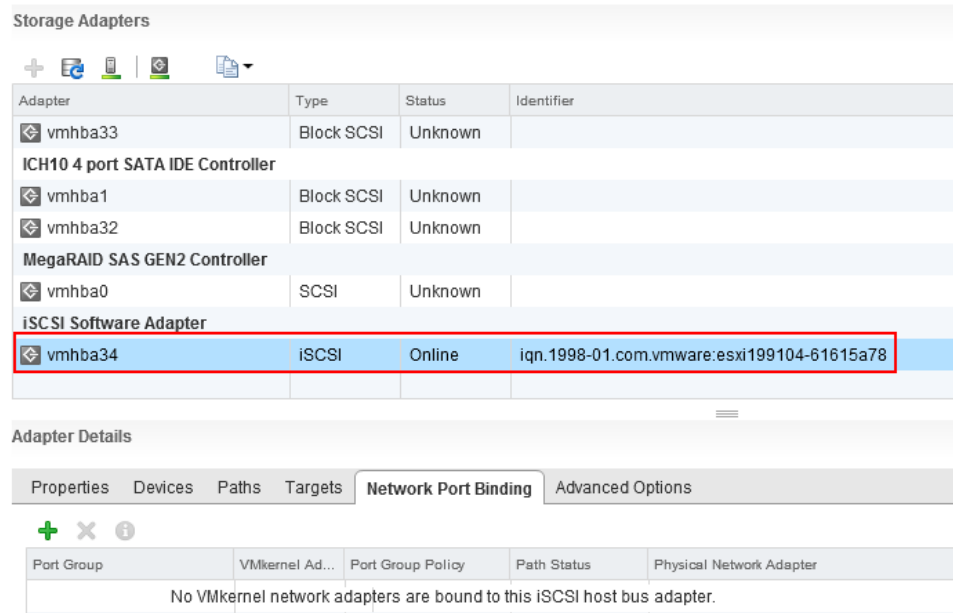
- Configure the IP addresses of the iSCSI host port and service network port onto the same network segment.
- If the two IP addresses are on different network segments, add a route to establish a connection between them.

#### Procedure

- Step 1** Log in to vSphere Web Client (vCenter 6.0 as an example).
- Step 2** Select the host that you want to manage.
- Step 3** Add a iSCSI adapter.
  1. Choose **Manage > Networking > Storage Adapters** and click **+**. The **Add Software iSCSI Adapter** dialog box is displayed.
  2. Click OK.

After the adapter is added, you can see the name of the initiator corresponding to the newly added iSCSI adapter on the **Storage Adapters** page, as shown in **Figure 4-8**.

**Figure 4-8 Storage Adapters page**

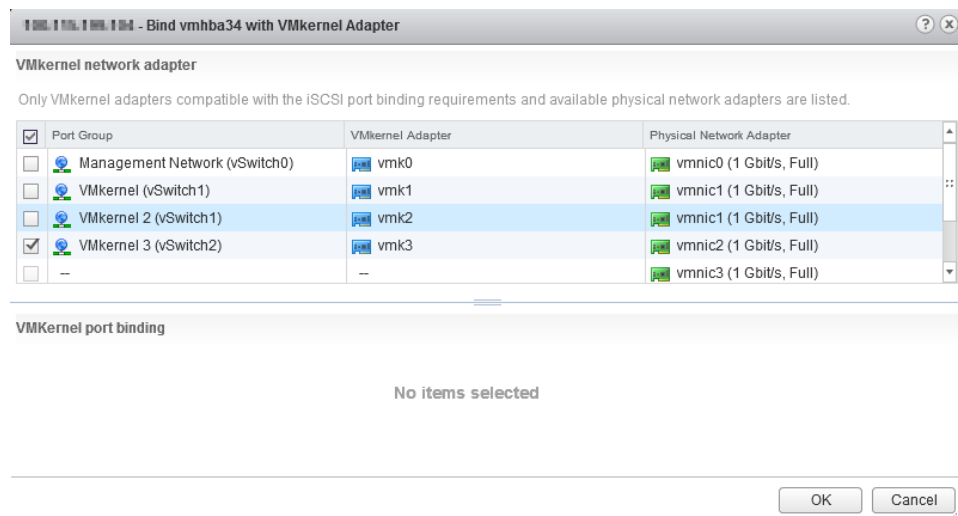


**Step 4** Bind with a VMkernel network adapter.

1. Select the iSCSI adapter newly added.
2. On **Adapter Details**, click **Networking Port Binding**.
3. Click **+**.

The **Bind with VMkernel Network Adapter** dialog box is displayed, as shown in **Figure 4-9**.

**Figure 4-9 Bind with VMkernel Network Adapter dialog box**



4. Select the VMkernel adapter to be bound with the iSCSI initiator.
5. Click **OK**.

The **Adapter Details** page is displayed. In **Networking Port Binding**, you can find the bound network port, as shown in **Figure 4-10**.

**Figure 4-10 Adapter Details page**

The screenshot shows the 'Storage Adapters' section with a table listing various adapters. Below it is the 'Adapter Details' section with tabs for Properties, Devices, Paths, Targets, Network Port Binding, and Advanced Options. The 'Network Port Binding' tab is active, showing a table with columns: Port Group, VMkernel Ad..., Port Group Policy, Path Status, and Physical Network Adapter. A red box highlights the row for 'VMkernel 3 (vSwitch2)' which is bound to 'vmk3' with a 'Compliant' policy and 'Not used' status, connected to 'vmnic2 (1 Gbit/s, Full)'.

Adapter	Type	Status	Identifier
vmhba33	Block SCSI	Unknown	
<b>ICH10 4 port SATA IDE Controller</b>			
vmhba1	Block SCSI	Unknown	
vmhba32	Block SCSI	Unknown	
<b>MegaRAID SAS GEN2 Controller</b>			
vmhba0	SCSI	Unknown	
<b>iSCSI Software Adapter</b>			
vmhba34	iSCSI	Online	iqn.1998-01.com.vmware:esxi199104-61615a78

Port Group	VMkernel Ad...	Port Group Policy	Path Status	Physical Network Adapter
VMkernel 3 (vSwitch2)	vmk3	Compliant	Not used	vmnic2 (1 Gbit/s, Full)

**NOTE**

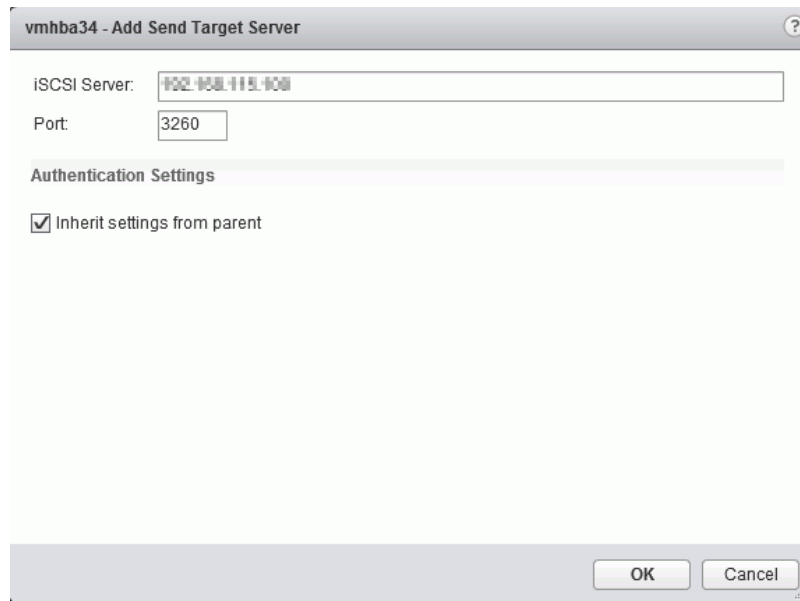
If only one path has been configured between the storage system and the application server, bind the iSCSI initiator with the only VMkernel adapter. If multiple paths have been configured, repeat the preceding steps to bind the iSCSI initiator with all the VMkernel adapters.

**Step 5** Configure the iSCSI target IP address.

1. Choose **Manage > Storage > Storage Adapter**.
2. Select the iSCSI adapter to be configured.
3. On the **Adapter Details** page, click **Targets**.
4. Choose **Dynamic Discovery**, click **Add**.

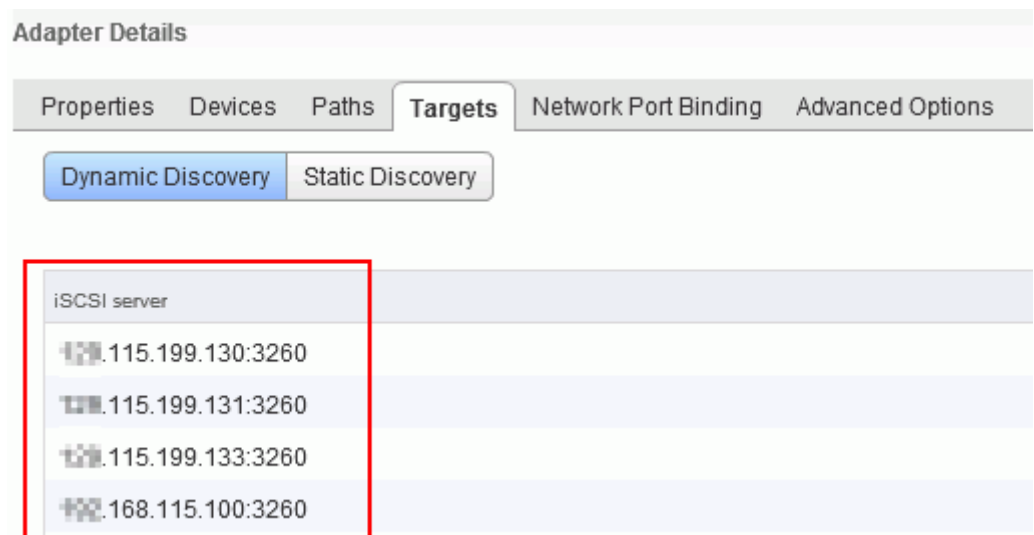
The **Add Send Target Server** dialog box is displayed, as shown in **Figure 4-11**.

**Figure 4-11 Add Send Target Server** dialog box



5. In the **iSCSI Server** text box, enter the IP address of the iSCSI target, which is the iSCSI port connecting the storage system to the application server.
  6. In the **Port** text box, enter **3260**.
- Inherit settings from parent** is selected by default.
7. Click **OK** to add the iSCSI target to the target list, as shown in [Figure 4-12](#).

**Figure 4-12** iSCSI target list



 **NOTE**

- The iSCSI target is added to the target list. You are advised to re-scan for the iSCSI adapter as prompted by the system.
- If the storage system connects to the application server through multiple paths, repeat the preceding steps to add all iSCSI port IP addresses to the target list.

----End

### 4.7.1.4 (Optional) Configuring CHAP Authentication

After CHAP authentication is enabled on the storage system, configure the CHAP user name and password on the VMware ESX-based application server to set up a connection to the storage system.

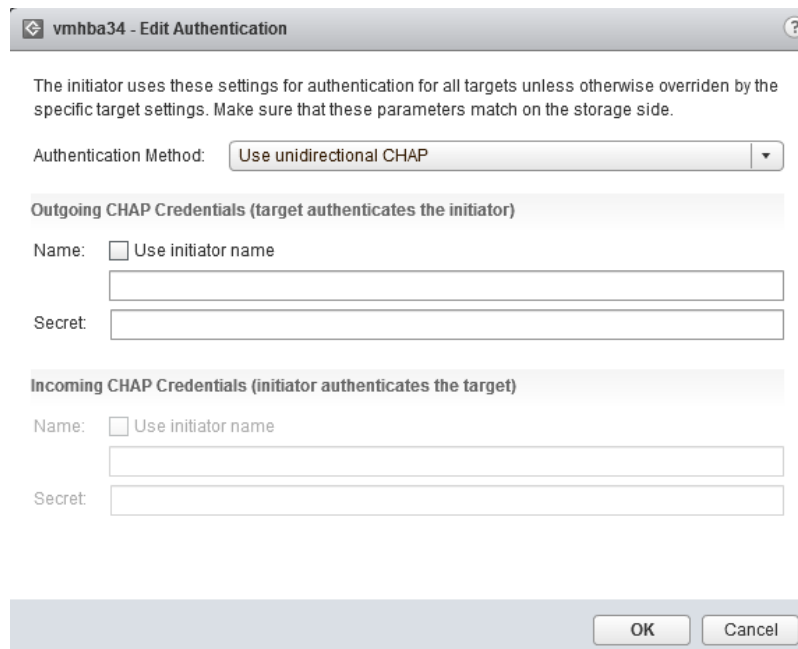
#### Procedure

**Step 1** Go to the CHAP authentication dialog box.

1. In vSphere Web Client (vCenter 6.0 as an example), choose **Manage > Storage > Storage Adapter**.
2. Select the iSCSI adapter to be configured.
3. On the **Adapter Details** page, click **Properties**.
4. On the **Authentication** page, click **Edit**.

The **Edit Authentication** dialog box is displayed, as shown in [Figure 4-13](#).

**Figure 4-13 Edit Authentication** dialog box



vmhba34 - Edit Authentication

The initiator uses these settings for authentication for all targets unless otherwise overridden by the specific target settings. Make sure that these parameters match on the storage side.

Authentication Method: Use unidirectional CHAP

**Outgoing CHAP Credentials (target authenticates the initiator)**

Name:  Use initiator name

Secret:

**Incoming CHAP Credentials (initiator authenticates the target)**

Name:  Use initiator name

Secret:

OK Cancel

**Step 2** Configure CHAP parameters.

---



## NOTICE

After you have successfully established an iSCSI connection between the application server and storage system, the storage system becomes inaccessible if CHAP authentication is disabled. In this case, you need to configure an initiator again.

---

1. Select **Use unidirectional CHAP** in **Authentication Method**.
2. In the **Name** and **Secret** text boxes, enter the CHAP user name and password that are created on the storage system and added for the initiator.

**Step 3** Click **OK**.

----End

### 4.7.1.5 Setting Ethernet Port Information

Configure Ethernet port parameters to ensure proper communication between the storage system and application server.



### Precautions

Note the following items when setting the properties of an Ethernet port:

- The default IP addresses of the internal heartbeat on the dual-controller storage system are **127.127.127.10** and **127.127.127.11**, and the default IP addresses of the internal heartbeat on the four-controller storage system are **127.127.127.10**, **127.127.127.11**, **127.127.127.12**, and **127.127.127.13**. Therefore, the IP address of a port cannot fall within the 127.127.127.XXX segment. Besides, the IP address of the gateway cannot be **127.127.127.10**, **127.127.127.11**, **127.127.127.12**, or **127.127.127.13**. Otherwise, routing will fail. (Internal heartbeat links are established between controllers for these controllers to detect each other's working status. You do not need to separately connect cables. In addition, internal heartbeat IP addresses have been assigned before delivery, and you cannot change these IP addresses).
- For 2000, 2000F, 5000, 5000F, 6000, 6000F series storage systems, the IP address of the Ethernet port cannot be in the same network segment as the management network port. For 18000, 18000F series storage systems, the IP address of the Ethernet port cannot be in the same network segment as the service processor (SVP) and engine management network ports.
- The IP address of the Ethernet port cannot be in the same network segment as that of a maintenance network port.
- If the Ethernet port connects to an application server, the IP address of the Ethernet port must be in the same network segment as that of the service network port on the application server. If the Ethernet port connects to another storage device, the IP address of the Ethernet port must be in the same network segment as that of the Ethernet port on the other storage device. If the network segment has insufficient available IP addresses, see [4.7.1.6 \(Optional\) Adding Routes](#).

### Procedure

**Step 1** Go to the **Ethernet Port** dialog box.

1. On the right navigation bar, click  **System**.
2. Click the controller enclosure where the Ethernet port resides.
3. Click  to switch to the rear view.
4. Click the Ethernet port whose information you want to view.  
The **Ethernet Port** dialog box is displayed.
5. Click **Modify**.

### Ethernet Port

Location:	CTE0.B.P0
Health Status:	Normal
Running Status:	Link up
Working Rate (Gbit/s):	1
Max. Working Rate (Gbit/s):	2

---

IPv4 Address:	<input type="text"/>
Subnet Mask:	<input type="text"/>

---

IPv6 Address:	<input type="text"/>
Prefix:	<input type="text"/>

---

MAC Address:	0022a105a50c
Port Switch:	Enable
MTU (Byte):	<input type="text" value="1500"/>
Bond Name:	--
iSCSI Target Name:	--

<<

**Step 2** Set the Ethernet port.

1. In the **IPv4 Address** or **IPv6 Address** text box, enter an IP address for the Ethernet port.
2. In the **Subnet Mask** or **Prefix** area, enter the subnet mask or prefix of the Ethernet port.
3. In **MTU (Byte)**, type a maximum transfer unit (MTU) for the packets transferred between the Ethernet port and the application server.  
The MTU must be an integer ranging from 1500 to 9000.

**Step 3** Confirm the Ethernet port configuration.

1. Click **Apply**.  
The **Danger** dialog box is displayed.
2. Confirm the information in the dialog box and select **I have read and understood the consequences associated with performing this operation**.



3. Click **OK**.  
The **Success** message box is displayed, indicating that the operation succeeded.
4. Click **OK**.

----End

### 4.7.1.6 (Optional) Adding Routes

If iSCSI networking is adopted and data needs to be transmitted across network segments, you need to configure routes.

#### Prerequisites

The Ethernet port has been assigned an IP address.

#### Procedure

**Step 1** Log in to DeviceManager.

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

**Step 3** Select the Ethernet port for which you want to add a route and click **Route Management**.  
The **Route Management** dialog box is displayed.

**Step 4** Configure the route information for the Ethernet port.

1. In **IP Address**, select the IP address of the Ethernet port.
2. Click **Add**.  
The **Add Route** dialog box is displayed.

---

#### NOTICE

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

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

There are three route options:

- Default route  
Data is forwarded through this route by default if no preferred route is available.  
The destination address field and the target mask field (IPv4) or prefix (IPv6) of the

default route are automatically set to 0. To use this option, you only need to add a gateway.

- Host route

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

- Network segment route

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

4. Set **Destination Address**.

- If **IP Address** is an IPv4 address, set **Destination Address** to the IPv4 address or network segment of the application server's service network port or that of the other storage system's Ethernet port.
- If **IP Address** is an IPv6 address, set **Destination Address** to the IPv6 address or network segment of the application server's service network port or that of the other storage system's Ethernet port.

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

- If **Destination Mask** is set for an IPv4 address, this parameter specifies the subnet mask of the IP address for the service network port on the application server or the other storage device.
- If **Prefix** is set for an IPv6 address, this parameter specifies the prefix of the IPv6 address for the application server's service network port or that of the other storage system's Ethernet port.

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

**Step 5** Click **OK**. The route information is added to the route list.

A security alert dialog box is displayed.

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

**Step 7** Click **OK**.

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

 **NOTE**

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

**Step 8** Click **Close**.

---End

## 4.7.2 Fibre Channel Networking

This section describes how to configure the connectivity between host and storage system through FC networking.

### 4.7.2.1 Configuring Fibre Channel Switches

Configuring zones for Fibre Channel switches can avoid conflicts and improve flexibility of service systems.

### 4.7.2.1.1 Querying the Switch Model and Version

Before using Fibre Channel switches, you need to query the switch model and version.

#### Context

The commonly used Fibre Channel switches are mainly from Brocade, Cisco, and QLogic. The following uses a Brocade switch as an example to explain how to configure switches.

#### Procedure

**Step 1** Log in to the Brocade switch from a web browser.

On a web browser, enter the IP address of the Brocade switch. The Web Tools switch login dialog box is displayed. Enter the account and password. The default account and password are **admin** and **password**. The switch management page is displayed.



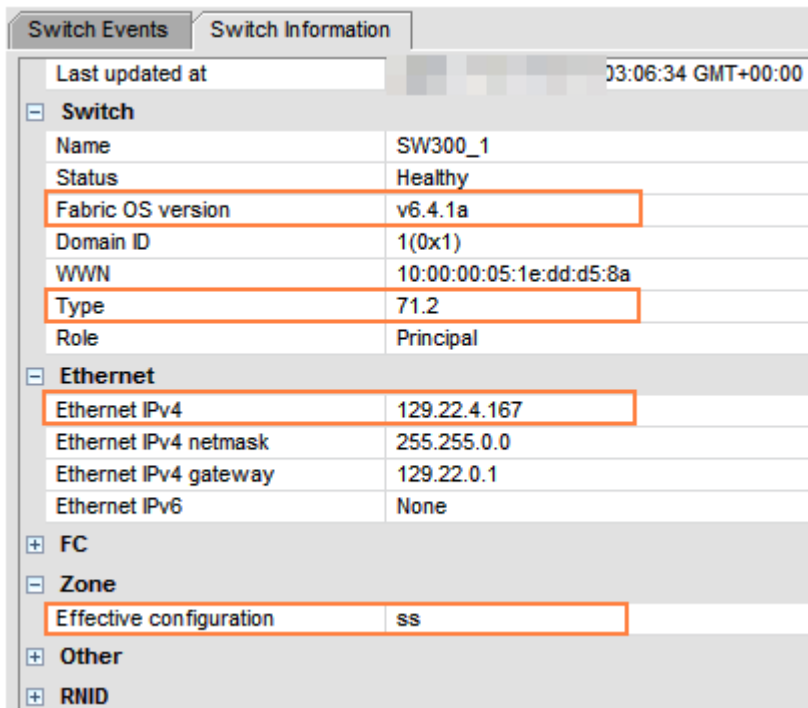
Web Tools works correctly only when Java is installed on the host. Java 1.6 or later is recommended.

---

**Step 2** View the switch information.

On the switch management page that is displayed, click **Switch Information**. The switch information is displayed, as shown in [Figure 4-14](#).

**Figure 4-14** Switch information



Switch Information	
Last updated at	03:06:34 GMT+00:00
<b>Switch</b>	
Name	SW300_1
Status	Healthy
Fabric OS version	v6.4.1a
Domain ID	1(0x1)
WWN	10:00:00:05:1e:dd:d5:8a
Type	71.2
Role	Principal
<b>Ethernet</b>	
Ethernet IPv4	129.22.4.167
Ethernet IPv4 netmask	255.255.0.0
Ethernet IPv4 gateway	129.22.0.1
Ethernet IPv6	None
<b>FC</b>	
<b>Zone</b>	
Effective configuration	ss
<b>Other</b>	
<b>RNID</b>	

You can obtain the following information from **Figure 4-14**:

- **Fabric OS version**: indicates the switch version information.

 **NOTE**

The interoperability between switches and storage systems varies with the switch version. Only switches of authenticated versions can interconnect correctly with storage systems. For details about the interoperability between switches and storage systems, use **OceanStor Interoperability Navigator**.

- **Type**: This parameter is a decimal consisting of an integer and a decimal fraction. The integer indicates the switch model and the decimal fraction indicates the switch template version. You only need to pay attention to the switch model. **Table 4-13** describes switch model mapping.

**Table 4-13** Mapping between switch types and names

Switch Type	Switch Name	Switch Type	Switch Name
1	Brocade 1000 Switch	58	Brocade 5000 Switch
2,6	Brocade 2800 Switch	61	Brocade 4424 Embedded Switch
3	Brocade 2100,2400 Switches	62	Brocade DCX Backbone
4	Brocade 20x0,2010,2040,2050 Switches	64	Brocade 5300 Switch
5	Brocade 22x0,2210,2240,2250 Switches	66	Brocade 5100 Switch
7	Brocade 2000 Switch	67	Brocade Encryption Switch
9	Brocade 3800 Switch	69	Brocade 5410 Blade
10	Brocade 12000 Director	70	Brocade 5410 Embedded Switch
12	Brocade 3900 Switch	71	Brocade 300 Switch
16	Brocade 3200 Switch	72	Brocade 5480 Embedded Switch
17	Brocade 3800VL	73	Brocade 5470 Embedded Switch
18	Brocade 3000 Switch	75	Brocade M5424 Embedded Switch
21	Brocade 24000 Director	76	Brocade 8000 Switch

Switch Type	Switch Name	Switch Type	Switch Name
22	Brocade 3016 Switch	77	Brocade DCX-4S Backbone
26	Brocade 3850 Switch	83	Brocade 7800 Extension Switch
27	Brocade 3250 Switch	86	Brocade 5450 Embedded Switch
29	Brocade 4012 Embedded Switch	87	Brocade 5460 Embedded Switch
32	Brocade 4100 Switch	90	Brocade 8470 Embedded Switch
33	Brocade 3014 Switch	92	Brocade VA-40FC Switch
34	Brocade 200E Switch	95	Brocade VDX 6720-24 Data Center Switch
37	Brocade 4020 Embedded Switch	96	Brocade VDX 6730-32 Data Center Switch
38	Brocade 7420 SAN Router	97	Brocade VDX 6720-60 Data Center Switch
40	Fibre Channel Routing (FCR) Front Domain	98	Brocade VDX 6730-76 Data Center Switch
41	Fibre Channel Routing, (FCR) Xlate Domain	108	Dell M8428-k FCoE Embedded Switch
42	Brocade 48000 Director	109	Brocade 6510 Switch
43	Brocade 4024 Embedded Switch	116	Brocade VDX 6710 Data Center Switch
44	Brocade 4900 Switch	117	Brocade 6547 Embedded Switch
45	Brocade 4016 Embedded Switch	118	Brocade 6505 Switch
46	Brocade 7500 Switch	120	Brocade DCX 8510-8 Backbone

Switch Type	Switch Name	Switch Type	Switch Name
51	Brocade 4018 Embedded Switch	121	Brocade DCX 8510-4 Backbone
55.2	Brocade 7600 Switch	-	-

- **Ethernet IPv4:** indicates the switch IP address.
- **Effective configuration:** indicates the currently effective configurations. This parameter is important and is related to zone configurations. In this example, the currently effective configuration is **ss**.

---End

### 4.7.2.1.2 Configuring Zones

Zone configuration is important for Fibre Channel switches. This section describes how to configure switch zones.

#### Context

The zone function of a Fibre Channel switch is similar to the VLAN function of an Ethernet switch. It allocates devices on a SAN network (such as hosts and storage devices) into different zones, and devices in different zones cannot communicate with each other. In this way, network devices are isolated and will not interfere with each other. When you are configuring zone information, small zones are preferred, namely, adding two ports carrying services to one zone.



#### NOTICE

If the host port and the storage port cannot reside in the same zone, you are advised to configure the zone in a way that high-throughput services (such as backup services) and real-time services are isolated during network configuration to avoid impacts on real-time services caused by bandwidth preemption.

#### Procedure

**Step 1** Log in to the Brocade switch from a web browser. This step is the same as that in section [4.7.2.1.1 Querying the Switch Model and Version](#).

**Step 2** Check the switch port status.

Normally, the switch port indicators are steady green, as shown in [Figure 4-15](#).

**Figure 4-15** Switch port indicator status



If ports connecting the host or storage system are not identified by the switch, check the connectivity between the host or storage system and the switch ports.

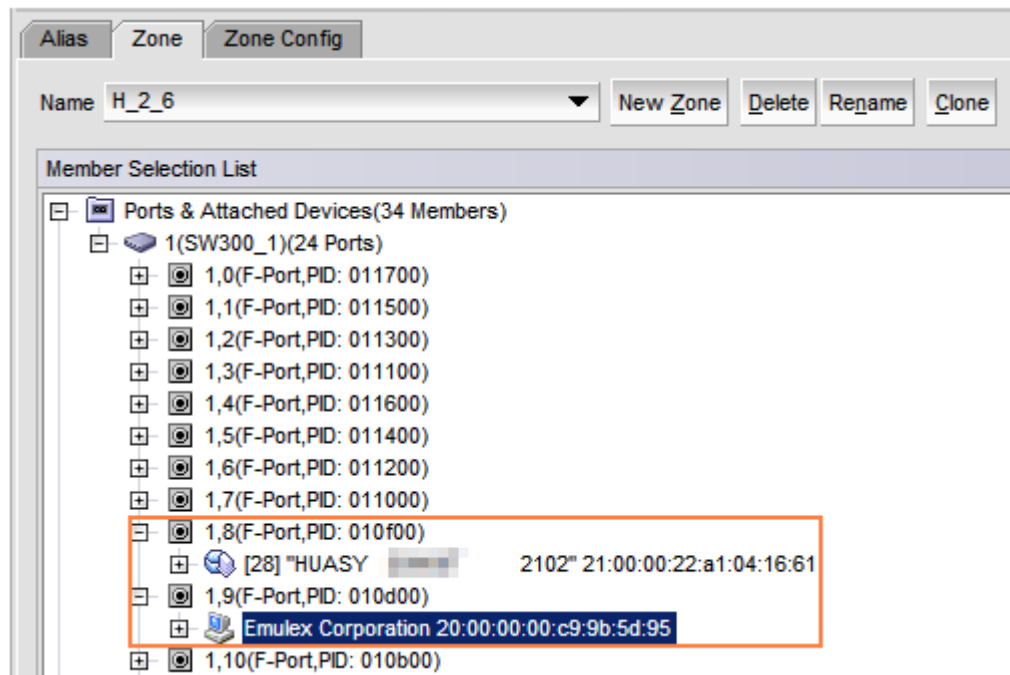
**Step 3** Go to the **Zone Admin** page.

In the navigation tree of **Web Tools**, choose **Task > Manage > Zone Admin**. You can also choose **Manage > Zone Admin** in the navigation bar.

**Step 4** Check whether the switch identifies hosts and storage systems.

On the **Zone Admin** page, click the **Zone** tab. In **Ports&Attached Devices**, check whether all related ports are identified, as shown in **Figure 4-16**.

**Figure 4-16** Zone tab page

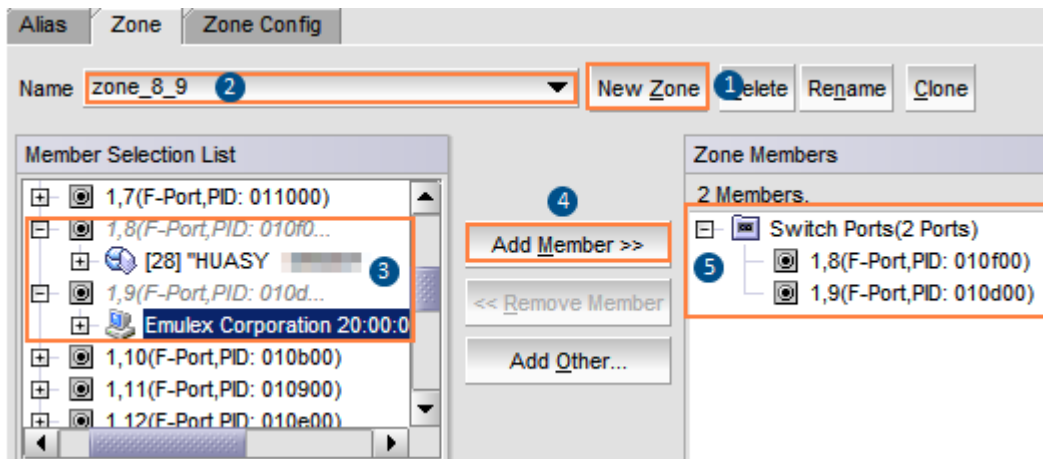


**Figure 4-16** shows that ports 1,8 and 1,9 in use are correctly identified by the switch. If ports connecting the host or storage system are not identified by the switch, check the connectivity between the host or storage system and the switch ports.

**Step 5** Create a zone.

On the **Zone** tab page, click **New Zone** to create a zone and name it **zone\_8\_9**. Select ports 1,8 and 1,9 and click **Add Member** to add them to the new zone, as shown in **Figure 4-17**.

Figure 4-17 Zone configuration

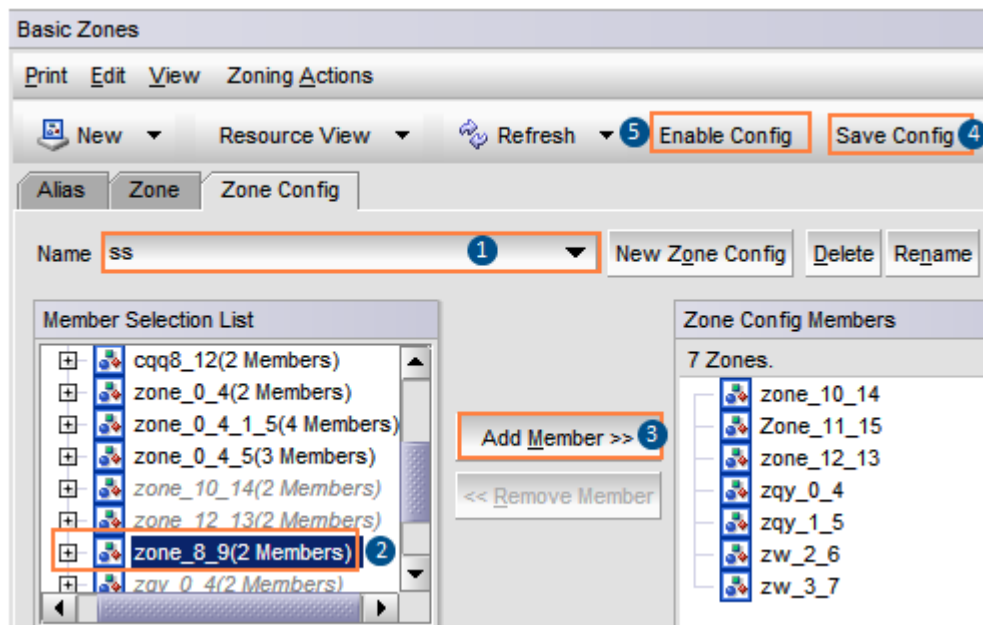


**Step 6** Add the new zone to the configuration file and activate the new zone.

1. On the **Zone Admin** page, click the **Zone Config** tab. In the **Name** drop-down list, choose the currently effective configuration **ss**.
2. In **Member Selection List**, select zone **zone\_8\_9** and click **Add Member** to add it to the configuration file.
3. Click **Save Config** to save the configuration and click **Enable Config** to make the configuration take effect.

Figure 4-18 shows the **Zone Config** page.

Figure 4-18 Zone Config tab page



**Step 7** Verify that the configuration takes effect.

In the navigation tree of **Web Tools**, choose **Task > Monitor > Name Server** to go to the **Name Server** page. You can also choose **Monitor > Name Server** in the navigation bar.

Figure 4-19 shows the **Name Server** page.



Figure 4-19 Name Server page

Domain	...	Device Port	WWN	Device Name	WWN Company ID	Member Of Zones
1(0x1)	0	10:00:00:00:c9:64:fe:1b		Emulex LPe111-H FV2.8...	Emulex Corporation	zone_0_4_1_5, zone_1
1(0x1)	1	10:00:00:00:c9:64:fe:91		Emulex LPe111-H FV2.8...	Emulex Corporation	zone_0_4, zone_0_4_
1(0x1)	2	20:18:36:32:33:39:38:34		2...		zw_2_6*
1(0x1)	3	20:08:36:32:33:39:38:34		2...		zw_3_7*
1(0x1)	4	20:08:00:22:a1:03:7e:bf		2...		zone_0_4, zone_0_4_
1(0x1)	5	20:18:00:22:a1:03:7e:bf		2...		zone_0_4_1_5, zone_1
1(0x1)	6	21:01:00:1b:32:26:1c:7d			Qlogic Corp.	zw_2_6*
1(0x1)	7	21:00:00:1b:32:06:1c:7d			Qlogic Corp.	zw_3_7*
1(0x1)	8	20:09:00:22:a1:04:16:61		2...		cqq8_12, zone_8_9*
1(0x1)	9	10:00:00:00:c9:9b:5d:95			Emulex Corporation	zone_8_9*
1(0x1)	10	50:06:01:69:30:20:97:f5		0226	Clariion	Zone_10_14, zone_10
1(0x1)	11	50:06:01:60:30:20:97:f5		0226	Clariion	Zone_11_15*
1(0x1)	12	20:18:00:22:a1:04:16:61		2...		cqq8_12, zone_12_13*
1(0x1)	13	10:00:00:00:c9:9b:5d:94			Emulex Corporation	zone_12_13*

The preceding figure shows that ports 8 and 9 are members of **zone\_8\_9** that is now effective. An effective zone is marked by an asterisk (\*).

----End

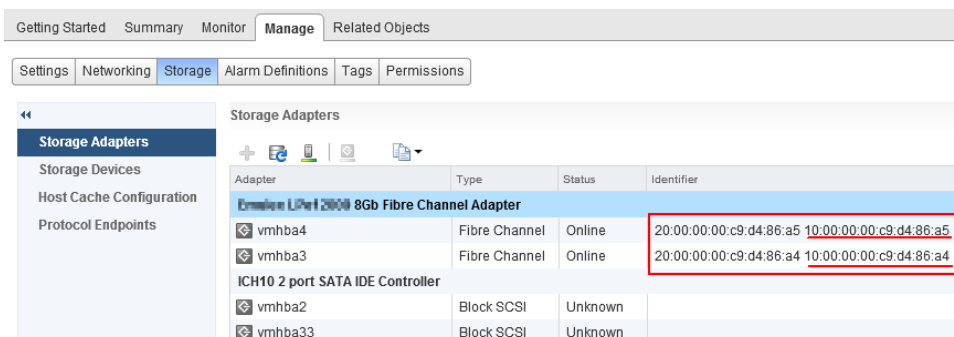
### 4.7.2.2 Querying a Host WWPN

Before connecting a host to a storage system, check whether a host HBA can be identified (whether the driver is properly installed) and record the WWPN of the HBA's port. This section describes how to query the WWPN of an HBA in a VMware environment.

### Procedure

- Step 1** Enable the host to identify an HBA. After an HBA is installed on the host, you can check the HBA information. Go to the vSphere Web Client configuration management page (vCenter 6.0 as an example) and choose **Manage > Storage > Storage Adapter**. In the function pane, view the HBA information, as shown in [Figure 4-20](#).

Figure 4-20 Viewing the HBA information



The command output indicates that the host has identified two Fibre Channel host ports.

**Step 2** Query the WWNs of the HBAs. You can see that the WWNs of the two ports are **10000000c9d486a5** and **10000000c9d486a4** (the WWPN is the last 16 characters).

---End

## Follow-up Procedure

If you want to view the HBA details, view them on the CLI. The HBA information varies according to different ESXi versions.

Run the **esxcli storage core adapter list** and **esxcfg-module -i qlnativefc** commands to check the HBA information. *qlnativefc* indicates the HBA driver that is queried by running the **esxcli storage core adapter list** command.

### 4.7.2.3 (Optional) Setting Fibre Channel Port Information

Configure Fibre Channel port parameters to ensure proper communication between the storage system and application server.

## Prerequisites

The HBA information, including the HBA identifier and speed, has been obtained on the application server.



## Context

Note the following when you set Fibre Channel ports:

- If the storage device connects to an application server through a Fibre Channel port, ensure that the rate of the Fibre Channel port on the storage device is the same as that of the peer host bus adapter (HBA) port on the application server.
- When two storage devices connect to each other through Fibre Channel ports, ensure that the rates of the Fibre Channel ports on both storage devices are the same.

## Procedure

**Step 1** Go to the **FC Port** dialog box.

1. On the right navigation bar, click  **System**.
2. Click the controller enclosure where the Fibre Channel port resides.
3. Click  to switch to the rear view.
4. Click the Fibre Channel port whose information you want to modify.  
The **FC Port** dialog box is displayed.

**Step 2** Click **Modify**.

**Step 3** In **Configured Rate (Gbit/s)**, select a data transfer rate for the Fibre Channel port.

Figure 4-21 FC Port

Location:	CTE0.L3.IOM0.P0
Health Status:	Normal
Running Status:	Link up
WWPN:	2218111545326912
Configured Rate (Gbit/s):	Autonegot...
Working Rate (Gbit/s):	8
Max. Working Rate (Gbit/s):	8
Working Mode:	P2P
Port Switch:	Enable

Apply Cancel Help

---



## NOTICE

- The rate and mode of the Fibre Channel port on a storage system must be consistent with those of the Fibre Channel HBA on the peer application server. If the rates and modes are inconsistent, the communication will fail.
- The rate and mode of the Fibre Channel ports on two storage systems that are connected to each other must be consistent. If the rates and modes are inconsistent, the communication will fail.

---

Available rates of a Fibre Channel port are **2 Gbit/s**, **4 Gbit/s**, **8 Gbit/s**, **16 Gbit/s**, and **Autonegotiation**. Select a fixed value after learning the rate of the peer Fibre Channel port.



## NOTE

- If the configured maximum rate of a port is 8 Gbit/s, you can set the value to be **2 Gbit/s**, **4 Gbit/s**, or **8 Gbit/s**.
- If the configured maximum rate of a port is 16 Gbit/s, you can set the value to be **4 Gbit/s**, **8 Gbit/s**, or **16 Gbit/s**.
- The system selects **Autonegotiation** by default. The rate of the Fibre Channel port on the storage system automatically becomes the same as that on the host.

### Step 4 Confirm the Fibre Channel port configuration.

1. Click **OK**.  
The **Danger** dialog box is displayed.
2. Confirm the information in the dialog box and select **I have read and understood the consequences associated with performing this operation..**
3. Click **OK**.  
The **Success** message box is displayed, indicating that the operation succeeded.

4. Click **OK**.

----End

## 4.8 Creating a Host

Create a host to establish a connection between a storage system and an application server, and add an initiator for the host to establish a mapping relationship between the host and application server.

### 4.8.1 Automatically Scanning for a Host

You can add hosts to a host list by automatically scanning for hosts to save your time.

#### Prerequisites

- Hosts have the UltraPath installed. Multipathing software provided with host operating systems is not supported.
- In an iSCSI networking environment, initiators have been configured for hosts to connect to the storage system.
- In an FC networking environment, the HBA port of a host and the port of the storage system are in the same zone.

#### Context

By default, automatic host scan is not enabled. If no hosts are found after the scan is complete, scan for disks on application servers and retry.

#### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Host**.

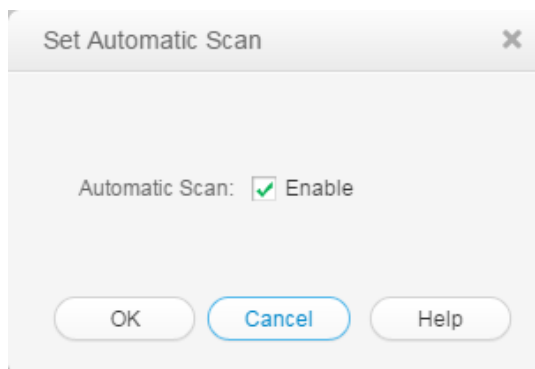
**Step 3 Optional:** Enable automatic host scan.

#### **NOTE**

- If automatic host scan is enabled, skip this step.
- If the storage system automatically detects a host initiator and the initiator has not been added to any host, a 16 KB virtual disk is displayed on the host operating system. After the initiator is added to a host, the virtual disk disappears.

1. Click **Parameter Settings**.

The **Set Automatic Scan** dialog box is displayed.



2. Select **Enable** and click **OK**.  
The **Execution Result** dialog box is displayed indicating that the operation succeeded.
3. Click **OK**.

**Step 4** Choose **Create > Automatic Scan**.  
The **Confirm** dialog box is displayed.

**Step 5** Click **OK**.  
The system starts scanning for hosts. Detected hosts will be added to the host list.

**Step 6** Click **Close**.

----End

## 4.8.2 Manually Creating a Host

You can manually create a virtual host for a storage device.

### Procedure


**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Host**.

**Step 3** Choose **Create > Manually Create**.  
The **Create Host Wizard** dialog box is displayed.

**Step 4** Set basic information for the host.

Create Host Wizard: Step 4-1

 **Set Host Information**  
Enter basic information for the host.

\* Name:

Description:

OS:  ▼

IP Address:

Device Location:

**Table 4-14** describes related parameters.

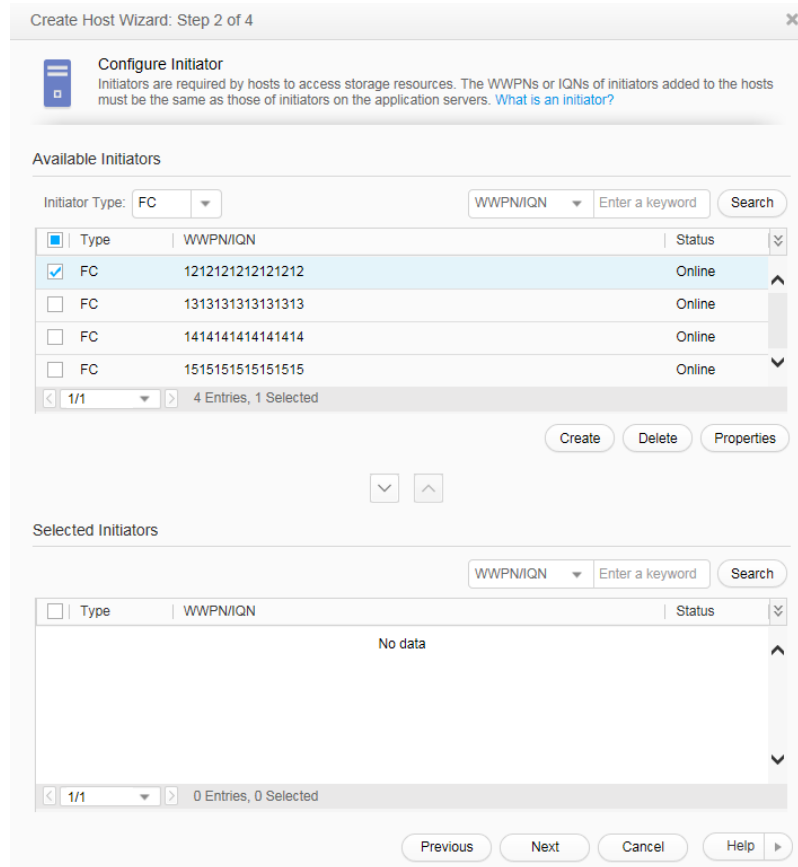
**Table 4-14** Host parameters


Parameter	Description	Setting
Name	Name of a host.	[Value range] <ul style="list-style-type: none"> <li>● The name must be unique.</li> <li>● The name can contain only letters, digits, periods (.), underscores (_), and hyphens (-).</li> <li>● The name contains 1 to 31 characters.</li> </ul> [Example] <b>Host001</b>
Description	Description of a host.	[Example] -

Parameter	Description	Setting
OS	Operating system used by a host. <b>NOTE</b> The selected operating system must be the same type of host operating system that the storage system is connected to.	[Value range] Possible values are <b>Linux, Windows, Windows Server 2012, Solaris, HP-UX, AIX, XenServer, Mac OS, VMware ESX, Oracle VM, and OpenVMS.</b> <b>NOTE</b> <ul style="list-style-type: none"> <li>● If the host runs the Windows operating system and you need to use the space reclaiming function of thin LUNs, you can only select Windows Server 2012.</li> <li>● If the application type is FusionCompute, you are advised to select <b>Linux</b> as the operating system.</li> </ul> [Example] <b>VMware ESX</b>
IP Address	IP address of a host.	[Example] <b>192.168.1.100</b> <b>NOTE</b> If the host is connected through iSCSI links, enter the real service IP address of the host for further management and search.
Device Location	Location of a host.	[Example] <b>Chengdu</b>

**Step 5** Click **Next**.

**Step 6** Configure an initiator for the host.



1. In the **Available Initiators** area, select **Initiator Type** based on your service needs.
2. In the initiator list, select one or multiple initiators.
3. Click  to add the initiator to the **Selected Initiators** area.

 **NOTE**

- If the initiator information has been configured on the application server, the DeviceManager can automatically detect the configured initiator. You only need to select the initiator information from the initiator list rather than manually creating it, and do not add initiators on different application servers to a same host. Create an initiator if none is available in the list.
- If the host operating system is **HP-UX**, create an initiator manually.
- If the CHAP authentication is not enabled on the initiator, click **Modify**. In the **Modify Initiator** dialog box that is displayed, configure the CHAP authentication parameters.
- If the CHAP authentication has been enabled on the initiator and you want to change the CHAP authentication password, click **Modify**. In the **Modify Initiator** dialog box that is displayed, change the CHAP authentication password. When you change the CHAP authentication password, you need to enter **Old password** to improve the storage system security instead of directly changing the password.
- The CHAP authentication user name and password configured on the storage system must be the same as those configured on the application server. After changing the CHAP authentication password on the storage system, you need to use the new password to configure the CHAP authentication again on the application server.

**Step 7** Confirm the host creation.

1. Click **Next**.  
The **Summary** page is displayed.



2. Click **Finish** to confirm the information of the host to be created.  
If you already added initiators to the host, execute [Step 7.3](#). If you do not add any initiator to the host, execute [Step 7.4](#).
3. The security alert dialog box is displayed. Carefully read the content of the dialog box. Then select **I have read and understood the consequences associated with performing this operation.** to confirm the information and click **OK**.
4. The **Execution Result** page is displayed, indicating that the operation succeeded. Click **Close** to finish creating a host.

----End

## 4.8.3 Batch Creating Hosts

This operation enables you batch create virtual hosts for storage devices.

### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Host**.

**Step 3** Choose **Create** > **Batch Create**.  
The **Batch Create Host** dialog box is displayed.

**Step 4** Set basic information about the host.  
[Table 4-15](#) describes related parameters.

**Table 4-15** Host parameters

Parameter	Description	Value
Name	Name of the host.	[Value range] <ul style="list-style-type: none"> <li>● Must be unique.</li> <li>● Contains only letters, digits, underscores (_), periods (.), and hyphens (-).</li> <li>● Contains 1 to 31 characters.</li> </ul> [Example] Host001
Description	Description of the host.	[Example] -

Parameter	Description	Value
OS	Operating system of the host. <b>NOTE</b> The selected operating system must be the same type of host operating system that the storage system is connected to.	[Value range] Possible values are <b>Linux, Windows, Windows Server 2012, Solaris, HP-UX, AIX, XenServer, Mac OS, and VMware ESX, Oracle VM and OpenVMS.</b> <b>NOTE</b> <ul style="list-style-type: none"> <li>● If the host runs the Windows operating system and you need to use the space reclaiming function of thin LUNs, you can only select Windows Server 2012.</li> <li>● If the application type is FusionCompute, you are advised to select <b>Linux</b> as the operating system.</li> </ul> [Example] Windows
Device Location	Location of the host.	[Example] Chengdu
Quantity	Number of hosts to be created.	[Value range] 1 to 500 <b>NOTE</b> <ul style="list-style-type: none"> <li>● A maximum of 500 hosts can be created at a time.</li> <li>● When creating multiple hosts, the system automatically appends a number to host names for distinction. You can manually append numbers to host names.</li> </ul>

**Step 5** Click **OK**.

In the **Execution Result** dialog box that is displayed, click **Close**. You have finished batch creating hosts.

----End

## 4.9 Creating a Host Group

To allow hosts to use LUNs, you must add hosts into host groups. Then, establish mapping views between the LUN groups and host groups. By doing so, the hosts in the host groups can use the LUNs in the LUN groups. A host group can contain one or multiple hosts.

### Context

- Hosts in a host group can run different operating systems.

- A host group can include a maximum of 64 hosts.
- A host can be added to a maximum of 64 host groups.

## Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Host** > **Host Group**.

**Step 3** Click **Create**.

The **Create Host Group** dialog box is displayed.

**Step 4** Set parameters of the host group. [Table 4-16](#) describes related parameters.

**Table 4-16** Host group parameters

Parameter	Description	Setting
Name	Name of a host group.	[Value range] <ul style="list-style-type: none"> <li>● The name must be unique.</li> <li>● The name can contain only letters, digits, periods (.), underscores (_), and hyphens (-).</li> <li>● The name contains 1 to 31 characters.</li> </ul> [Example] <b>HostGroup001</b>
Description	Description of a host group.	[Example] -

**Step 5** Select the hosts you want to add to the host group.

1. In the **Available Hosts** area, select one or multiple hosts based on your service requirements.

---

### NOTICE

If hosts to be added into the host group belong to different clusters, data access conflicts may occur, resulting in data loss. Before this operation, you are advised to install cluster software to manage hosts.

---

### NOTE

By default, the **Shows only the hosts that do not belong to any host group** checkbox in the bottom left corner of the dialog box is selected to facilitate host locating.

2. Click  to add the hosts to the **Selected Hosts** area.

**Step 6** Confirm the creation of the host group.

1. Click **OK**.
  - If multiple hosts have been selected to add to a host group, a security alert dialog box is displayed. Confirm the information and click **OK**. The **Execution Result** dialog box is displayed, indicating that the operation succeeded.
  - If only one host has been selected to add to a host group, the **Execution Result** dialog box is displayed, indicating that the operation succeeded.
2. Click **Close**.

----End

## 4.10 (Optional) Creating a Port Group

A port group is a logical combination of multiple physical ports. The storage system specifies ports to set up mappings between storage resources (LUNs) and servers. This operation enables you to create a port group and add it to a mapping view. After that, LUNs of a specified LUN group use the ports of the port group to communicate with the corresponding hosts of the host group. If no port group is added to the mapping view, available ports are randomly used. A port group can be added to a maximum of 64 mapping views. A port can be added to a maximum of 64 port groups.

### Procedure

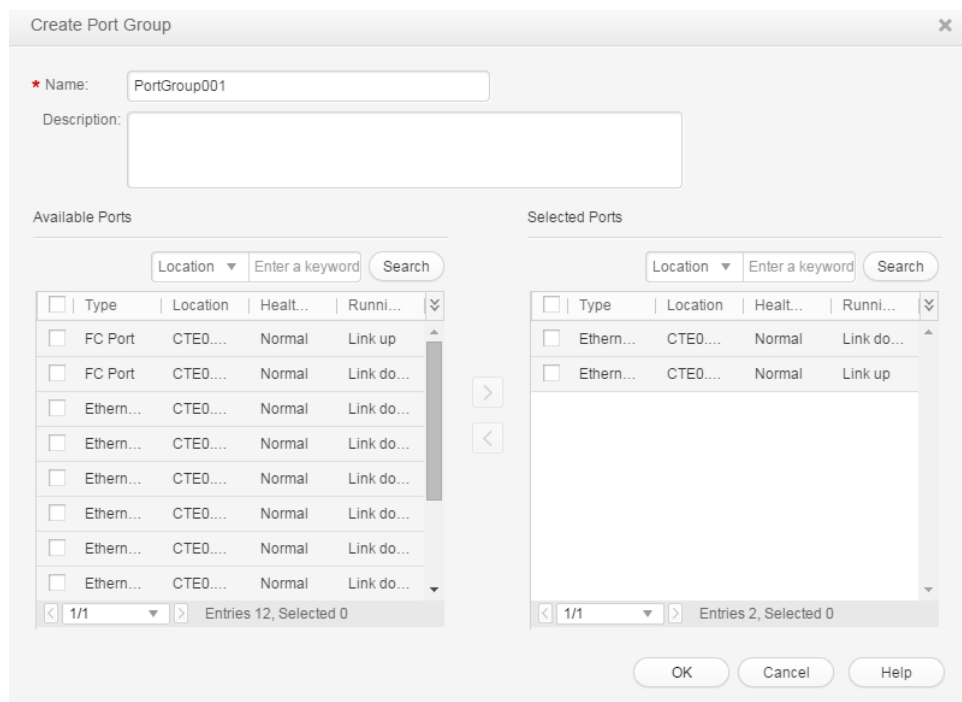
**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Port** > **Port Groups**.

**Step 3** Click **Create**.

The **Create Port Group** message box is displayed.

**Step 4** Set parameters of the port group. [Table 4-17](#) describes related parameters.



**Table 4-17** Port group parameters


Parameter	Description	Setting
Name	Name of a port group. Name a port group in accordance with the following rules so that the port group is available to host applications: <ul style="list-style-type: none"> <li>● The name must be unique.</li> <li>● The name can contain only letters, digits, periods (.), underscores (_), and hyphens (-).</li> <li>● The value contains 1 to 31 characters.</li> </ul>	[Example] <b>PortGroup001</b>
Description	Description of a host group.	[Example] <b>None</b>

**Step 5** Select the ports you want to add to the port group.

1. Select the ports you want to add to the port group in **Available Ports** list.



One port can be added to different port groups.

2. Click  and add the ports to **Selected Ports**.

**Step 6** Confirm your operation.

1. Click **OK**.  
 The **Execution Result** message box is displayed, indicating that the operation succeeded.
2. Click **Close**.

----End

## Result

On the **Port Groups** page, the newly created port group is displayed in the port group list.

## 4.11 Creating a Mapping View

This operation enables you to create a mapping view and manage the mapping relationship between multiple host groups and LUN groups by adding them to the mapping view.

### Context

- A host group can be added to a maximum of 64 mapping views.
- A LUN group can be added to a maximum of 64 mapping views.
- A port group can be added to a maximum of 64 mapping views.

Based on the ports used by mapping views, mapping views can be classified into LUN masking and LUN mapping.

- LUN masking: A LUN is bound with the WWPN or IQN of a host port to establish a one-to-one or N-to-one connection and access relationship with the host port. A host can identify the same LUN regardless of whichever port on the storage system is connected to the host.
- LUN mapping: A LUN is bound with a front-end port on the storage system. The LUN that a host can access varies with the storage port connected to the host.

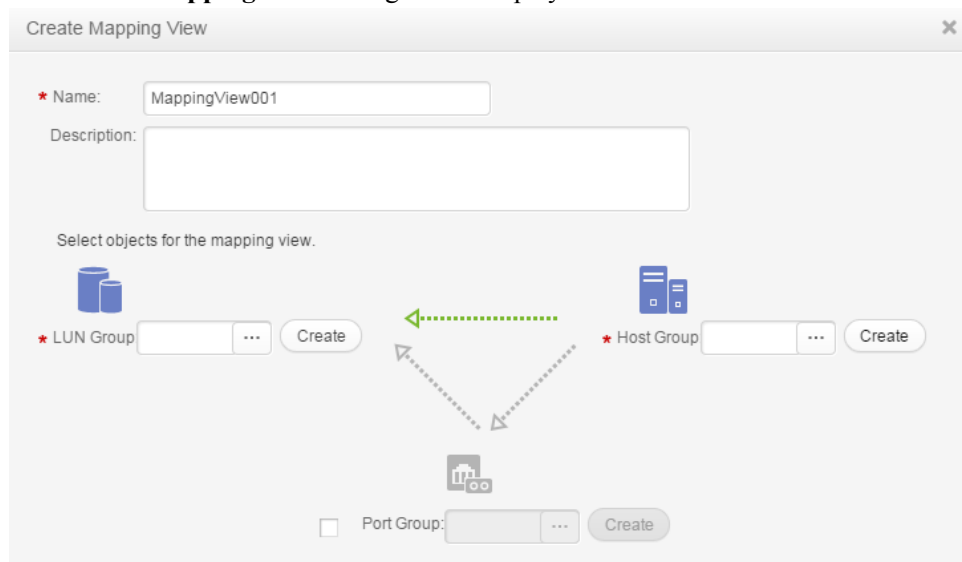
## Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Mapping View**.

**Step 3** Click **Create**.

The **Create Mapping View** dialog box is displayed.



**Step 4** Set basic properties for the mapping view.

1. In the **Name** text box, enter a name for the mapping view.
2. **Optional:** In the **Description** text box, add the mapping view description.

**Step 5** Add a host group to the mapping view.

1. In **Host Group**, click .
- The **Select Host Group** dialog box is displayed.

### **NOTE**

1. If the service requires a new host group, click **Create** to create one.
2. From the host group list, select the host group you want to add to the mapping view.
3. Click **OK**.

**Step 6** Add a LUN group to the mapping view.

1. In **LUN Group**, click .

The **Select LUN Group** dialog box is displayed.

 **NOTE**

- If the service requires a new LUN group, click **Create** to create one.
- By default, the **Show only the LUN groups that do not belong to any mapping view** checkbox in the bottom left corner of the dialog box is selected to facilitate LUN group locating.

2. **Optional:** Select **Set host LUN ID**. In **Start ID**, select an ID.

 **NOTE**

- A host LUN ID is an ID allocated by the storage system to a LUN mapped to a host.
- Starting from the selected ID, the system will automatically assign a unique host LUN ID to each LUN in the selected LUN group.
- If you do not select **Set host LUN ID** and there is no other mapped LUN in the host, the system will automatically assign a unique host LUN ID (starting from 0) to each LUN in the selected LUN group by default.

3. From the LUN group list, select the LUN group you want to add to the mapping view.
4. Click **OK**.

**Step 7 Optional:** Add a port group to the mapping view.

 **NOTE**

This operation is required if the mapping view type is port mapping.

1. Select **Port Group**

 **NOTE**

If a port group is added to the mapping view, LUNs of a specified LUN group use the ports of the port group to communicate with the corresponding hosts of the host group. If no port group is added to the mapping view, available ports are randomly used.

2. Click .

The **Select Port Group** dialog box is displayed.

 **NOTE**

If your service requires a new port group, click **Create** to create one.

3. From the port group list, select the port group you want to add to the mapping view.
4. Click **OK**.

**Step 8** Confirm the creation of the mapping view.

1. Click **OK**.

The security alert dialog box is displayed.

 **NOTE**

If multiple hosts are added to one same mapping view, it is possible that multiple hosts write data to the same LUN, this may cause data damage or inconsistent. You are advised to install cluster management software on application servers.


2. Carefully read the content of the dialog box. Then 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



## Follow-up Procedure

After creating a mapping view, scan for the mapped LUNs manually on the ESXi host. The scanning method is as follows:

1. Log in to vSphere Web Client (vCenter 6.0 as an example). Choose **Manage > Storage > Storage Devices**.
2. Click .  
The **Rescan Storage** dialog box is displayed.
3. Keep the default system settings and click **OK**. Mapped LUNs are scanned automatically.

## 4.12 Configuring the VVols Function

Install VASA Provider to provide the Virtual Volumes (VVols) function.

### Prerequisites

The eSDK Storage VASA manual has been downloaded. To obtain the manual, log in to <http://support.huawei.com/enterprise/>, and apply for an account and password. Log in to the website using the user name and password. In the search field, enter **eSDK Storage Plugins**. Select the path that is automatically associated with this parameter. Go to the documentation page to download the *Quick Guide (VASA2.0)* of the required version.

### Procedure

- Step 1** Install the VASA Provider.
- Step 2** Register the storage system in eSDK and configure a storage container.
- Step 3** Register VASA Provider in vCenter.

----End

## 4.13 Using a VVOL Datastore to Create a VM

This section describes how to use a virtual datastore to create a VM.


### Prerequisites

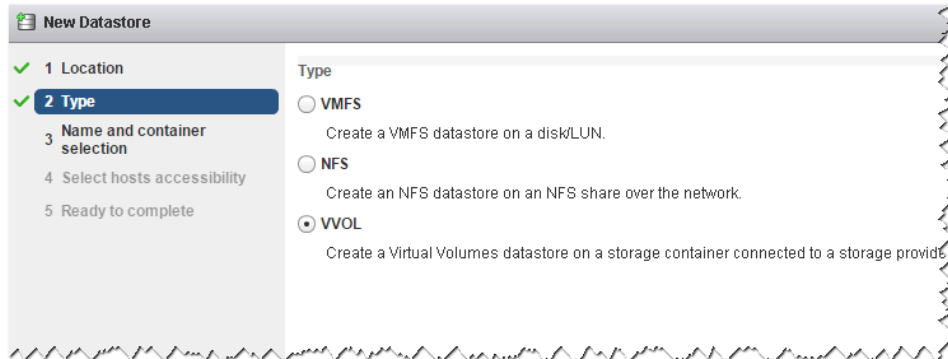
- A PE LUN has been mapped to the ESXi server.
- A storage system has been registered and a storage container has been configured on the unified eSDK management platform.
- The VASA Provider has been registered in vCenter.

### Procedure

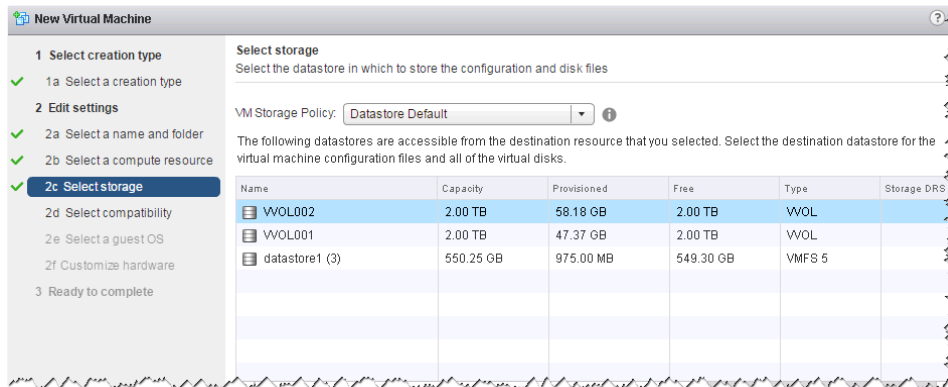
- Step 1** Log in to the ESXi server.
- Step 2** In **VM Storage Policies**, configure data service rules.

**Step 3** If the vCenter is newly built, you need to create a data center.

**Step 4** In the vCenter, click **Storage**, right-click the vCenter data center, and choose **Related Objects** > **Datstores** > . Create a datastore whose type is VVOL.



**Step 5** Right-click the vCenter data center, choose **New Virtual Machine** > **New Virtual Machine**, and select an appropriate VM storage policy and a VVOL datastore to create a VM.



----End

## Follow-up Procedure

- After creating a VM, you can find the following information when checking the storage system:
  - If the VM is powered off, two VVols, the data Volume and configuration Volume, are generated on the storage array. The configuration Volume is a thin Volume with fixed 4 GB in size.
  - If the VM is powered on, another memory VVol is generated. This VVol is a thick VVol and has the same memory size as the VM.
- After creating snapshots for the VMs, you will find that snapshots are created for data VVols that are used by VMs.
- After creating clones for the VMs (from VVOL datastore to VVOL datastore), you will find that full LUN copy tasks are created for data VVols of the VMs.
- After creating migration tasks for the VMs (from VVOL datastore to VVOL datastore), you will find the following situations:
  - If a VM has no snapshots, full LUN copy tasks are created for data VVols of VMs.

- If a VM has snapshots, then the system creates a full copy task for a VVol LUN snapshot, and then creates incremental copy tasks for the data VVols of other VVol LUN snapshots and VMs.
- After creating fast clone tasks for the VMs, you can find the following information when checking the storage system:  
VVol snapshots are generated for data VVols used by VMs. Snapshots for these snapshots are generated as well.
- After expanding the capacity of volumes on the VMs, you will find that the capacities of data VVols used by VMs are expanded or new data VVols are generated.
- If you roll back a snapshot of a VM in vCenter when snapshot rollback is being executed in the storage system, you are not allowed to perform the following operations in vCenter:
  - Delete the snapshot that is being rolled back.
  - Roll back other snapshots of the VM.
- For fast clone of VMs, a maximum of 2 levels of cascading is recommended to ensure system performance.

# 5 Creating Storage Resources Based on Applications

---

## About This Chapter

For 2000, 5000 and 6000 series storage systems, you can configure the storage resources for Microsoft Exchange, VMware, Hyper-V, Oracle, and SQL Server according to the characteristics of storage system and to enable the application server to use allocated storage resources.

### [5.1 Configuring Microsoft Exchange](#)

This section describes Microsoft Exchange and the steps to configure storage resources for it.

### [5.2 Configuring VMware](#)

This section describes VMware and the steps to configure storage resources for it.

### [5.3 Configuring Hyper-V](#)

This section describes Hyper-V and the steps to configure storage resources for it.

### [5.4 Configuring Oracle](#)

This section describes Oracle and the steps to configure storage resources for it.

### [5.5 Configuring SQL Server](#)

This section describes SQL Server and the steps to configure storage resources for it.

## 5.1 Configuring Microsoft Exchange

This section describes Microsoft Exchange and the steps to configure storage resources for it.

### 5.1.1 About Microsoft Exchange

Developed by Microsoft, Microsoft Exchange is a software product that provides the email and collaboration services.

The application scenarios of Microsoft Exchange are as follows:

- As an email system, Microsoft Exchange can be used to construct email servers for enterprises and education institutions.

- As a collaboration platform, Microsoft Exchange can be used to develop work flows, knowledge management systems, web systems, and other information systems.

## 5.1.2 Creating a Microsoft Exchange Instance

This operation allows you to create a Microsoft Exchange instance.

### Prerequisites

The system has sufficient storage space.

### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Application** >  **Microsoft Exchange**.

**Step 3** Click **Create**.

The **Create Microsoft Exchange Storage Resource Wizard** dialog box is displayed.

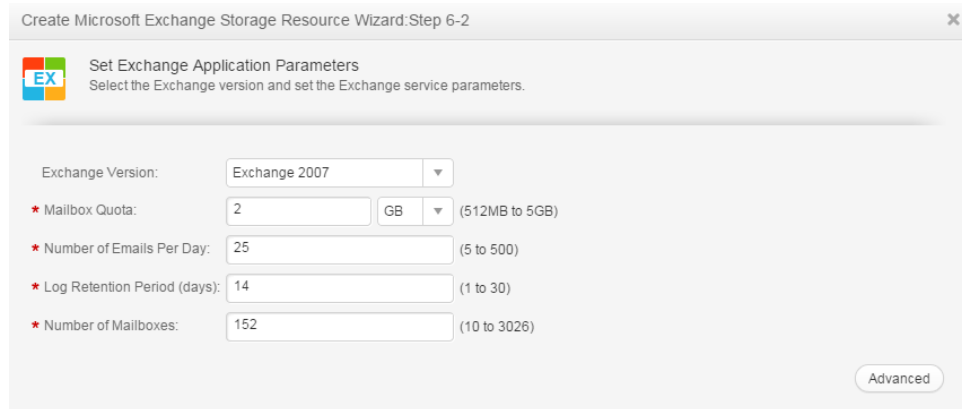
**Step 4** Set basic information about the Microsoft Exchange instance, as shown in [Table 5-1](#).

**Table 5-1** Parameters of a Microsoft Exchange instance

Parameter	Description	Value
Name	Name of a Microsoft Exchange instance.  The name must meet the following requirements so that the instance is available to host applications: <ul style="list-style-type: none"> <li>● Must be unique.</li> <li>● Contains only letters, digits, underscores (_), periods (.), and hyphens (-).</li> <li>● Contains 1 to 22 characters.</li> </ul>	[Example] <b>ExchangeApp_001</b>
Description	Description of a Microsoft Exchange instance. <b>Description</b> must contains 0 to 255 characters.	[Example] -

**Step 5** Click **Next** to set the Exchange application parameters.

[Table 5-2](#) describes related parameters.



**Table 5-2** Parameters of a Microsoft Exchange application

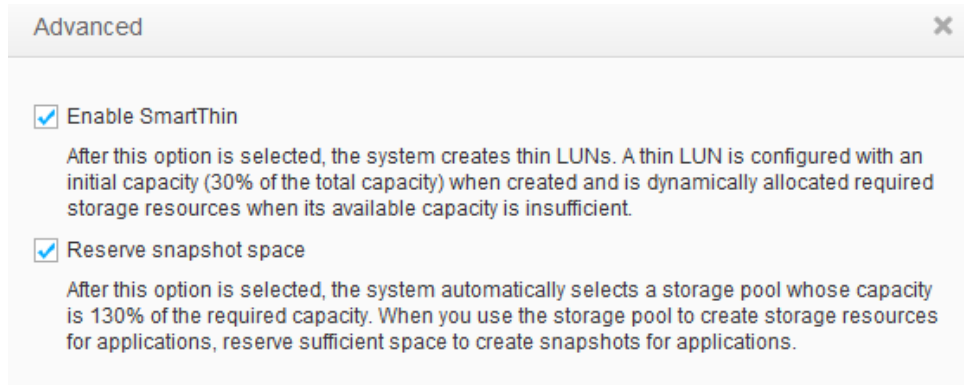
Parameter	Description	Value
Exchange Version	Version of the Exchange software.	[Value range] The value can be <b>Exchange 2007</b> , <b>Exchange 2007 LCR</b> , <b>Exchange 2007 local LCR</b> , <b>Exchange 2007 remote LCR</b> , <b>Exchange 2010</b> , or <b>Exchange 2010 with DAG</b> . The default value is <b>Exchange 2010</b> . [Example] <b>Exchange 2010</b>
Mailbox Quota	Maximum capacity of a Microsoft Exchange email box. The unit of the parameter value can be <b>MB</b> or <b>GB</b> .	[Value range] The value ranges from 512 MB to 5 GB. The default value is <b>2 GB</b> . [Example] <b>512 MB</b>
Number of Emails Per Day	Maximum emails that a Microsoft Exchange email box can send and receive per day.	[Value range] The value ranges from 5 to 500. The default value is <b>25</b> . [Example] <b>25</b>
Log Retention Period (days)	Maximum retention period of logs generated by the Exchange email server.	[Value range] The value ranges from 1 to 30 days. The default value is <b>14</b> . [Example] <b>14</b>

Parameter	Description	Value
Number of Mailboxes	Maximum number of email boxes supported by the Exchange email server.	[Value range] The value of this parameter is subject to the number of emails per day, log retention period (days), and remaining capacities of storage pools. The value dynamically changes. [Example] <b>152</b>

**Step 6 Optional:** Set advanced Exchange properties.

1. Click **Advanced**.  
The **Advanced** dialog box is displayed.
2. Set advanced properties for exchange applications.

**Table 5-3** describes related parameters.



**Table 5-3** Parameters in advanced properties of a Microsoft Exchange application

Parameter	Description	Value
Enable SmartThin	After this function is enabled, the system will create thin LUNs. After being created, a thin LUN is only assigned initial capacity (30% of the total capacity). If the available capacity is insufficient, the system dynamically assigns storage resources in storage pools to the thin LUN based on the actual required capacity.	[Example] <b>Enable SmartThin</b>

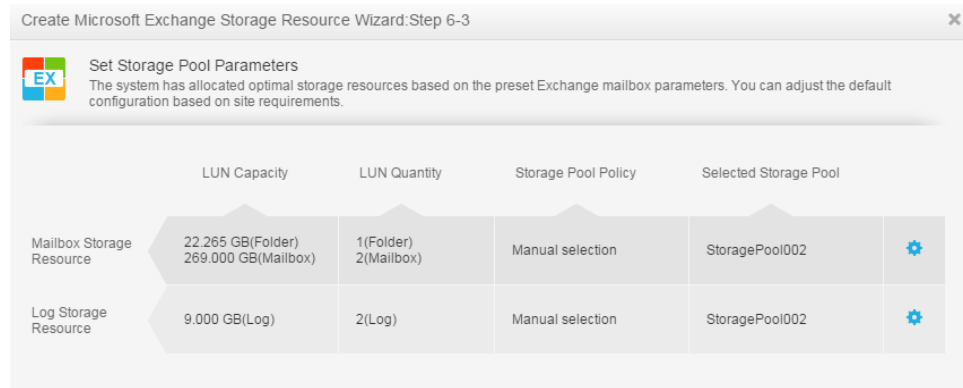
Parameter	Description	Value
Reserve snapshot space	After this function is enabled, the system automatically selects storage pools whose capacities are 130% of the actual required capacity. When using storage pools to create storage resources for applications, remember to reserve sufficient space for snapshots.	[Example] -

3. Click **OK**.

You are returned to the **Set Exchange Application Parameters** page.

**Step 7** Click **Next** and set parameters for Microsoft Exchange storage resources. The system will allocate optimal storage resources based on preset Microsoft Exchange parameters.

**Table 5-4** describes storage resource parameters.



**Table 5-4** Exchange storage resource parameters

Parameter	Description	Value
LUN Capacity	LUN storage space allocated to store emails or logs.	[Example] <b>300 GB</b>
LUN Quantity	Number of LUNs allocated to store emails, folders, or logs.	[Example] <b>7 (log)</b>



Parameter	Description	Value
Storage Pool Policy	<p>The system sets storage pool allocation policies based on preset Microsoft Exchange application parameters. The value can be <b>High performance</b>, <b>Performance/Cost balance</b>, <b>Low cost</b>, or <b>Manual selection</b>. The four values are described as follows:</p> <ul style="list-style-type: none"> <li>● <b>High performance</b>: The system automatically selects a RAID 6 storage pool containing SAS disks only. If such a storage pool does not exist in the system, create one.</li> <li>● <b>Performance/Cost balance</b>: The system automatically selects a RAID 6 storage pool containing SAS and NL-SAS disks only. If such a storage pool does not exist in the system, create one.</li> <li>● <b>Low cost</b>: The system automatically selects a RAID 6 storage pool containing NL-SAS disks only. If such a storage pool does not exist in the system, create one.</li> <li>● <b>Manual selection</b>: Users define storage pools that meet the Exchange service requirements.</li> </ul>	<p>[Example] <b>Manual selection</b></p>
Selected Storage Pool	Name of the storage pool automatically allocated by the system to a Microsoft Exchange instance.	<p>[Example] <b>StoragePool001</b></p>

**Step 8 Optional:** If no desired storage pools are available, click  and modify **Storage Pool Policy** in the displayed dialog box, or click **Create Storage Pool** to create one. [Table 5-4](#) describes related parameters.


**Step 9 Optional:** Select a host to which you want to map the instance.

 **NOTE**

If a host is selected, the system automatically creates a host group for the host and adds the host group to a mapping view. If no host is selected, manually create a host group and add the host group to a mapping view when you add a mapping host, so that the mapping host can access storage resources.

1. Click **Next**.

The **Select Mapping Hosts** page is displayed.

2. In the **Available Hosts** list, select the host that is used to access storage resources.
3. Click  to add the host to **Selected Hosts**.

**Step 10** Confirm your settings.

1. Click **Next**.

The **Summary** page is displayed.



2. Verify that the information about the Microsoft Exchange instance to be created is correct and click **Finish**.

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

 **NOTE**

- If a mapped host is selected, the system automatically creates a LUN group, a host group, and a mapping view, and adds the LUN group and host group to the mapping view.
- If no mapped host is selected, the system automatically creates a LUN group only. You need to manually create a host group and a mapping view for a mapped host and add the host to the mapping view. After being added to the mapping view, the host can access storage resources.
- The LUN group must contain all LUNs in the application instance.

3. Click **Close**. You have finished creating a Microsoft Exchange instance.

----End

## Follow-up Procedure

After successfully creating the application instance, scan for disks on the application server. For details, see the section **Making Storage Space Available** operation.

## 5.2 Configuring VMware

This section describes VMware and the steps to configure storage resources for it.

## 5.2.1 About VMware

VMware is a set of virtualization server software developed by VMware.

VMware can reduce operating expenses by consolidating and automating servers and minimize revenue loss through scheduled or unscheduled shutdown.

VMware mainly applies to:

- Server virtualization: Multiple operating systems run on one physical server as virtual machines. Each virtual machine can access computing resources on underlying servers.
- Storage resource virtualization: Software is used to divide storage layers. The performance and space utilization can be improved without new hardware.
- Desktop virtualization: Desktops are deployed in hosting mode, helping you quickly respond to changing requirements.
- Application virtualization: Critical service applications and platforms, such as databases, ERP, CRM, emails, collaboration systems, Java middleware, and business intelligence platforms, can be virtualized.
- Network virtualization: Software is used to reproduce physical networks completely and virtualize logical network connection devices and services (such as logical ports, switches, routers, firewalls, load balancers, and VPN). Then those virtualized resources can be used by other connected devices.

The storage system can automatically allocate storage resources based on service configurations of VMware applications.

## 5.2.2 Creating a VMware Instance

This operation allows you to create a VMware instance.

### Prerequisites

The system has sufficient storage space.

### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Application** >  **VMware**.

**Step 3** Select **LUN** in **Resource Type**.

**Step 4** Click **Create**.

The **Create VMware Storage Resource Wizard** is displayed.

**Step 5** Set basic information about the VMware instance to be created.

[Table 5-5](#) describes related parameters.

**Table 5-5** Parameters of a VMware instance

Parameter	Description	Value
Name	Name of a VMware instance. The name must meet the following requirements so that the instance is available to host applications: <ul style="list-style-type: none"> <li>● Must be unique.</li> <li>● Contains only letters, digits, and underscores (_).</li> <li>● Contains 1 to 22 characters.</li> </ul>	[Example] <b>VMwareApp_001</b>
Description	Description of a VMware instance. <b>Description</b> must contains 0 to 255 characters.	[Example] -

**Step 6** Click **Next** and select a virtualization type.

**Table 5-6** describes related parameters.

**Table 5-6** VMware application parameters

Parameter	Description	Value
Virtual desktop	Allows enterprise-level applications to dynamically access desktop systems remotely and implements central hosting of data centers.	[Example] Virtual desktop
Virtual server	Reduces consumption of manpower and material resources and simplifies work for small- and mid-size enterprises and enterprises that construct websites for the first time.	[Example] Virtual server

**Step 7** Set related parameters based on the selected virtualization type.

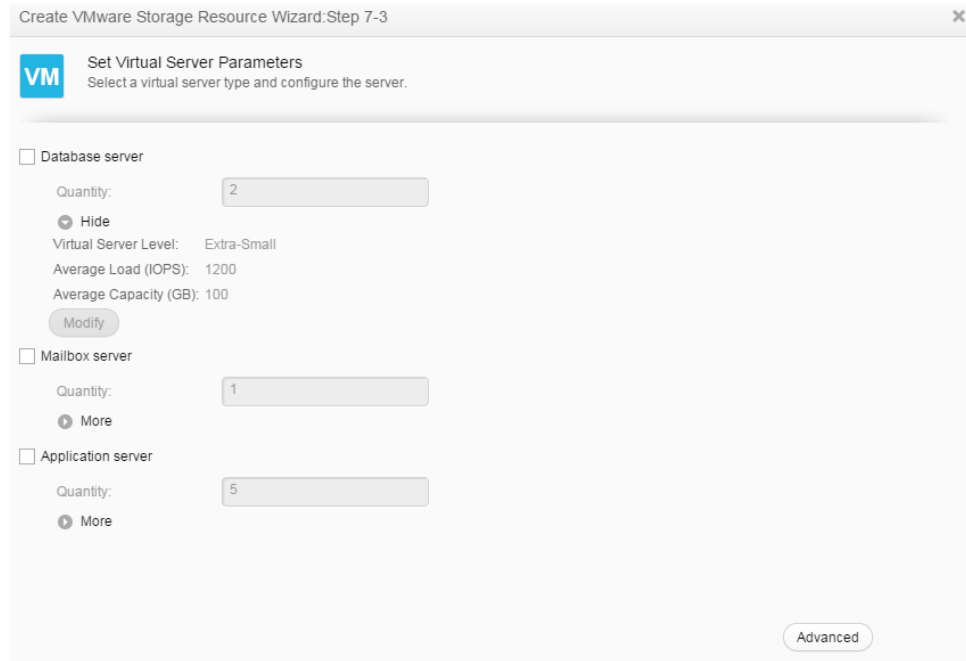
- If **Virtual desktop** is selected, set virtual desktop parameters, as shown in **Table 5-7**.



**Table 5-7** Virtual desktop parameters

Parameter	Description	Value
Virtual Desktop Level	Level of the virtual desktop constructed by VMware. The value of this parameter affects the values of <b>Space per Desktop (GB)</b> , <b>Memory per Desktop (GB)</b> , and <b>Load per Desktop (IOPS)</b> .	[Value range] The value can be <b>Small</b> , <b>Medium</b> , <b>Large</b> and <b>Extra-Large</b> . [Example] Medium
Space per Desktop (GB)	Maximum storage space allocated by VMware to each virtual desktop. The value of this parameter is subject to <b>Virtual Desktop Level</b> and is user-definable.	[Example] 160
Memory per Desktop (GB)	Maximum memory capacity allocated by VMware to each virtual desktop. The value of this parameter is subject to <b>Virtual Desktop Level</b> and is user-definable.	[Example] 4
Load per Desktop (IOPS)	Maximum IOPS of each virtual desktop. The value of this parameter is subject to <b>Virtual Desktop Level</b> and is user-definable.	[Example] 16
Desktop Quantity	Number of virtual desktops constructed by VMware.	[Example] 10

- If **Virtual server** is selected, set virtual server parameters, as shown in [Table 5-8](#).



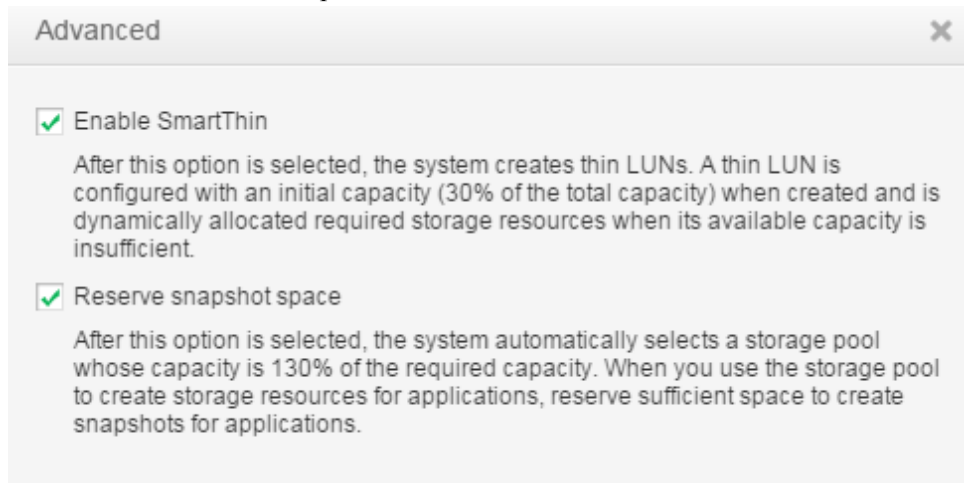
**Table 5-8** Virtual server parameters

Parameter	Description	Value
Database server	Type of a VMware virtual server.	[Example] -
Mailbox server	Type of a VMware virtual server.	[Example] -
Application server	Type of a VMware virtual server.	[Example] -
Quantity	Number of virtual servers constructed by VMware.	[Value range] The number of servers is subject to <b>Average Load (IOPS)</b> , <b>Average Capacity (GB)</b> , and type. [Example] <b>2</b>
Virtual Server Level	Level of a virtual server constructed by VMware. The value of this parameter affects the values of <b>Average Load (IOPS)</b> and <b>Average Capacity (GB)</b> .	[Value range] The value can be <b>Extra-Small</b> , <b>Small</b> , <b>Medium</b> , <b>Large</b> and <b>Extra-Large</b> . [Example] <b>Medium</b>

Parameter	Description	Value
Average Load (IOPS)	IOPS of a virtual server. The value of this parameter is subject to <b>Virtual Server Level</b> and is user-definable.	[Example] <b>25</b>
Average Capacity (GB)	Storage capacity allocated to virtual servers. The value of this parameter is subject to <b>Virtual Server Level</b> and is user-definable.	[Example] <b>25</b>

**Step 8 Optional:** Set advanced properties for VMware applications.

1. Click **Advanced**.  
The **Advanced** dialog box is displayed.
2. Set advanced properties for VMware applications.  
**Table 5-9** describes related parameters.



**Table 5-9** Parameters in advanced properties of a VMware application

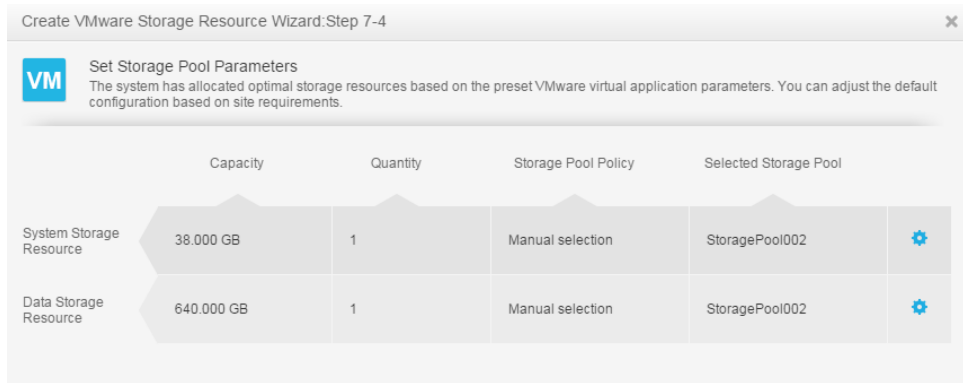
Parameter	Description	Value
Enable SmartThin	After this function is enabled, the system will create thin LUNs. After being created, a thin LUN is only assigned initial capacity (30% of the total capacity). If the available capacity is insufficient, the system dynamically assigns storage resources in storage pools to the thin LUN based on the actual required capacity.	[Example] Enable SmartThin

Parameter	Description	Value
Reserve snapshot space	After this function is enabled, the system automatically selects storage pools whose capacities are 130% of the actual required capacity. When using storage pools to create storage resources for applications, remember to reserve sufficient space for snapshots.	[Example] -

3. Click **OK**.

You are returned to the **Set Virtual Desktop Parameters** or **Set Virtual Server Parameters** page.

**Step 9** Click **Next** and set parameters for VMware storage resources. The system will allocate optimal storage resources based on preset VMware parameters.




**Table 5-10** VMware storage resource parameters

Parameter	Description	Value
LUN Capacity	LUN storage space allocated to store system data or data.	[Example] <b>640 GB</b>
LUN Quantity	Number of LUNs allocated to store system data or data.	[Example] <b>1</b>



Parameter	Description	Value
Storage Pool Policy	<p>The system sets storage pool allocation policies based on preset VMware parameters. The performance level of each VM is defined by <b>High performance</b>, <b>Performance/Cost balance</b>, <b>Low cost</b>, or <b>Manual selection</b>, described as follows:</p> <ul style="list-style-type: none"> <li>● High performance: The system automatically selects a RAID 6 storage pool containing SAS disks only. If such a storage pool does not exist in the system, create one.</li> <li>● Performance/Cost balance: The system automatically selects a RAID 6 storage pool containing SAS and NL-SAS disks only. If such a storage pool does not exist in the system, create one.</li> <li>● Low cost: The system automatically selects a RAID 6 storage pool containing NL-SAS disks only. If such a storage pool does not exist in the system, create one.</li> <li>● Manual selection: Users define storage pools that meet the VMware service requirements.</li> </ul>	[Example] Manual selection
Selected Storage Pool	Name of the storage pool automatically allocated by the system to a VMware instance.	[Example] <b>StoragePool001</b>


**Step 10 Optional:** If no desired storage pools are available, click  and modify **Storage Pool Policy** in the displayed dialog box, or click **Create Storage Pool** to create one. [Table 5-10](#) describes related parameters.

**Step 11 Optional:**

- If the **Use shared folders** is disabled in [Step 7](#), you are about to create block storage resource for the VMware application. Please select a host to which you want to map the instance.

-  **NOTE**

If a host is selected, the system automatically creates a host group for the host and adds the host group to a mapping view. If no host is selected, manually create a host group and add the host group to a mapping view when you add a mapping host, so that the mapping host can access storage resources.

- a. Click **Next**.  
The **Select Mapping Hosts** page is displayed.
  - b. In the **Available Hosts** list, select the host that is used to access storage resources.
  - c. Click  to add the host to **Selected Hosts**.
- If the **Use shared folders** is disabled in [Step 7](#), you are about to create file storage resource for the VMware application. Please select clients which can access the instance.

**Step 12** Confirm your settings.

1. Click **Next**.  
The **Summary** page is displayed.
2. Verify that the information about the VMware instance to be created is correct and click **Finish**.  
The **Execution Result** dialog box is displayed indicating that the operation succeeded.

 **NOTE**

- If a mapped host is selected, the system automatically creates a LUN group, a host group, and a mapping view, and adds the LUN group and host group to the mapping view.
- If no mapped host is selected, the system automatically creates a LUN group only. You need to manually create a host group and a mapping view for a mapped host and add the host to the mapping view. After being added to the mapping view, the host can access storage resources.

The LUN group must contain all LUNs in the application instance.

3. Click **Close**. You have finished creating a VMware instance.

----End

## Follow-up Procedure

After successfully creating the application instance, scan for disks on the application server. For details, see the section **Making Storage Space Available** operation.

## 5.3 Configuring Hyper-V

This section describes Hyper-V and the steps to configure storage resources for it.

### 5.3.1 About Hyper-V

Hyper-V is a virtualization product developed by Microsoft.

Hyper-V provides infrastructure and basic tools for the creation and management of the virtualization server computing environment. This virtualization environment can improve efficiency and decrease costs. Common application scenarios of Hyper-V are as follows:

- Constructing or expanding a private cloud environment: Hyper-V helps you get in touch with or expand the application scope of shared resources and adjusts resource usage on demand, delivering flexible IT services.
- Increasing hardware utilization: Hyper-V combines servers and work loads to fewer powerful physical computers, reducing the consumption of resources (such as power and physical space).
- Improving service continuity: Hyper-V minimizes the impact caused by scheduled and unscheduled shutdown on work loads.

- Constructing or expanding Virtual Desktop Infrastructure (VDI): Hyper-V provides a centralized desktop policy including the VDI. This policy helps you increase service flexibility, safeguard data security, simplify regulatory compliance, and facilitate the management of desktop operating systems and application programs. You can deploy Hyper-V and a remote desktop virtualization host on a same physical computer to provide virtual machines or virtual machine pools to individual users.
- Facilitating deployment and tests: You can reproduce different computing environments using virtual machines instead of hardware.

## 5.3.2 Creating a Hyper-V Instance

This operation allows you to create a Hyper-V instance.

### Prerequisites

The system has sufficient storage space.

### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Application** >  **Hyper-V**.

**Step 3** Click **Create**.

The **Create Hyper-V Storage Resource Wizard** is displayed.

**Step 4** Set basic information about the Hyper-V instance to be created.

[Table 5-11](#) describes related parameters.

**Table 5-11** Parameters in the basic information about a Hyper-V instance

Parameter	Description	Value
Name	Name of a Hyper-V instance. The name must meet the following requirements so that the instance is available to host applications: <ul style="list-style-type: none"> <li>● Must be unique.</li> <li>● Contains only letters, digits, underscores (_), periods (.), and hyphens (-).</li> <li>● Contains 1 to 22 characters.</li> </ul>	[Example] <b>HyperV_App_001</b>
Description	Description of a Hyper-V instance. <b>Description</b> must contain 0 to 255 characters.	[Example] -

**Step 5** Click **Next** and select a virtualization type.

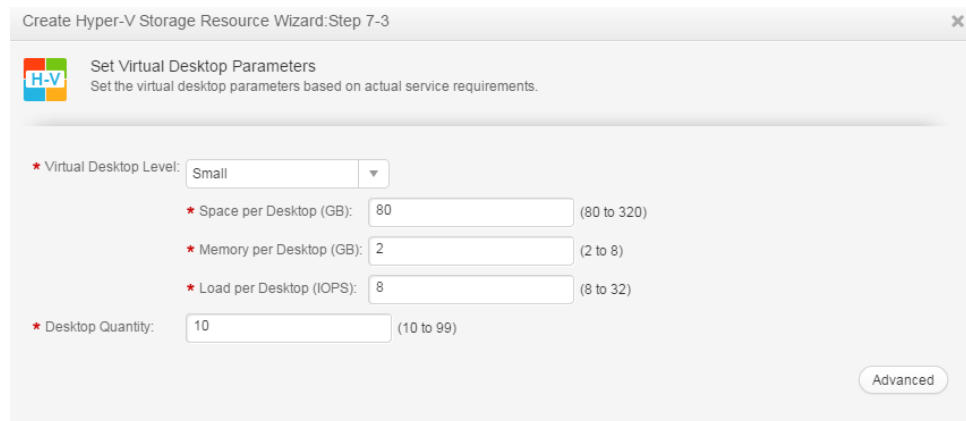
[Table 5-12](#) describes related parameters.

**Table 5-12** Parameters of a Hyper-V application

Parameter	Description	Value
Virtual desktop	Allows enterprise-level applications to dynamically access desktop systems remotely and implements central hosting of data centers.	[Example] <b>Virtual desktop</b>
Virtual server	The virtualization server technology logically divides services of a server into multiple service units, which are externally demonstrated as servers. In this way, the server hardware is fully utilized. This technology reduces consumption of manpower and material resources and simplifies work for small- and mid-size enterprises and enterprises that construct websites for the first time. Virtualization servers are a good choice for enterprises to release information.	[Example] <b>Virtual server</b>

**Step 6** Set related parameters based on the selected virtualization type.

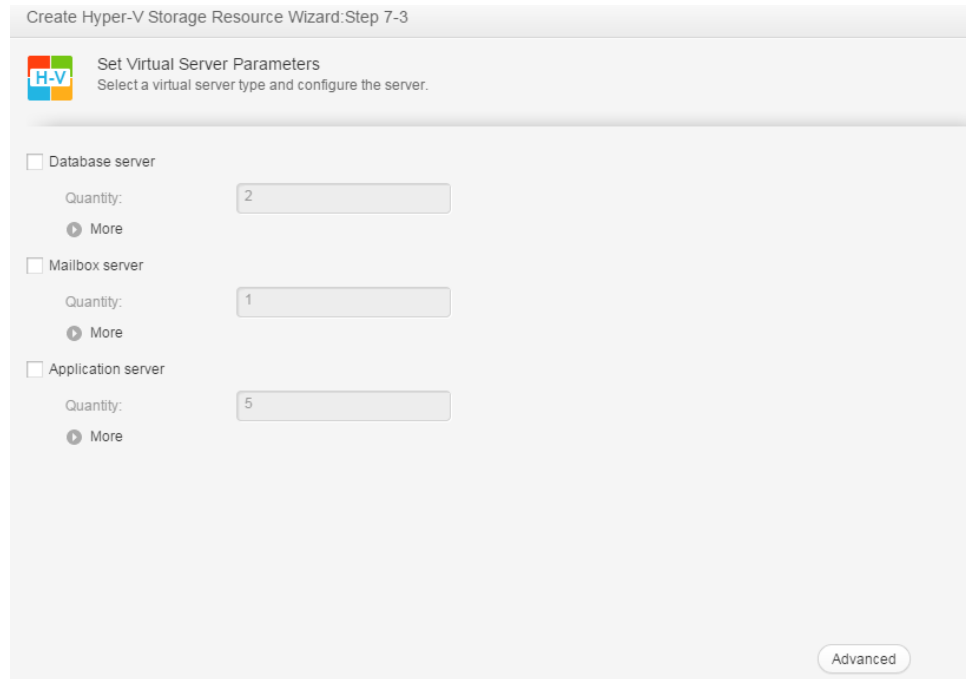
- If **Virtual desktop** is selected, set virtual desktop parameters, as shown in [Table 5-13](#).



**Table 5-13** Virtual desktop parameters

Parameter	Description	Value
Virtual Desktop Level	Level of the virtual desktop constructed by Hyper-V. The value of this parameter affects the values of <b>Space per Desktop (GB)</b> , <b>Memory per Desktop (GB)</b> , and <b>Load per Desktop (IOPS)</b> .	[Value range] The value can be <b>Small</b> , <b>Medium</b> , <b>Large</b> and <b>Extra-Large</b> . [Example] <b>Small</b>
Space per Desktop (GB)	Maximum storage space allocated by Hyper-V to each virtual desktop. The value of this parameter is subject to <b>Virtual Desktop Level</b> and is user-definable.	[Example] <b>80</b>
Memory per Desktop (GB)	Maximum memory capacity allocated by Hyper-V to each virtual desktop. The value of this parameter is subject to <b>Virtual Desktop Level</b> and is user-definable.	[Example] <b>2</b>
Load per Desktop (IOPS)	Maximum IOPS of each virtual desktop. The value of this parameter is subject to <b>Virtual Desktop Level</b> and is user-definable.	[Example] <b>8</b>
Desktop Quantity	Number of virtual desktops constructed by Hyper-V.	[Example] <b>10</b>

- If **Virtual server** is selected, set virtual server parameters, as shown in [Table 5-14](#).



**Table 5-14** Virtual server parameters

Parameter	Description	Value
Database server	Type of a Hyper-V virtual server.	[Example] -
Mailbox server	Type of a Hyper-V virtual server.	[Example] -
Application server	Type of a Hyper-V virtual server.	[Example] -
Quantity	Number of virtual servers constructed by Hyper-V.	[Example] <b>2</b>
Virtual Server Level	Level of the virtual server constructed by Hyper-V. The value of this parameter affects the values of <b>Average Load (IOPS)</b> and <b>Average Capacity (GB)</b> .	[Value range] The value can be <b>Extra-Small, Small, Medium, Large</b> and <b>Extra-Large</b> . [Example] <b>Medium</b>
Average Load (IOPS)	IOPS of a virtual server. The value of this parameter is subject to <b>Virtual Server Level</b> and is user-definable.	[Example] <b>25</b>

Parameter	Description	Value
Average Capacity (GB)	Storage capacity allocated to virtual servers. The value of this parameter is subject to <b>Virtual Server Level</b> and is user-definable.	[Example] <b>25</b>

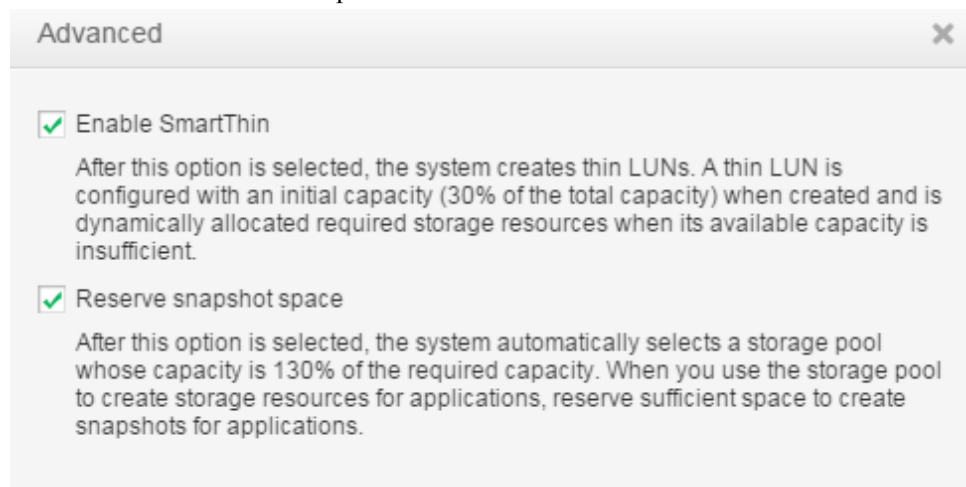
**Step 7 Optional:** Set advanced properties of Hyper-V applications.

1. Click **Advanced**.

The **Advanced** dialog box is displayed.

2. Set advanced properties of Hyper-V applications.

**Table 5-15** describes related parameters.



**Table 5-15** Parameters in advanced properties of a Hyper-V application

Parameter	Description	Value
Enable SmartThin	After this function is enabled, the system will create thin LUNs. After being created, a thin LUN is only assigned initial capacity (30% of the total capacity). If the available capacity is insufficient, the system dynamically assigns storage resources in storage pools to the thin LUN based on the actual required capacity.	[Example] <b>Enable SmartThin</b>

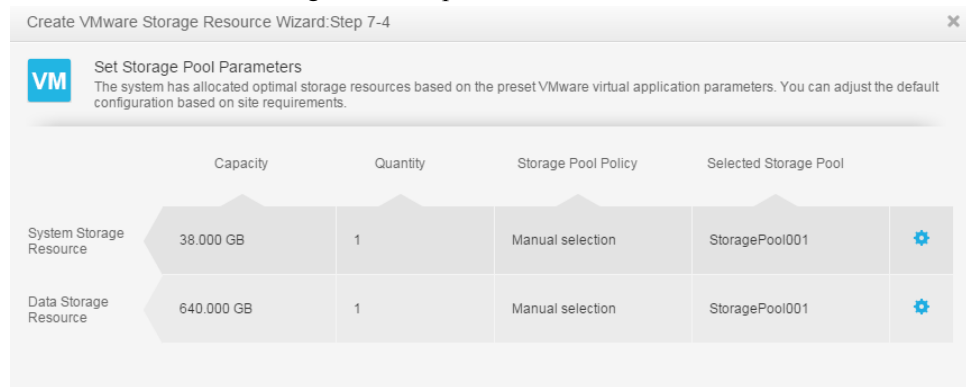
Parameter	Description	Value
Reserve snapshot space	After this function is enabled, the system automatically selects storage pools whose capacities are 130% of the actual required capacity. When using storage pools to create instances for applications, remember to reserve sufficient space for snapshots.	[Example] -

3. Click **OK**.

You are returned to the **Set Virtual Desktop Parameters** or **Set Virtual Server Parameters** page.

**Step 8** Click **Next** and set parameters for Hyper-V storage resources. The system will allocate optimal storage resources based on preset Hyper-V parameters.

**Table 5-16** describes storage resource parameters.




**Table 5-16** Hyper-V storage resource parameters

Parameter	Description	Value
LUN Capacity	LUN storage space allocated to system storage resources or data storage resources.	[Example] <b>640.000GB</b>
LUN Quantity	Number of allocated LUNs.	[Example] <b>1</b>



Parameter	Description	Value
Storage Pool Policy	<p>The system sets storage pool allocation policies based on preset Hyper-V application parameters. The performance level of each VM is defined by <b>High performance</b>, <b>Performance/Cost balance</b>, <b>Low cost</b>, or <b>Manual selection</b>, described as follows:</p> <ul style="list-style-type: none"> <li>● <b>High performance:</b> The system automatically selects a RAID 6 storage pool containing SAS disks only. If such a storage pool does not exist in the system, create one.</li> <li>● <b>Performance/Cost balance:</b> The system automatically selects a RAID 6 storage pool containing SAS and NL-SAS disks only. If such a storage pool does not exist in the system, create one.</li> <li>● <b>Low cost:</b> The system automatically selects a RAID 6 storage pool containing NL-SAS disks only. If such a storage pool does not exist in the system, create one.</li> <li>● <b>Manual selection:</b> Users define storage pools that meet the Hyper-V service requirements.</li> </ul>	[Example] <b>Manual selection</b>
Selected Storage Pool	Storage pool automatically allocated by the system to a Hyper-V instance.	[Example] <b>StoragePool001</b>

**Step 9 Optional:** If no desired storage pools are available, click  and modify **Storage Pool Policy** in the dialog box that is displayed, or click **Create Storage Pool** to create one. [Table 5-16](#) describes related parameters.


**Step 10 Optional:** Select a host to which you want to map the instance.

 **NOTE**

If a host is selected, the system automatically creates a host group for the host and adds the host group to a mapping view. If no host is selected, manually create a host group and add the host group to a mapping view when you add a mapping host, so that the mapping host can access storage resources.

1. Click **Next**.

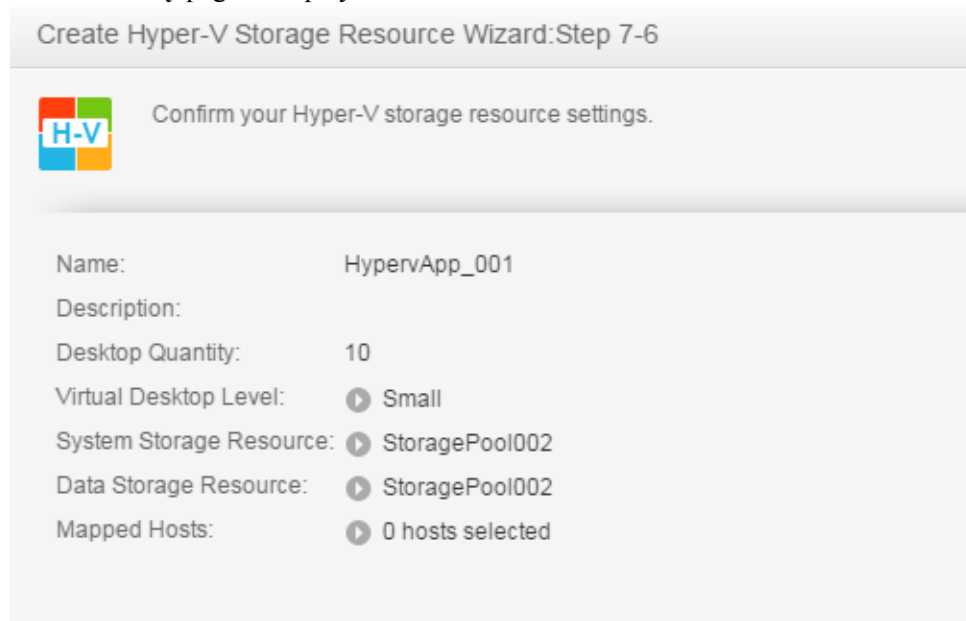
The **Select Mapping Hosts** page is displayed.

2. In the **Available Hosts** list, select the host that is used to access storage resources.
3. Click  to add the host to **Selected Hosts**.

**Step 11** Confirm your settings.

1. Click **Next**.

The **Summary** page is displayed.



2. Verify that the information about the Hyper-V instance to be created is correct and click **Finish**.

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

 **NOTE**

- If a mapped host is selected, the system automatically creates a LUN group, a host group, and a mapping view, and adds the LUN group and host group to the mapping view.
- If no mapped host is selected, the system automatically creates a LUN group only. You need to manually create a host group and a mapping view for a mapped host and add the host to the mapping view. After being added to the mapping view, the host can access storage resources.
- The LUN group must contain all LUNs in the application instance.

3. Click **Close**. You have finished creating a Hyper-V instance.

----End

## Follow-up Procedure

After successfully creating the application instance, scan for disks on the application server. For details, see the section **Making Storage Space Available** operation.

## 5.4 Configuring Oracle

This section describes Oracle and the steps to configure storage resources for it.

## 5.4.1 About Oracle

Oracle database is a distributed database product developed by ORACLE. This product is one of the most popular Client/Server (C/S) and Browser/Server (B/S) databases.

Oracle database features:

- Rich data management functions
- Comprehensive relational algebra
- Distributed processing capability
- Easy data warehouse operation

## 5.4.2 Creating an Oracle Instance




This operation allows you to create an Oracle instance.

### Prerequisites

The system has sufficient storage space.

### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Application** >  **Oracle**.

**Step 3** Click **Create**.

The **Create Oracle Storage Resource Wizard** is displayed.

**Step 4** Set basic information about the Oracle instance to be created.

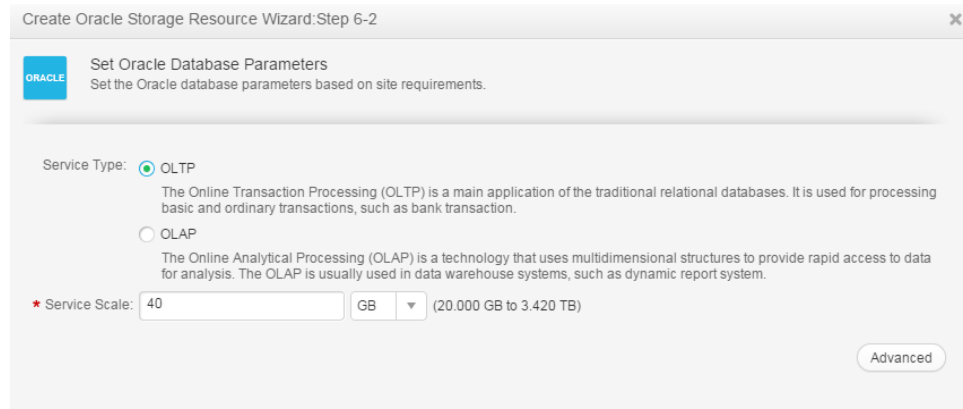
[Table 5-17](#) describes related parameters.

**Table 5-17** Parameters of an Oracle instance

Parameter	Description	Value
Name	Name of an Oracle instance. The name must meet the following requirements so that the instance is available to host applications: <ul style="list-style-type: none"> <li>● Must be unique.</li> <li>● Contains only letters, digits, underscores (_), periods (.), and hyphens (-).</li> <li>● Contains 1 to 22 characters.</li> </ul>	[Example] <b>Oracle_App_001</b>
Description	Description of an Oracle instance. <b>Description</b> must contains 0 to 255 characters.	[Example] -

**Step 5** Click **Next** and set the Oracle application parameters.

**Table 5-18** describes related parameters.

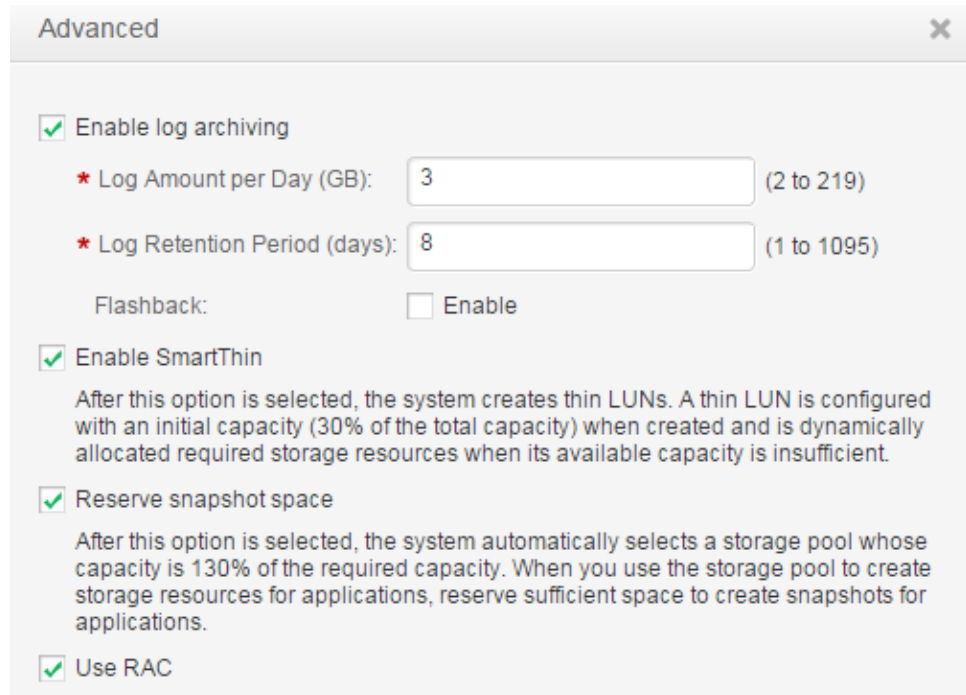


**Table 5-18** Oracle application parameters

Parameter	Description	Value
Service Type	Type of an Oracle application. The possible values are described as follows: <ul style="list-style-type: none"> <li>● Online transaction processing (OLTP): The OLTP is a main application of traditional relational databases. It is used for processing basic and ordinary transactions, such as bank transaction.</li> <li>● Online analytical processing (OLAP): A technology that uses multidimensional structures to provide rapid accesses to data for analysis. This application mainly applies to data warehouse systems, such as dynamic reporting system.</li> </ul>	[Example] <b>OLTP</b>
Service Scale	Storage space required by Oracle services.	[Example] <b>40 GB</b>

**Step 6 Optional:** Set advanced properties for an Oracle application.

1. Click **Advanced**.  
The **Advanced** dialog box is displayed.
2. Set advanced properties for an Oracle application.  
**Table 5-19** describes related parameters.



**Table 5-19** Parameters in advanced properties of an Oracle application

Parameter	Description	Value
Enable log archiving	If this function is enabled, the system will allocate storage resources to Oracle applications to archive data and logs. If this function is disabled, the system will not allocate storage resources for achieving.	[Example] -
Log Amount per Day (GB)	Maximum storage space used to store logs per day. This parameter is available after <b>Enable log archiving</b> is selected.	[Example] <b>3</b>
Log Retention Period (days)	Retention period of system logs. After this period expires, logs are not stored. This parameter is available after <b>Enable log archiving</b> is selected.	[Example] <b>8</b>

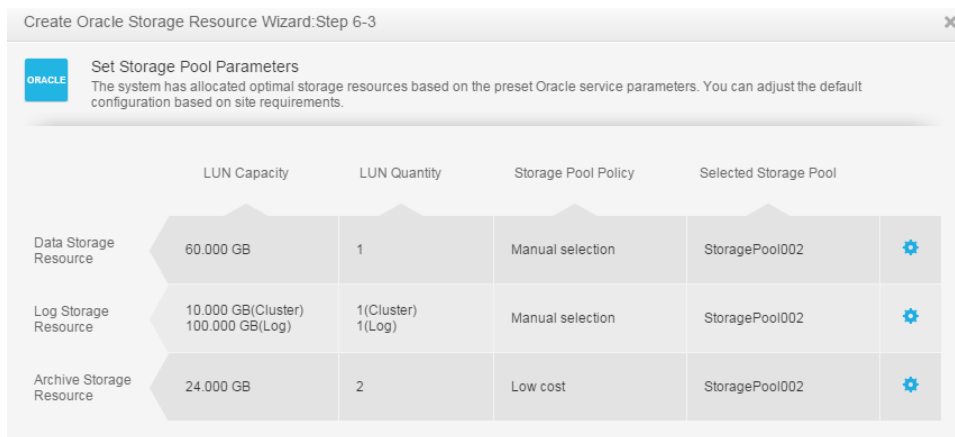
Parameter	Description	Value
Enable SmartThin	After this function is enabled, the system will create thin LUNs. After being created, a thin LUN is only assigned initial capacity (30% of the total capacity). If the available capacity is insufficient, the system dynamically assigns storage resources in storage pools to the thin LUN based on the actual required capacity.	[Example] <b>Enable SmartThin</b>
Reserve snapshot space	After this function is enabled, the system automatically selects storage pools whose capacities are 130% of the actual required capacity. When using storage pools to create storage resources for applications, remember to reserve sufficient space for snapshots.	[Example] -
Flashback	After this function is enabled, the Oracle supports flashback deletion, which means a cancel button is added for a table and its related objects. After this function is enabled, the system will enable the log archiving function accordingly.	[Example] -
Use RAC	After this function is enabled, Oracle provides cluster software and storage management software, reducing application costs. If the scale of applications needs to be expanded, users can expand the system on demand to ensure system performance. If this function is disabled, the system will not allocate LUNs to store cluster logs.	[Example] -

3. Click **OK**.

You are returned to the **Set Oracle Database Parameters** page.

**Step 7** Click **Next** and set parameters for Oracle storage resources. The system will allocate optimal storage resources based on preset Oracle parameters.


**Table 5-20** describes storage resource parameters.



**Table 5-20** Oracle storage resource parameters

Parameter	Description	Value
LUN Capacity	LUN storage space allocated to store data, logs, or archives.	[Example] <b>60 GB</b>
LUN Quantity	Number of LUNs allocated to store data, logs, or archives.	[Example] <b>1</b>

Parameter	Description	Value
Storage Pool Policy	<p>The system sets storage pool allocation policies based on preset Oracle parameters. The value can be <b>High performance</b>, <b>Performance/Cost balance</b>, <b>Low cost</b>, or <b>Manual selection</b>. The four values are described as follows:</p> <ul style="list-style-type: none"> <li>● <b>High performance</b>: The system automatically selects a RAID 6 storage pool containing SAS disks only. If such a storage pool does not exist in the system, create one.</li> <li>● <b>Performance/Cost balance</b>: The system automatically selects a RAID 6 storage pool containing SAS and NL-SAS disks only. If such a storage pool does not exist in the system, create one.</li> <li>● <b>Low cost</b>: The system automatically selects a RAID 6 storage pool containing NL-SAS disks only. If such a storage pool does not exist in the system, create one.</li> <li>● <b>Manual selection</b>: Users define storage pools that meet the Oracle service requirements.</li> </ul>	[Example] Manual selection
Selected Storage Pool	Name of the storage pool automatically allocated by the system to an Oracle instance.	[Example] <b>StoragePool001</b>

**Step 8 Optional:** If no desired storage pools are available, click  and modify **Storage Pool Policy** in the dialog box that is displayed, or click **Create Storage Pool** to create one. [Table 5-20](#) describes related parameters.


**Step 9 Optional:** Select a host to which you want to map the instance.

 **NOTE**

If a host is selected, the system automatically creates a host group for the host and adds the host group to a mapping view. If no host is selected, manually create a host group and add the host group to a mapping view when you add a mapping host, so that the mapping host can access storage resources.

1. Click **Next**.  
The **Select Mapping Hosts** page is displayed.
2. In the **Available Hosts** list, select the host that is used to access storage resources.



3. Click  to add the host to **Selected Hosts**.

**Step 10** Confirm your settings.

1. Click **Next**.

The **Summary** page is displayed.



2. Verify that the information about the Oracle instance to be created is correct and click **Finish**.

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

 **NOTE**

- If a mapped host is selected, the system automatically creates a LUN group, a host group, and a mapping view, and adds the LUN group and host group to the mapping view.
  - If no mapped host is selected, the system automatically creates a LUN group only. You need to manually create a host group and a mapping view for a mapped host and add the host to the mapping view. After being added to the mapping view, the host can access storage resources.
  - The LUN group must contain all LUNs in the application instance.
3. Click **Close**. You have finished creating an Oracle instance.

----End

## Follow-up Procedure

After successfully creating the application instance, scan for disks on the application server. For details, see the section **Making Storage Space Available** operation.

## 5.5 Configuring SQL Server

This section describes SQL Server and the steps to configure storage resources for it.

### 5.5.1 About SQL Server

SQL Server is a relational database product developed by Microsoft.

SQL Server functions as a database platform for large-scale transaction processing, database warehouses, and electronic commerce applications. Besides, SQL Server is an intelligent business platform for data integration, data analysis, and report solutions.

Mainstream SQL Server versions are as follows:

- Microsoft SQL Server 2000
- Microsoft SQL Server 2005
- Microsoft SQL Server 2008
- Microsoft SQL Server 2012

The storage system supports SQL Server 2008 and SQL Server 2012.

## 5.5.2 Creating an SQL Server Instance

This operation allows you to create an SQL Server instance.

### Prerequisites

The system has sufficient storage space.

### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Application** >  **SQL Server**.

**Step 3** Click **Create**.

The **Create SQL Server Storage Resource Wizard** is displayed.

**Step 4** Set basic information about the SQL Server instance to be created.

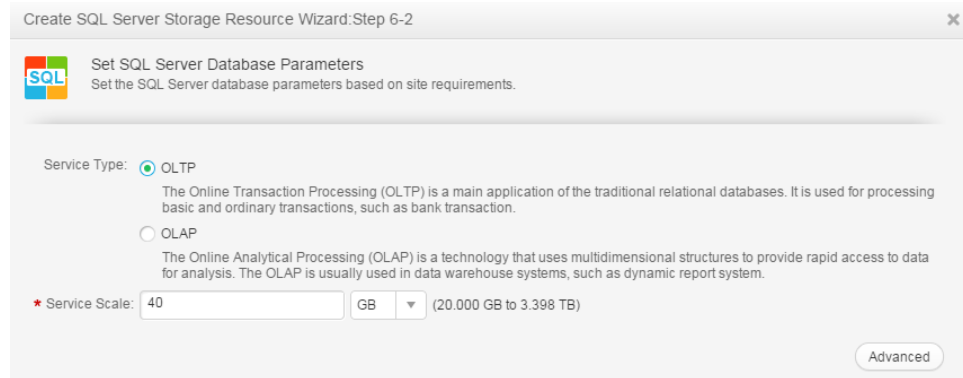
[Table 5-21](#) describes related parameters.

**Table 5-21** Parameters of an SQL Server instance

Parameter	Description	Value
Name	Name of an SQL Server instance. The name must meet the following requirements so that the instance is available to host applications: <ul style="list-style-type: none"> <li>● Must be unique.</li> <li>● Contains only letters, digits, underscores (_), periods (.), and hyphens (-).</li> <li>● Contains 1 to 22 characters.</li> </ul>	[Example] <b>SQLServer_App_001</b>
Description	Description of an SQL Server instance. <b>Description</b> must contain 0 to 255 characters.	[Example] -

**Step 5** Click **Next** and set the SQL Server application parameters.

**Table 5-22** describes related parameters.

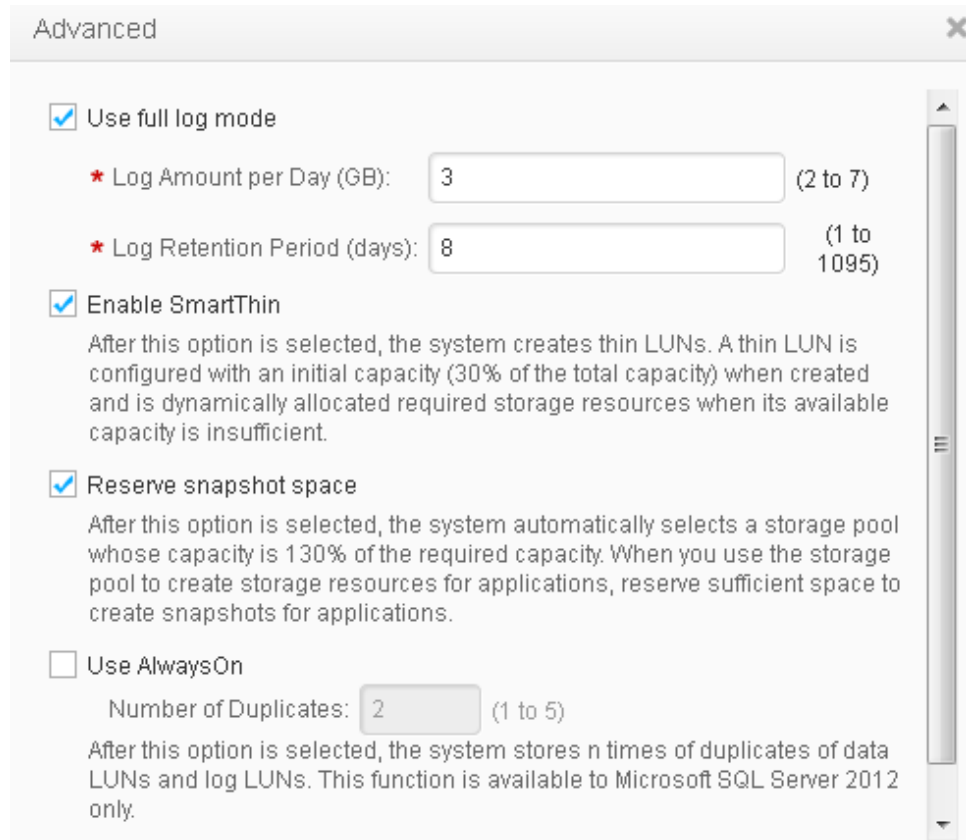


**Table 5-22** SQL Server application parameters

Parameter	Description	Value
Service Type	Type of an SQL Server application. The possible values are described as follows: <ul style="list-style-type: none"> <li>● <b>OLTP</b>: The OLTP is a main application of traditional relational databases. It is used for processing basic and ordinary transactions, such as bank transaction.</li> <li>● <b>OLAP</b>: A technology that uses multidimensional structures to provide rapid accesses to data for analysis. This application mainly applies to data warehouse systems, such as dynamic reporting system.</li> </ul>	[Example] <b>OLTP</b>
Service Scale	Storage space required by SQL Server services.	[Example] <b>40 GB</b>

**Step 6 Optional:** Set advanced properties for SQL Server applications.

1. Click **Advanced**.  
 The **Advanced** dialog box is displayed.
2. Set advanced properties for SQL Server applications.  
**Table 5-23** describes related parameters.



**Table 5-23** Parameters in advanced properties of an SQL Server application

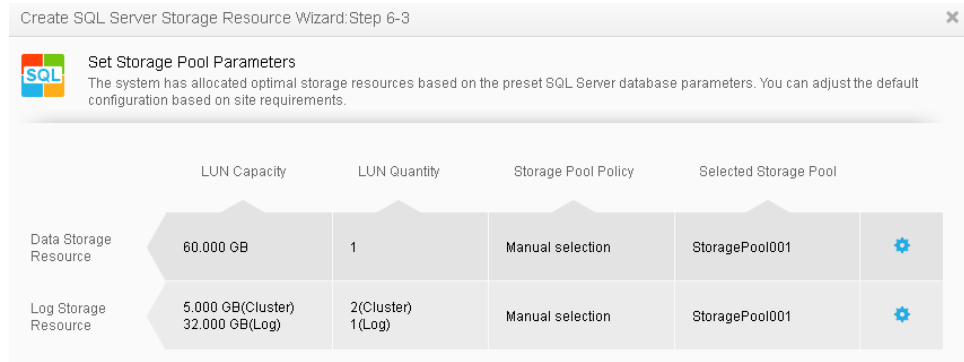
Parameter	Description	Value
Use full log mode	After this function is enabled, the system will allocate storage resources to SQL Server applications to store SQL Server database logs.	[Example] -
Log Amount per Day (GB)	Maximum storage space used to store logs per day. This parameter is available after <b>Enable log archiving</b> is selected.	[Example] <b>3</b>
Log Retention Period (days)	Retention period of system logs. After this period expires, logs are not stored. This parameter is available after <b>Enable log archiving</b> is selected.	[Example] <b>8</b>

Parameter	Description	Value
Enable SmartThin	After this function is enabled, the system will create thin LUNs. After being created, a thin LUN is only assigned initial capacity (30% of the total capacity). If the available capacity is insufficient, the system dynamically assigns storage resources in storage pools to the thin LUN based on the actual required capacity.	[Example] <b>Enable SmartThin</b>
Reserve snapshot space	After this function is enabled, the system automatically selects storage pools whose capacities are 130% of the actual required capacity. When using storage pools to create storage resources for applications, remember to reserve sufficient space for snapshots.	[Example] -
Use clusters	After this function is enabled, the system automatically allocates two 5 GB of LUNs to store cluster logs.	[Example] -
Use AlwaysOn	After this function is enabled, the system stores n duplicates of data LUNs and log LUNs. n indicates the number of duplicates. This function is available to Microsoft SQL Server 2012 only.	[Example] -
Number of Duplicates	Number of duplicates of data LUNs and log LUNs. This parameter is available after <b>Use AlwaysOn</b> is selected.	[Value range] The value ranges from 1 to 5 and the default value is 2. [Example] <b>2</b>

3. Click **OK**.

You are returned to the **Set SQL Server Database Parameters** page.


**Step 7** Click **Next** to set parameters for SQL Server storage resources. The system will allocate optimal storage resources based on preset SQL Server parameters.



**Table 5-24** SQL Server storage resource parameters

Parameter	Description	Value
LUN Capacity	LUN storage space allocated to store data or logs.	[Example] <b>60.000 GB</b>
LUN Quantity	Number of LUNs allocated to store data or logs.	[Example] <b>1</b>

Parameter	Description	Value
Storage Pool Policy	<p>The system sets storage pool allocation policies based on preset SQL Server parameters. The value can be <b>High performance</b>, <b>Performance/Cost balance</b>, <b>Low cost</b>, or <b>Manual selection</b>. The four values are described as follows:</p> <ul style="list-style-type: none"> <li>● <b>High performance</b>: The system automatically selects a RAID 6 storage pool containing SAS disks only. If such a storage pool does not exist in the system, create one.</li> <li>● <b>Performance/Cost balance</b>: The system automatically selects a RAID 6 storage pool containing SAS and NL-SAS disks only. If such a storage pool does not exist in the system, create one.</li> <li>● <b>Low cost</b>: The system automatically selects a RAID 6 storage pool containing NL-SAS disks only. If such a storage pool does not exist in the system, create one.</li> <li>● <b>Manual selection</b>: Users define storage pools that meet the SQL Server service requirements.</li> </ul>	[Example] <b>Manual selection</b>
Selected Storage Pool	Name of the storage pool automatically allocated by the system to an SQL Server instance.	[Example] <b>StoragePool001</b>

**Step 8 Optional:** If no desired storage pools are available, click  and modify **Storage Pool Policy** in the dialog box that is displayed, or click **Create Storage Pool** to create one. [Table 5-24](#) describes related parameters.


**Step 9 Optional:** Select a host to which you want to map the instance.

 **NOTE**

If a host is selected, the system automatically creates a host group for the host and adds the host group to a mapping view. If no host is selected, manually create a host group and add the host group to a mapping view when you add a mapping host, so that the mapping host can access storage resources.

1. Click **Next**.

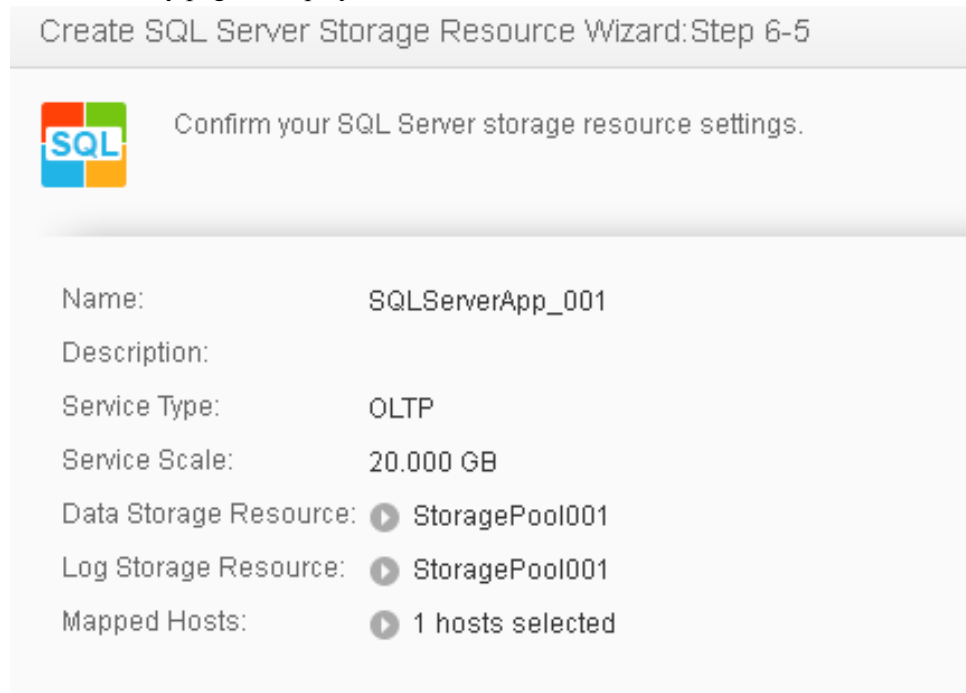
The **Select Mapping Hosts** page is displayed.

2. In the **Available Hosts** list, select the host that is used to access storage resources.
3. Click  to add the host to **Selected Hosts**.

**Step 10** Confirm your settings.

1. Click **Next**.

The **Summary** page is displayed.



2. Verify that the information about the SQL Server instance to be created is correct and click **Finish**.

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

 **NOTE**

- If a mapped host is selected, the system automatically creates a LUN group, a host group, and a mapping view, and adds the LUN group and host group to the mapping view.
- If no mapped host is selected, the system automatically creates a LUN group only. You need to manually create a host group and a mapping view for a mapped host and add the host to the mapping view. After being added to the mapping view, the host can access storage resources.

The LUN group must contain all LUNs in the application instance.

3. Click **Close**. You have finished creating an SQL Server instance.

---End

## Follow-up Procedure

After successfully creating the application instance, scan for disks on the application server. For details, see the section **Making Storage Space Available** operation.



# 6 Managing Basic Storage Services

---

## About This Chapter

This chapter describes how to manage basic storage services through DeviceManager, to meet your service requirements.

### [6.1 Managing Access Permission of a Storage System](#)

To ensure device and service data security, the storage systems support security policy adjustment, IP address access control, and user management.

### [6.2 Managing iSCSI Host Ports](#)

This function allows you to manage and monitor the iSCSI host ports.

### [6.3 Managing Fibre Channel Host Ports](#)

This function allows you to manage and monitor the Fibre Channel host ports.

### [6.4 Managing Disk Domains](#)

This chapter describes the operations for managing disk domain, including viewing disk domain information, modifying the properties of disk domain, expanding disk domain and more.

### [6.5 Managing Storage Pools](#)

This function enables you to consolidate the storage resources provided by different types of hard disks into storage pools as well as centrally manage the storage resources.

### [6.6 Managing LUNs](#)

LUNs are provided by a storage system to enable the application servers to make full use of the storage resources.

### [6.7 Managing LUN Groups](#)

For easy management of multiple LUNs, logically add the LUNs to a LUN group.

### [6.8 Managing Hosts](#)

This function allows you to manage hosts so that the hosts can obtain and use the storage resources allocated by the storage system.

### [6.9 Managing Host Groups](#)

To centrally manage multiple hosts, you can aggregate hosts into a host group.

### [6.10 Managing a Port Group](#)

This section describes how to manage a port group, including viewing information about the port group and the mapping view where the port group resides.

### 6.11 Managing Mapping Views

This function allows you to flexibly allocate storage resources to hosts using mapping views.

## 6.1 Managing Access Permission of a Storage System

To ensure device and service data security, the storage systems support security policy adjustment, IP address access control, and user management.

### 6.1.1 Configuring a Security Policy for System User




You can set the username and password policies to control the username and password complexity of new accounts. The login policy enables the system to lock the accounts with security exceptions.

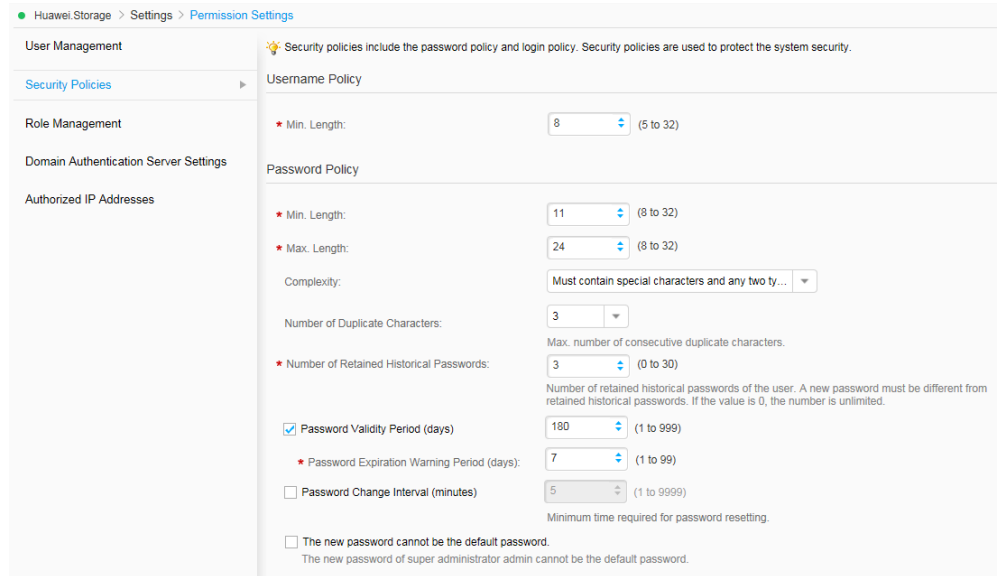
#### Context

The storage system supports the following password policies to ensure account security.

- The storage system supports strong password complexity to prevent brute-force password cracking.
- Passwords must be encrypted before they are stored and transferred.
- Passwords can be changed only after authentication and users can only change their own passwords.

#### Procedure

1. Log in to DeviceManager.
2. Choose  **Settings** >  **Permission Settings** > **Security Policies**.
  - a. On the right navigation bar, click  **Settings**.
  - b. In the **Basic Service Settings** area on the function pane, click  **Permission Settings**.  
The **Security Policies** page is displayed.
  - c. In the left navigation tree, select **Security Policies**.  
The **Security Policies** page is displayed.



3. [Table 6-1](#), [Table 6-2](#), [Table 6-3](#), and [Table 6-4](#) describe the parameters related to configuration of user name, password, login, and account audit policies.

**Table 6-1** User name policy

Parameter	Description	Value
Minimal length	Minimum length of a user name. The user name cannot be too simple.	[Value range] The value is an integer ranging from 5 to 32. [Example] 6

**Table 6-2** 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 <b>0</b> , there is no restriction.	[Value range] The value is an integer ranging from 0 to 30. [Example] 3
Password Validity Period (days)	Setting of a password's validity period. After <b>Password Validity Period</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 super administrator admin cannot be the default password.	[Value range] The value is an integer ranging from 1 to 9999. [Example] 5

**Table 6-3** 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] <b>Enable</b> or <b>Disable</b> [Example] <b>Enable</b>

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]</p> <p>The value is an integer ranging from 1 to 9.</p> <p>[Example]</p> <p>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]</p> <p><b>Temporary</b> or <b>Permanent</b></p> <p>[Example]</p> <p><b>Temporary</b></p>
Automatic Unlock in (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]</p> <p>The value is an integer ranging from 3 to 2000.</p> <p>[Example]</p> <p>15</p>
Lock Account When Idle	<p>A system account will be locked if it is not used for login and the idle period exceeds the specified days.</p>	<p>[Value range]</p> <p><b>Enable</b> or <b>Disable</b></p> <p>[Example]</p> <p><b>Enable</b></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] <b>Enable</b> or <b>Disable</b> [Example] <b>Enable</b>
User-Defined Info	After an account's successful login, an alarm is displayed indicating the preset information.	[Value range] <b>Enable</b> or <b>Disable</b> [Example] <b>Enable</b>
Info	The information to prompt the successful login of user account.	[Value range] The information contains 1 to 511 characters. [Example] Login successful

**Table 6-4** Account audit policies

Parameter	Description	Value
User Account Audit	Periodically audits the number and permission of user accounts to ensure account security.	[Value range] <b>Enable</b> or <b>Disable</b> [Example] <b>Enable</b>
Audit Period (Days)	Periodically audits period of the account.	[Value range] The value is an integer ranging from 0 to 999. [Default] 120

4. Confirm the security policy configuration.
  - a. Click **Save**.  
The **Execution Results** dialog box is displayed, indicating that the security policy configuration succeeds.
  - b. Click **Close**.

## 6.1.2 Configuring Authorized IP Addresses

You can specify the IP addresses that can access the device from DeviceManager to prevent unauthorized access.

### Prerequisites

You are a super administrator. (Only super administrators have the permission to perform this operation.)

### Procedure

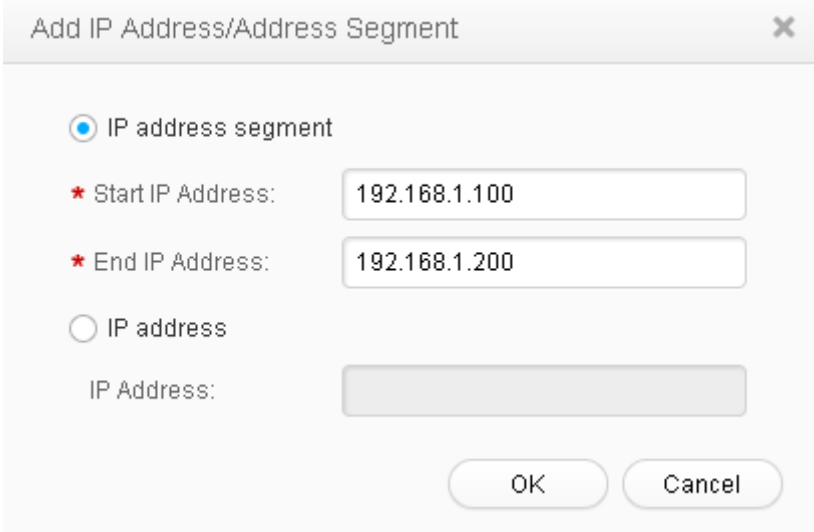
**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Settings** >  **Permission Settings** > **Authorized IP Addresses**.

**Step 3** Authorize IP addresses.

1. Select **Enable**.
2. Click **Add**.

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



3. Enter the IP segment or IP address that can access the storage device.
  - To authorize an IP address segment, select **IP address segment** and set **Start IP Address** and **End IP Address**. IP addresses included in the IP address segment are allowed to access the storage device.
  - To authorize IP addresses, select **IP address** and set **IP Address**.
4. Click **OK**. The specified IP segment or IP address is added to the IP address segment/IP address list.

#### **NOTE**

After this function is enabled, if you want to prevent one IP address or IP address segment from accessing devices, select the IP address or IP address segment from the IP address/IP address segment list and click **Remove**. Note that at least one IP address or IP address segment must be allowed access.

5. Click **Save**, read and confirm the prompt information.



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

**Step 4** Click **Close**.

----End

## 6.1.3 Managing Users and Their Access Permissions

To prevent misoperations from affecting device stability and service data security, the storage device defines three user levels, each with certain permission.

### 6.1.3.1 Creating a Local User

To ensure device stability and service data security, a super administrator can create different levels of users based on service requirements.

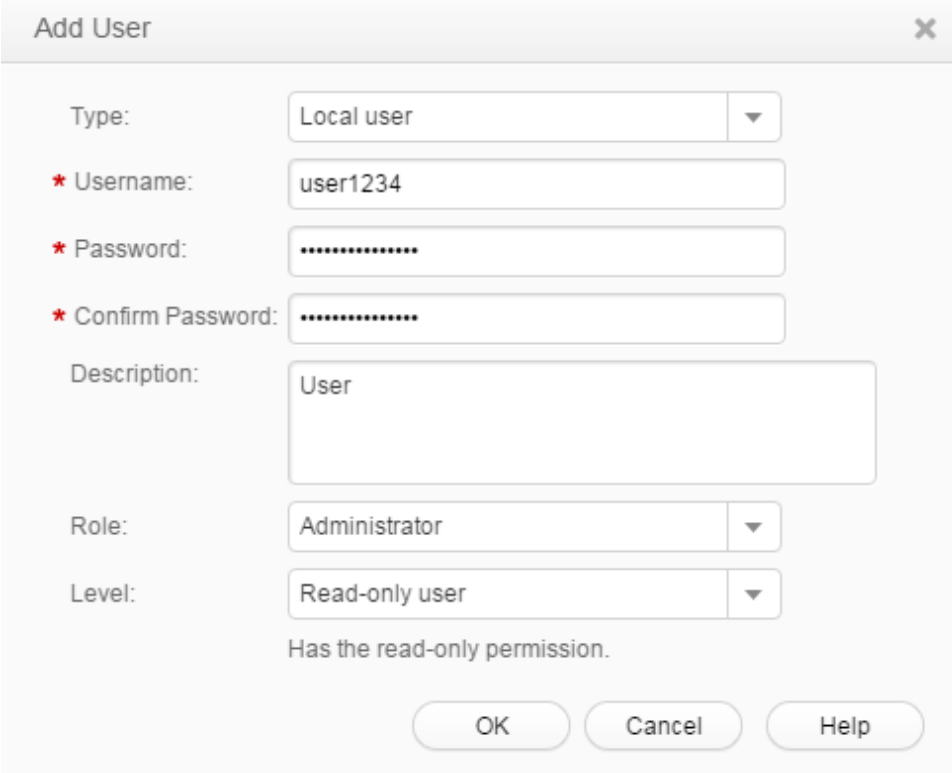
#### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Settings** >  **Permission Settings** > **User Management**.

**Step 3** In the right function pane, click **Add**.  
The **Add User** dialog box is displayed.

**Step 4** Set user information. Select **Local user** in **Type** and configure relevant parameters.



The screenshot shows the 'Add User' dialog box with the following configuration:

- Type: Local user
- \* Username: user1234
- \* Password: [masked]
- \* Confirm Password: [masked]
- Description: User
- Role: Administrator
- Level: Read-only user

Has the read-only permission.

Buttons: OK, Cancel, Help

**Table 6-5** describes the local user parameters.

**Table 6-5** Local user parameters

Parameter	Description	Value
Username	Name of a newly created user.	<p>[Value range]</p> <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> <p><b>NOTE</b> You can modify the username policy in <b>Permission Settings &gt; Security Policies</b>.</p> <p>[Example] user1234</p>
Password	Password of a newly created user.	<p>[Value range]</p> <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] a#123456</p>

Parameter	Description	Value
Confirm password	Password for confirmation.	[Value range] The value must be the same as that of <b>Password</b> . [Example] a#123456
Description	Description of a newly created user.	[Example] User
Role	Set permissions for users. You can select a built-in role or create a self-defined role.	[Example] Administrator
Level	Level of a user. Possible values are as follows: <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

### 6.1.3.2 Creating a Domain User

DeviceManager allows users to log in to the storage system using the Lightweight Directory Access Protocol (LDAP) server authentication mode to centrally manage user information.

## Prerequisites

Configure a domain authentication server before creating an LDAP user or LDAP user group. For details, see **Configuring Domain Authentication for a Storage System** in the *Installation Guide* of the corresponding product model.

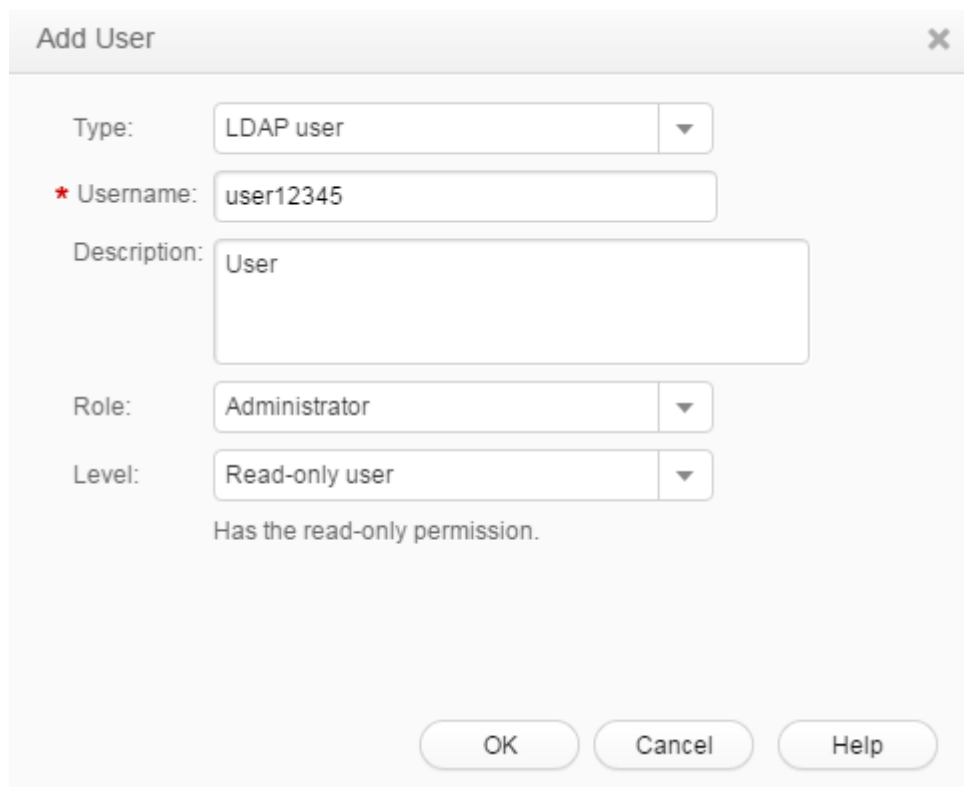
## Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Settings** >  **Permission Settings** > **User Management**.

**Step 3** In the right function pane, click **Add**.  
The **Add User** dialog box is displayed.

**Step 4** Set user information. Select **LDAP user** or **LDAP user group** in **Type** and configure the relevant parameters. [Table 6-6](#) describes these parameters.



**Add User** [Close]

Type: LDAP user

\* Username: user12345

Description: User

Role: Administrator

Level: Read-only user

Has the read-only permission.

OK Cancel Help

**Table 6-6** 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] <ul style="list-style-type: none"> <li>● The username contains 1 to 64 characters.</li> <li>● The username must be unique.</li> </ul> [Example] user12
Description	Description of a newly created user.	[Example] User
Role	Set permissions for users. You can select a built-in role or create a self-defined role.	[Example] Administrator
Level	Level of a newly created LDAP user or LDAP user group. Possible values are as follows: <ul style="list-style-type: none"> <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

### 6.1.3.3 Managing User Levels

A super administrator can change the level of a read-only user or an administrator according to the actual requirements.

#### Prerequisites

- Only super administrators have the right to perform this operation.
- The super administrator can modify the level and initiate the password only for users whose **Status** is **Offline**.

## Context

User levels include:

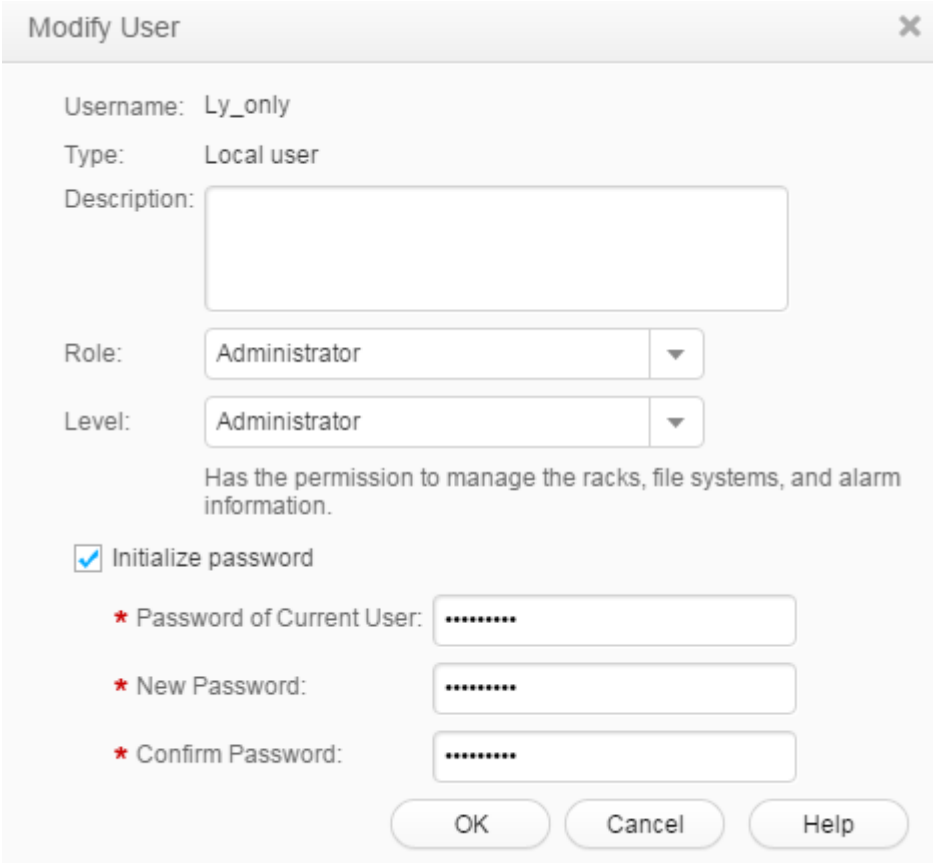
- **Administrator:** has permission to control the storage device and modify password of administrator, but cannot manage users, upgrade the storage device, modify system time, activate license files, restart device, or power off device. Local user administrator cannot import license files, and LDAP user administrator cannot perform any import or export operation.
- **Read-only user:** has permission to access the storage device and change its password. After logging in to the storage device, the read-only user can only query device information but cannot perform other operations.

## Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Settings** >  **Permission Settings** > **User Management**.

**Step 3** In the middle function pane, select a user that you want to modify and click **Modify**. The **Modify User** dialog box is displayed.



**Modify User** [Close]

Username: Ly\_only

Type: Local user

Description:

Role: Administrator [v]

Level: Administrator [v]

Has the permission to manage the racks, file systems, and alarm information.

Initialize password

\* Password of Current User:

\* New Password:

\* Confirm Password:

OK Cancel Help

**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

### 6.1.3.4 Customizing User Roles

User roles control the scopes of permission for users. A super administrator can change the role of a read-only user or an administrator to adjust the user's scope of permission according to the actual requirements. After a role is assigned to a user, the user has the permission to access or operate the objects specified by the role.

#### Prerequisites

The super administrator can modify the level and role and initiate the password only for users whose **Status** is **Offline**.

#### Context

The storage system provides typical default roles. If the default roles cannot meet your requirements, you can create roles.

#### Procedure

**Step 1** Log in to DeviceManager.

**Step 2 Optional:** Choose  **Settings** >  **Permission Settings** > **Role Management** and manage user-defined roles. [Table 6-7](#) 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 6-7** 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 6-8</a> describes the parameters.</li><li>3. On the <b>Execution Result</b> page, click <b>Close</b>.</li></ol>

Operation	Procedure
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. <b>Table 6-8</b> 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>. The <b>Success</b> dialog box is displayed.</li> <li>2. Click <b>OK</b>.</li> </ol>

**Table 6-8** User-defined role parameters

Parameter	Description
Name	Name of a role.
Owning group	<p>The value can be <b>System Group</b> or <b>vStore Group</b>.</p> <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 <b>B Permission Matrix for Self-defined Roles</b> .
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.



Modify User

Username: Ly\_only  
Type: Local user  
Description:   
Role: Administrator  
Level: Administrator  
Has the permission to manage the racks, file systems, and alarm information.  
 Initialize password  
\* Password of Current User:   
\* New Password:   
\* Confirm Password:   
OK Cancel Help

3. Select a desired role from the **Role** drop-down list.

**NOTE**

You can select a built-in or user-defined role based on your actual requirements.

**Step 4** Confirm the user modification.

1. Click **OK**.  
The security alert dialog box is displayed. Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation**.
2. Click **OK**.  
The **Execution Result** dialog box is displayed, indicating that the operation is successful.
3. Click **Close**.

----End

### 6.1.3.5 Locking or Unlocking a User

A super administrator can prevent a user from logging in to the storage device by locking the user. Locked users online at the time they are locked can continue using DeviceManager but will not be able to log in again after they log out.

#### Prerequisites

- Only super administrators have the permission to perform this operation.

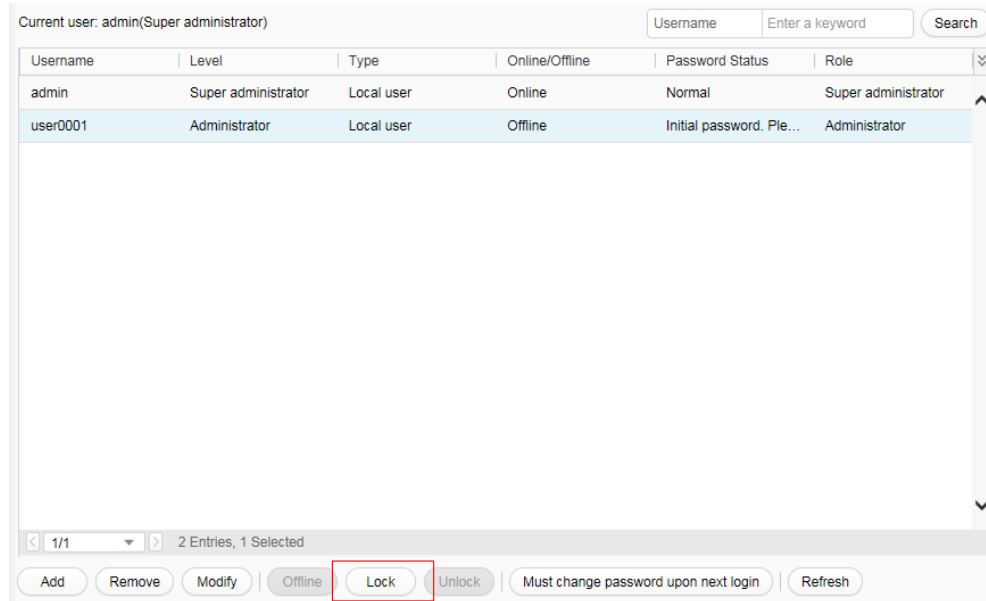
- **Lock Status** of the user to be locked is **Unlock**.

## Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Settings** >  **Permission Settings** > **User Management**.

**Step 3** In the middle function pane, choose a user that you want to lock and click **Lock**.



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

### **NOTE**



You can also right-click the user that you want to lock and choose **Lock**.

**Step 4** Click **OK**.

----End

## Follow-up Procedure

A super administrator can allow the user to log in to the storage device by unlocking the user.

1. Log in to DeviceManager.
2. Choose  **Settings** >  **Permission Settings** > **User Management**.
3. In the middle function pane, choose a user that you want to unlock and click **Unlock**.

### **NOTE**

You can also right-click the user that you want to unlock and choose **Unlock**.

The **Permission Authentication** dialog box is displayed.

4. Enter the password of the login user, and click **OK**.  
The **Success** dialog box is displayed indicating that the operation succeeded.
5. Click **OK**.

### 6.1.3.6 Logging Out a User

A super administrator can prevent a logged-in user from using the storage device by forcibly logging the user out of DeviceManager.

#### Prerequisites

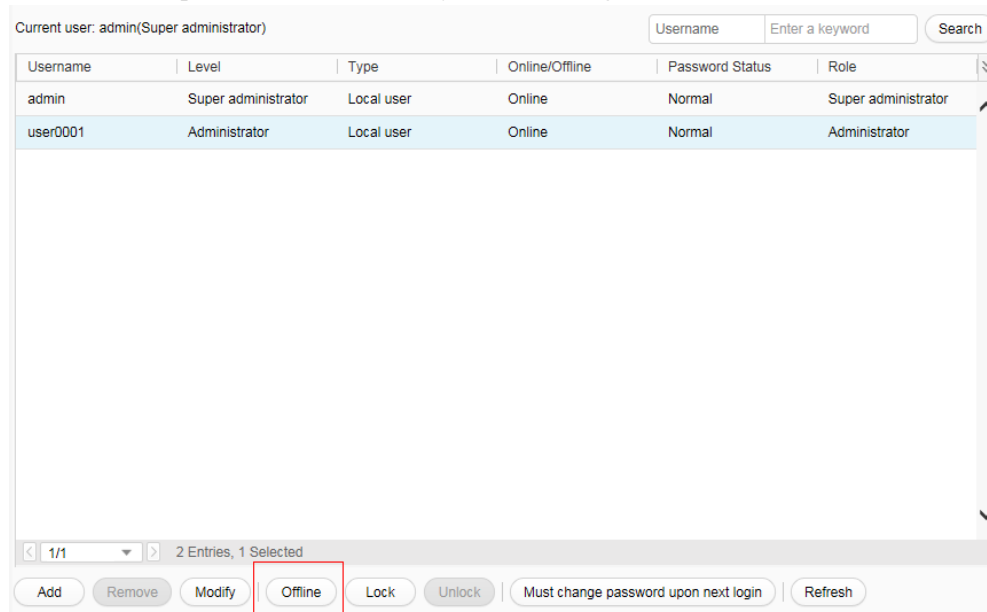
- Only a super administrator has the permission to perform this operation.
- Users whose **Status** is **Online** can be logged out.

#### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Settings** >  **Permission Settings** > **User Management**.

**Step 3** In the function pane, select a user that you want to log out and click **Offline**.



The security alert dialog box is displayed.

#### **NOTE**

You can also right-click the user, and choose **Offline**.

**Step 4** Confirm the logout of the user.

1. Carefully read the content in the dialog box and select **I have read and understand the consequences associated with performing this operation** to confirm the information.
2. Click **OK**.  
The **Success** dialog box is displayed indicating that the operation succeeded.
3. Click **OK**.

----End

## 6.2 Managing iSCSI Host Ports

This function allows you to manage and monitor the iSCSI host ports.

### 6.2.1 Viewing Bit Error Statistics


You can learn about the data transmission quality of a storage device port by checking its bit error statistics. The access performance of application servers deteriorates upon a high bit error rate.

#### Procedure

**Step 1** Log in to DeviceManager.

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

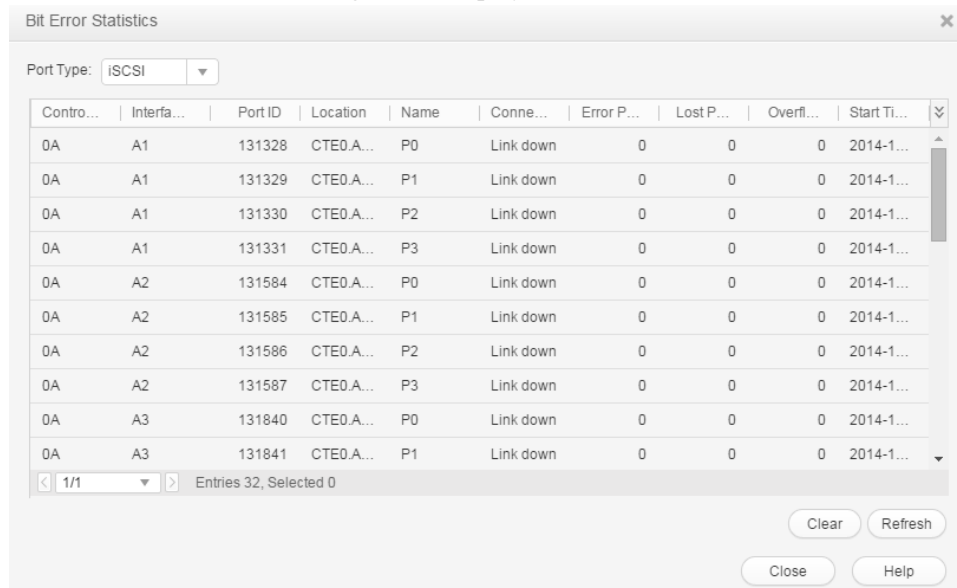
**Step 3** Click the controller enclosure where the bonded Ethernet ports reside.

**Step 4** Click  to switch to the rear view.

**Step 5** Click the Ethernet port you want to view.

**Step 6** In the lower function pane, click **Bit Error Statistics**.

The **Bit Error Statistics** dialog box is displayed.



**Step 7** View bit error information about the Ethernet port.

1. Select **iSCSI** from **Port Type**.
2. From the port list, select the port and view bit error statistics.

 **NOTE**

To clear bit error statistics, click **Clear**.

----End

## 6.2.2 Managing Routes

If cross-segment data transmission is required in an iSCSI network, this operation guides you to configure routes, enabling cross-segment data transmission.

### Prerequisites

The IP address of an Ethernet port has been configured.

 **NOTE**


On redundant links, you must configure IP addresses and route for multiple Ethernet ports.

### Procedure

**Step 1** Log in to DeviceManager.

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

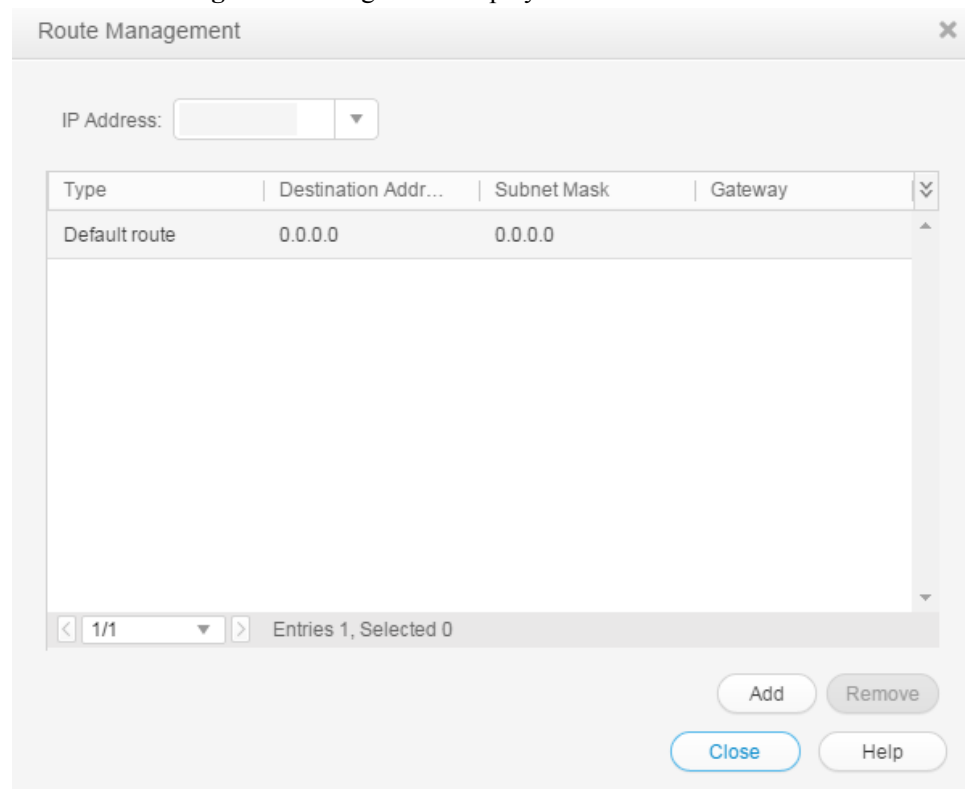
**Step 3** Select the controller enclosure where the Ethernet ports reside.

**Step 4** Click  to switch to the rear view.

**Step 5** Click the Ethernet port that you want to configure.

**Step 6** Click **Route Management**.

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



**Step 7** Set route information for the Ethernet port.

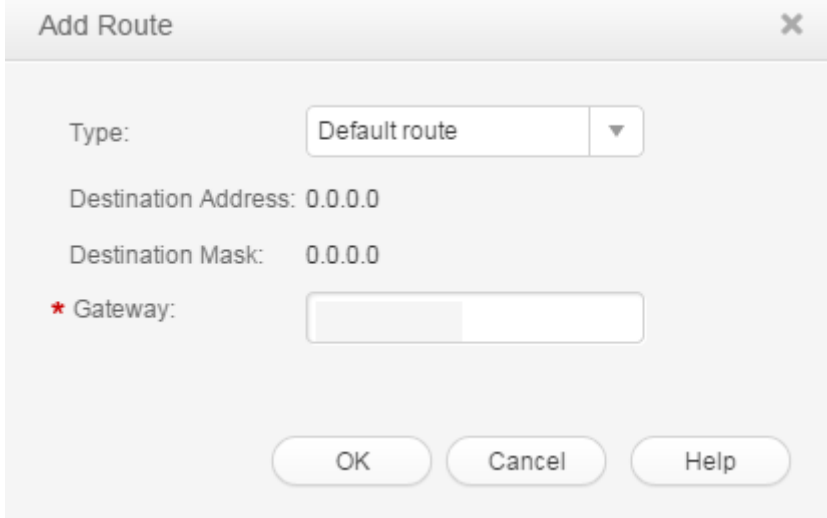
---

**NOTICE**

- The default internal heartbeat IP addresses of a dual-controller storage system are **127.127.127.10** and **127.127.127.11**, and those of a four-controller storage system are **127.127.127.10**, **127.127.127.11**, **127.127.127.12**, and **127.127.127.13**. Therefore, the IP address of the router cannot fall within the 127.127.127.XXX segment. Additionally, the IP address of the gateway cannot be **127.127.127.10**, **127.127.127.11**, **127.127.127.12**, or **127.127.127.13**. Otherwise, routing will fail.
- Internal heartbeat links are established between controllers for the controllers to detect each other's working status. Heartbeat links do not require separate cable connections. In addition, internal heartbeat IP addresses have been assigned before delivery and cannot be changed.

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

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



3. In the text box of **Type**, select the type of the route to be added and the route parameters. [Table 6-9](#) describes related parameters.

**Table 6-9** Route parameters

Parameter	Description
Type	There are three route options: <ul style="list-style-type: none"> <li>- <b>Default route</b>                          The route through which data is forwarded by default if no preferred route is available. The destination address field and the destination mask field (IPv4) or prefix (IPv6) of the default route are automatically set to 0. To use this option, simply add a gateway.</li> <li>- <b>Host route</b>                          A route to an individual host. The destination mask (IPv4) or prefix (IPv6) of the host route is automatically set to 255.255.255.255 or 128. To use this option, add the destination address and a gateway.</li> <li>- <b>Network segment route</b>                          The route to a network segment. To use this option, add the destination address, the destination address mask (IPv4) or prefix (IPv6), and gateway.</li> </ul>
Destination address	IPv4/IPv6 address or network segment of the storage device's Ethernet port or the application server's service network port that connects to the storage device's Ethernet port.
Destination mask/Prefix	Subnet mask of the IPv4 address or the prefix of the IPv6 address for the storage device's Ethernet port or the application server's service network port that connects to the storage device's Ethernet port.
Gateway	Gateway where the IP address of the Ethernet port on the local storage system resides.

**Step 8** Confirm the route management operation.

1. Click **OK**. The route information is added to the route list.  
 The security alert dialog box is displayed.
2. Confirm the information in the dialog box and select **I have read the previous information and understand subsequences of the operation..**
3. Click **OK**.  
 The **Success** dialog box is displayed, indicating that the operation succeeded.

 **NOTE**

To delete a route, select the route and click **Remove**.

4. Click **Close**.

----End

## 6.2.3 Bonding Ethernet Ports

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

### Prerequisites

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

### Context

- Port bonding provides more bandwidth and redundancy for links. Although ports are bonded, each host still transmits data through a single port and the total bandwidth can be increased only when there are multiple hosts. Determine whether to bond ports based on site requirements.
- The port bond mode of a storage system has the following restrictions:
  - On the same controller, a bond port is formed by a maximum of eight Ethernet ports.
  - Only the interface modules with the same port rate (GE or 10GE) can be bonded.
  - The port cannot be bonded across controllers. Non-Ethernet network ports cannot be bonded.
  - SmartIO cards cannot be bonded if they work in cluster or FC mode or run FCoE service in FCoE/iSCSI mode.
  - Read-only users are unable to bind Ethernet ports.
  - Each port is only allowed to be added to only one bonded port. It cannot be added to multiple bonded ports.
  - Physical ports are bonded to create a bond port that cannot be added to the port group.
- After Ethernet ports are bonded, **MTU** changes to the default value and you must set the link aggregation mode for the ports. For example, on Huawei switches, you must set the ports to the static LACP mode.

 **NOTE**

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


### Procedure

**Step 1** Log in to DeviceManager.

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

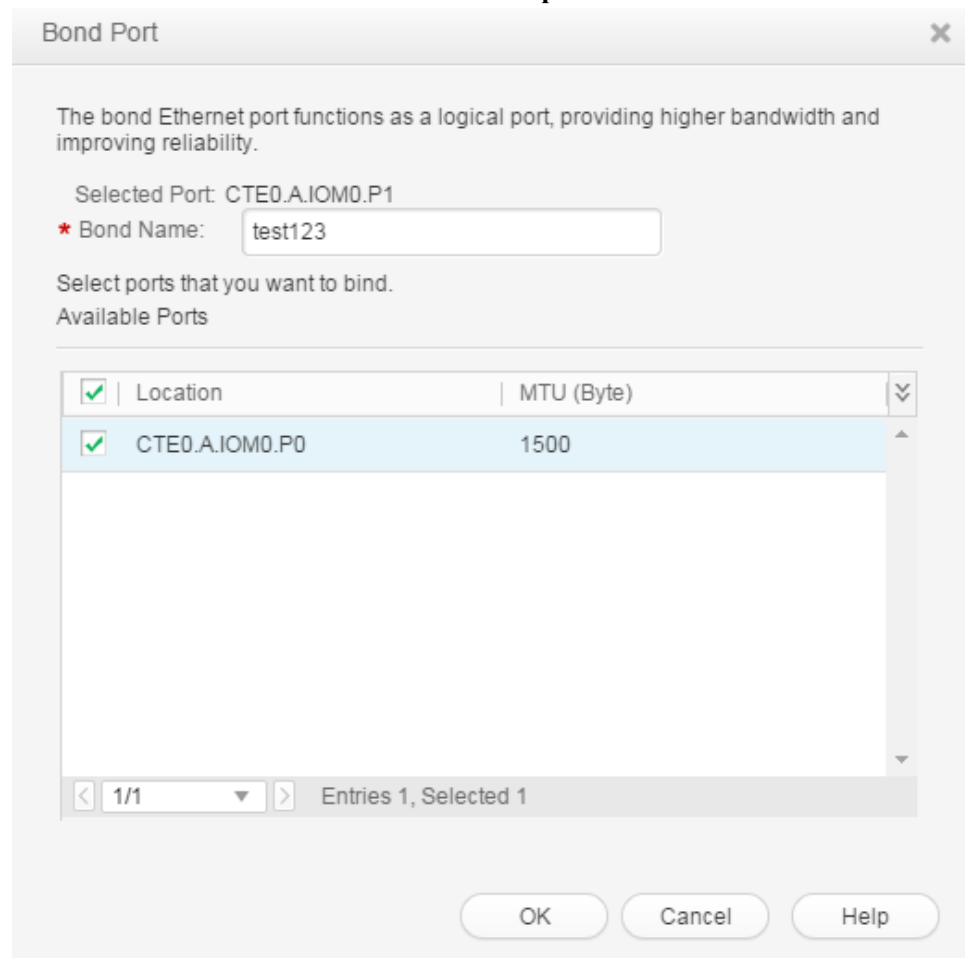
**Step 3** Click the controller enclosure where the Ethernet ports reside.



**Step 4** Click  to switch to the rear view.

**Step 5** Select an Ethernet port you want to bond and click **Bond Port**.

The **Bond Port** dialog box and the selected port are displayed. The format of the port name is **controller enclosure ID.interface module ID.port ID**.



**Step 6** Set the bonding name and available ports for the Ethernet port.

1. In **Bond Name**, enter a name for the port to be bound.  
The name:
  - Can contain only letters, digits, periods (.), underscores (\_), and hyphens (-).
  - Contains 1 to 31 characters.
2. From the **Available Ports** list, select the Ethernet ports you want to bond with the current Ethernet port.
3. Click **OK**.  
The security alert dialog box is displayed.

**Step 7** Confirm the bonding of the Ethernet ports.

1. Confirm the information in the dialog box and select **I have read and understood the consequences associated with performing this operation..**
2. Click **OK**.  
If the operation succeeded, the **Success** message box is displayed.

3. Click **OK**.

----End

## 6.2.4 Canceling Ethernet Port Bonding

This topic guides you through the process of canceling Ethernet port bonding to use them separately.

### Prerequisites

All services running on the Ethernet ports that you want to unbind have been stopped, because canceling Ethernet port bonding interrupts ongoing services.

### Precautions


After an unbinding is complete, the IP addresses of the unbound Ethernet ports are cleared.

### Procedure

**Step 1** Log in to DeviceManager.

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

**Step 3** Click the controller enclosure where the bonded Ethernet ports reside.

**Step 4** Click  to switch to the rear view.

**Step 5** Select the Ethernet port whose bonding you want to cancel.  
The page for canceling Ethernet port bonding is displayed.

**Step 6** Cancel the port bonding.

1. Click **Cancel Bonding**.  
The security alert dialog box is displayed.
2. Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation..**
3. Click **OK**.  
The **Success** message box is displayed, indicating that the operation succeeded.
4. Click **OK**.

----End



## 6.2.5 Viewing Ethernet Port Information

The following procedure guides you through how to view the information about the Ethernet ports on a storage device.

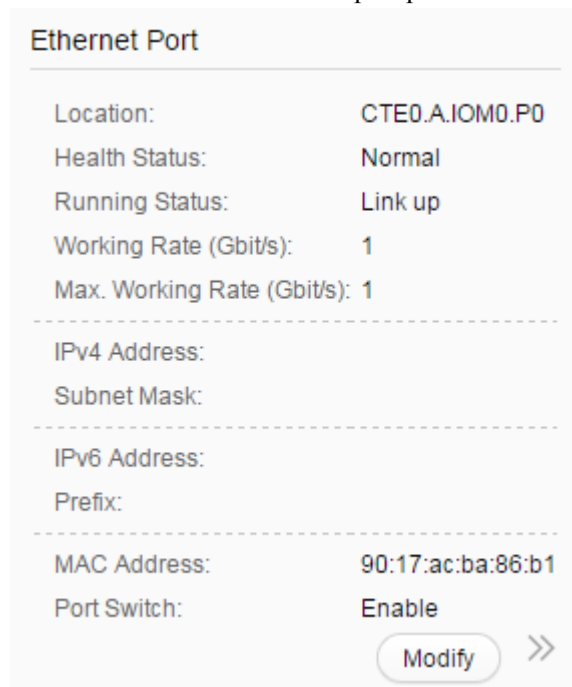
### Prerequisites

An Ethernet interface module has been correctly installed on a controller.

## Procedure

- Step 1** Log in to DeviceManager.
- Step 2** Choose  **System**.
- Step 3** Click the controller enclosure where the Ethernet port resides.
- Step 4** Click  to switch to the rear view.
- Step 5** Click the Ethernet port whose information you want to view.  
 The **Ethernet Port** dialog box is displayed.
- Step 6** View the Ethernet port information.

**Table 6-10** describes Ethernet port parameters.



**Table 6-10** Ethernet port parameters

Parameter	Description	Value
Name	Name of the Ethernet port.	[Example] P0
Location	Location of the Ethernet port.	[Example] XXX0.A1.P0 or XXX0.R5.IOM0.P0 <b>NOTE</b> The displayed information is consistent with actual product specifications.

Parameter	Description	Value
Health Status	Health status of the Ethernet port.	[Example] <b>Normal</b>
Running Status	Running status of the Ethernet port.	[Example] <b>Link Down</b>
Working Rate (Gbit/s)	Data transfer rate of the Ethernet port.	[Example] <b>1</b>
Max. Working Rate (Gbit/s)	Maximum data transfer rate of the Ethernet port.	[Example] 1
IPv4 Address	IPv4 address of the Ethernet port.	[Example] <b>192.168.100.11</b>
Subnet Mask	Subnet mask of IPv4 address of the Ethernet port.	[Example] <b>255.255.255.0</b>
IPv6 Address	IPv6 address of the Ethernet port.	[Example] <b>21DA:D3:0:2F3B:2BB:FF:FE28:9C5B</b>
Prefix	Number of prefix characters of IPv6 address of the Ethernet port.	[Example] <b>64</b>
MAC Address	MAC address of the Ethernet port.	[Example] <b>90:17:ac:ba:86:b1</b>
Port Switch	Switch of the Ethernet port. Port connection will be disconnected if the port switch is set to <b>Disable</b> .	[Example] <b>Enable</b>
MTU (Byte)	Maximum size of a data packet that can be transferred between the Ethernet port and the application server.	[Example] <b>2500</b>
Bond Name	Name of the bonded Ethernet port.	[Example] <b>bond01</b>
iSCSI Target Name	Target name of the network where the Ethernet port resides.	[Example] <b>iqn.2006-08.com.xxx:xxx:53000022a10b58b4::20100:192.168.100.11</b>
Host Initiator Quantity	Number of initiators on the host to which the port belongs.	[Example] <b>1</b>

---End

## 6.2.6 Modifying an Ethernet Port

When the networking mode between a storage device and an application server changes, modify the settings of Ethernet port parameters to ensure proper communication between them.

### Precautions

- Ensure that the storage device has redundant connections or that services running on the storage device are stopped. Change the IP address of the Ethernet port only when necessary.
- The IP addresses of the Ethernet port and internal heartbeat must be on different network segments.

The default IP addresses of the internal heartbeat on the dual-controller storage system are **127.127.127.10** and **127.127.127.11**, and those of the internal heartbeat on the four-controller storage system are **127.127.127.10**, **127.127.127.11**, **127.127.127.12**, and **127.127.127.13**.


- Internal heartbeat links are established between controllers for the controllers to detect each other's working status. Heartbeat links do not require separate cable connections. In addition, internal heartbeat IP addresses have been assigned before delivery and cannot be changed.
- The IP address of an Ethernet port cannot be in the same network segment as that of a management network port.
- The IP address of an Ethernet port cannot be in the same network segment as that of a maintenance network port. The default IP address of the maintenance network port must fall within the **172.31.XXX.XXX** segment.
- If an Ethernet port connects to an application server, the IP address of the Ethernet port must be in the same network segment as that of the service network port on the application server. If an Ethernet port connects to another storage device, the IP address of the Ethernet port must be in the same network segment as that of the peer Ethernet port on the other storage device. If available IP address become insufficient for a network segment for which you want to add an IP address, manually add routes.
- After an Ethernet port is bound, its properties cannot be modified.

### Procedure

**Step 1** Log in to DeviceManager.

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

**Step 3** Select the controller enclosure where the Ethernet port resides.

**Step 4** Click  to switch to the rear view.

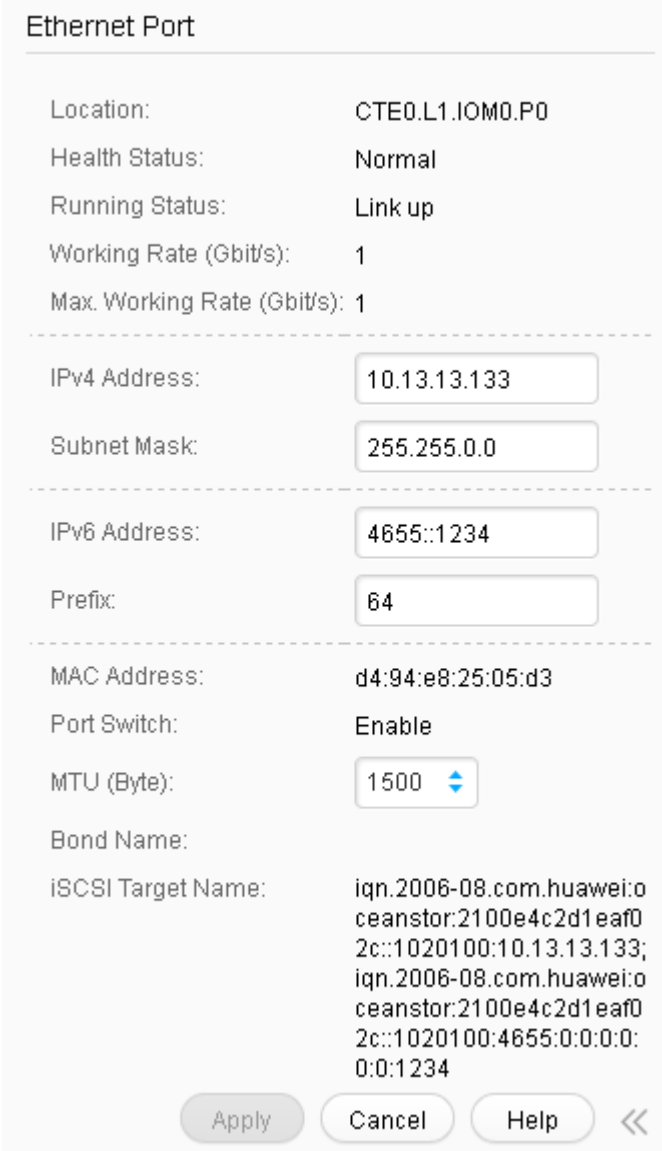
**Step 5** Click the Ethernet port whose information you want to modify.  
The **Ethernet Port** dialog box is displayed.

**Step 6** Modify the Ethernet port.

1. Click **Modify**.

 **NOTE**

You can also click **Properties** to modify the parameters of the Ethernet port.



**Ethernet Port**

Location: CTE0.L1.IOM0.P0

Health Status: Normal

Running Status: Link up

Working Rate (Gbit/s): 1

Max. Working Rate (Gbit/s): 1

---

IPv4 Address: 10.13.13.133

Subnet Mask: 255.255.0.0

---

IPv6 Address: 4655::1234

Prefix: 64

---

MAC Address: d4:94:e8:25:05:d3

Port Switch: Enable

MTU (Byte): 1500

Bond Name:

iSCSI Target Name: iqn.2006-08.com.huawei:oc  
ceanstor:2100e4c2d1eaf0  
2c::1020100:10.13.13.133;  
iqn.2006-08.com.huawei:oc  
ceanstor:2100e4c2d1eaf0  
2c::1020100:4655:0:0:0:0:  
0:0:1234

Apply Cancel Help <<

2. In the **IPv4 address** or **IPv6 address** text box, enter an IP address for the Ethernet port.
3. In the **Subnet Mask** or **Prefix** text box, enter the subnet mask or prefix of the Ethernet port.
4. In **MTU (Byte)**, type a maximum transfer unit (MTU) for the packets transmitted between the Ethernet port and the application server.

**Step 7** Confirm the Ethernet port modification.

1. Click **Apply**.  
The security alert dialog box is displayed.
2. Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation.**

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

----End

## 6.2.7 Naming an iSCSI Device and an iSCSI Initiator

Both the iSCSI device name and iSCSI initiator name contain two parts: the default part and the user-defined part. Only the user-defined part can be modified. The iSCSI target name is dynamically generated based on the iSCSI device name and the identifier of a specific port. (For details about how the iSCSI target name is generated, contact your maintenance personnel.)

### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Settings** >  **Storage Settings** > **Block Storage Service** > **Name Settings**.

**Step 3** Change the iSCSI device name and initiator name.

1. In **iSCSI Device Name**, enter the user-defined part of the iSCSI device name.  
The name can contain 0 to 31 characters.
2. In **iSCSI Initiator Name**, enter the user-defined part of the iSCSI initiator name.  
The name can contain 0 to 31 characters.
3. Click **Save**.  
The **Execution Result** dialog box is displayed, indicating that the operation succeeded.
4. Click **Close**.

----End

## 6.2.8 Setting iSNS

An Internet Storage Name Service (iSNS) server operates as a unified configuration node and allows you to configure and manage the entire storage network, including iSCSI and Fibre Channel devices.

### Context

The traditional device-by-device mode used to configure and manage devices on a storage network requires that each storage device be configured with an initiator and a target separately. As a result, the management and maintenance expenses are high. After configuring iSNS, you do not need to manually configure initiators and targets for each storage device. Instead, the iSNS server takes over the initiator detection and management work, greatly reducing costs.

### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Settings** >  **Storage Settings** > **Block Storage Service** > **iSNS Settings**.

**Step 3** Configure the iSNS service.

1. Type the IP address of the iSNS server in **iSNS Server**.  
The IP address of an iSNS server can be an IPv4 or IPv6 address.
2. Click **Save**.  
The **Execution Result** dialog box is displayed indicating that the operation succeeded.
3. Click **Close**.

----End

## 6.3 Managing Fibre Channel Host Ports

This function allows you to manage and monitor the Fibre Channel host ports.

### 6.3.1 Viewing Bit Error Statistics


You can learn about the data transmission quality of a storage device port by checking its bit error statistics. The access performance of application servers deteriorates upon a high bit error rate.

#### Procedure

**Step 1** Log in to DeviceManager.

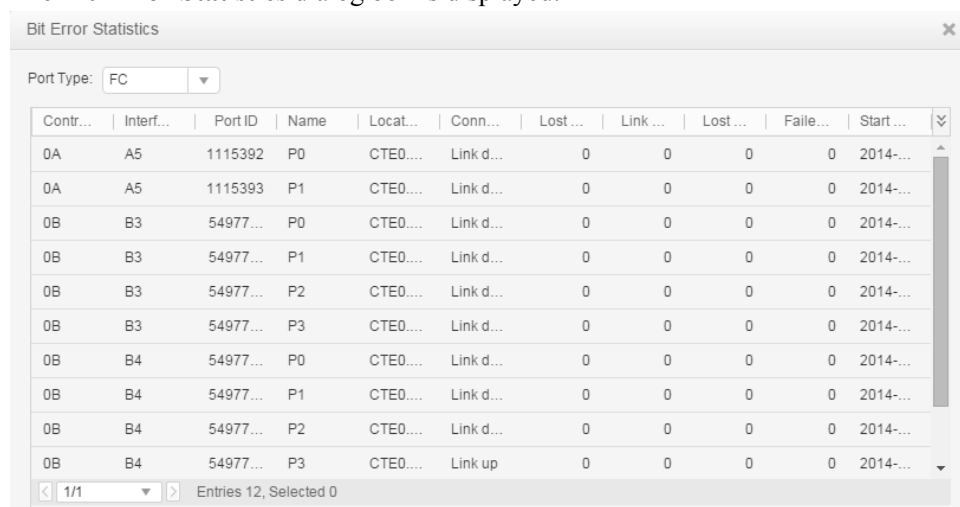
**Step 2** Choose  **System**.

**Step 3** Click the controller enclosure where the Fibre Channel port to be viewed resides.

**Step 4** Click  to switch to the rear view.

**Step 5** Select the Fibre Channel port that you want to view.

**Step 6** In the lower function pane, click **Bit Error Statistics**.  
The **Bit Error Statistics** dialog box is displayed.



Contr...	Interf...	Port ID	Name	Locat...	Conn...	Lost...	Link...	Lost...	Faile...	Start...
0A	A5	1115392	P0	CTE0...	Link d...	0	0	0	0	2014-...
0A	A5	1115393	P1	CTE0...	Link d...	0	0	0	0	2014-...
0B	B3	54977...	P0	CTE0...	Link d...	0	0	0	0	2014-...
0B	B3	54977...	P1	CTE0...	Link d...	0	0	0	0	2014-...
0B	B3	54977...	P2	CTE0...	Link d...	0	0	0	0	2014-...
0B	B3	54977...	P3	CTE0...	Link d...	0	0	0	0	2014-...
0B	B4	54977...	P0	CTE0...	Link d...	0	0	0	0	2014-...
0B	B4	54977...	P1	CTE0...	Link d...	0	0	0	0	2014-...
0B	B4	54977...	P2	CTE0...	Link d...	0	0	0	0	2014-...
0B	B4	54977...	P3	CTE0...	Link up	0	0	0	0	2014-...



**Step 7** View bit error information about the Fibre Channel port.

1. Select **FC** from **Port Type**.
2. From the port list, select the port and view bit error statistics.



To clear bit error statistics, click **Clear**.

---End

## 6.3.2 Viewing Fibre Channel Port Information

The following procedure guides you through how to view the information about the Fibre Channel ports on a storage device.

### Prerequisites


A Fibre Channel interface module has been correctly installed on a controller.

### Procedure

**Step 1** Log in to DeviceManager.

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

**Step 3** Click the controller enclosure where the Fibre Channel port resides.

**Step 4** Click  to switch to the rear view.

**Step 5** Click the Fibre Channel port whose information you want to view.  
The **FC Port** dialog box is displayed.

**Step 6** View the Fibre Channel port information. [Table 6-11](#) describes Fibre Channel port parameters.

FC Port	
Location:	CTE011.P0
Health Status:	Normal
Running Status:	Link up
WWPN:	21000022a105a002
Configured Rate (Gbit/s):	Autonegotiation
Working Rate (Gbit/s):	8
Max. Working Rate (Gbit/s):	2
Working Mode:	Fabric
Port Switch:	Disable

[Modify](#)

**Table 6-11** Fibre Channel port parameters

Parameter	Description	Value
Name	Name of the Fibre Channel port.	[Example] P0
Location	Location of the Fibre Channel port.	[Example] XXX0.A1.P0 or XXX0.B.IOM1.P0 <b>NOTE</b> The displayed information is consistent with actual product specifications.
Health Status	Health status of the Fibre Channel port.	[Example] Normal
Running Status	Running status of the Fibre Channel port.	[Example] Link up
WWPN	WWPN of the Fibre Channel port.	[Example] 21000022a105a50e
Configured Rate (Gbit/s)	Configured rate of the Fibre Channel port.	[Example] Autonegotiation
Working Rate (Gbit/s)	Data transfer rate of the Fibre Channel port.	[Example] 8
Max. Working Rate (Gbit/s)	Maximum data transfer rate of the Fibre Channel port.	[Example] 8
Working Mode	Working mode of the Fibre Channel port.	[Example] FC-AL
Port Switch	Switch of the Fibre Channel port. Possible values are <b>Enable</b> and <b>Disable</b> . Port connection will be disconnected if the port switch is set to <b>Disable</b> .	[Example] Enable
Host Initiator Quantity	Number of initiators on the host to which the port belongs.	[Example] 1

----End

### 6.3.3 Modifying a Fibre Channel Port

When the networking mode between the storage device and application servers varies, modify the settings of Fibre Channel ports to retain normal communication between them.

## Context

Note the following when you modify Fibre Channel ports:

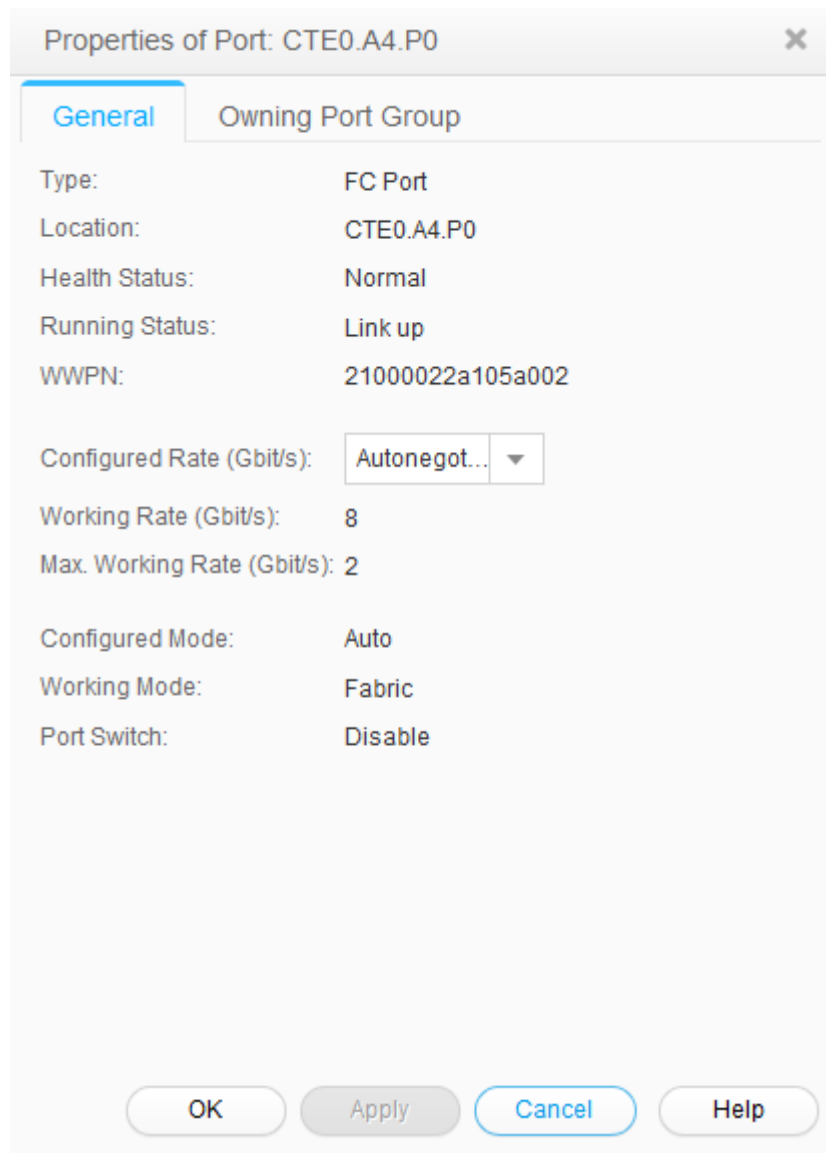
- If the storage device connects to an application server through a Fibre Channel port, ensure that the rate of the Fibre Channel port on the storage device is the same as that of the peer host bus adapter (HBA) port on the application server. Otherwise, the communication between the storage device and application server may fail.
- When two storage devices connect to each other through Fibre Channel ports, ensure that the rates of the Fibre Channel ports on both storage device are the same. Otherwise, the communication between the storage device and application server may fail.
- Given modifying the Fibre Channel ports interrupts the communication between the storage device and application servers, do not modify any Fibre Channel port settings when ongoing services are present on the storage device.

## Procedure

**Step 1** Log in to DeviceManager.

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

**Step 3** Select a Fibre Channel port and click **Properties**.



**Step 4** In **Configured Rate (Gbit/s)**, select a data transfer rate for the Fibre Channel port.

---

 **NOTICE**

- The rate and mode of the Fibre Channel port on a storage system must be consistent with those of the Fibre Channel HBA on the peer application server. If the rates and modes are inconsistent, the communication fails.
- The rate and mode of the Fibre Channel ports on two storage systems that are connected to each other must be consistent. If the rates and modes are inconsistent, the communication fails.

---

Available rates of a Fibre Channel port are **2 Gbit/s, 4 Gbit/s, 8Gbit/s, 16Gbit/s** and **Autonegotiation**. Select a fixed value after learning the rate of the peer Fibre Channel port.

 **NOTE**

- If the configured maximum rate of the port is 4 Gbit/s, you can set the value to be **2 Gbit/s** or **4 Gbit/s**.
- If the configured maximum rate of the port is 8 Gbit/s, you can set the value to be **2 Gbit/s**, **4 Gbit/s**, or **8 Gbit/s**.
- If the configured maximum rate of the port is 16 Gbit/s, you can set the value to be **4 Gbit/s**, **8 Gbit/s**, or **16 Gbit/s**.

**Step 5** Confirm the Fibre Channel port modification.

1. Click **OK**.  
The security alert dialog box is displayed.
2. Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation..**
3. Click **OK**.  
The **Success** message box is displayed, indicating that the operation succeeded.
4. Click **OK**.

----End

## 6.4 Managing Disk Domains

This chapter describes the operations for managing disk domain, including viewing disk domain information, modifying the properties of disk domain, expanding disk domain and more.

### 6.4.1 Viewing Disk Domain Information

This operation enables you to view disk domain information.

#### Prerequisites

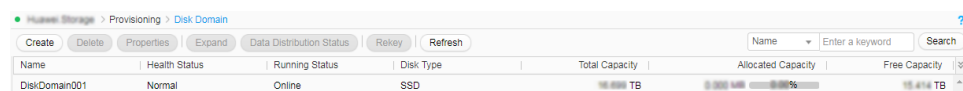
A disk domain has been created in the system.

#### Procedure

**Step 1** Log in to DeviceManager.

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

**Step 3** View disk domain information in the upper left area. [Table 6-12](#) describes related parameters.




Name	Health Status	Running Status	Disk Type	Total Capacity	Allocated Capacity	Free Capacity
DiskDomain001	Normal	Online	SSD	16.000 TB	0.000 TB	16.000 TB

**Table 6-12** Disk domain parameters

Parameter	Description	Setting
Name	Name of a disk domain.	[Example] DiskDomain001
ID	ID of a disk domain.	[Example] 1
Health Status	Health status of a disk domain.	[Example] Normal
Running Status	Running status of a disk domain.	[Example] Online
Disk Type	Type of disks in a disk domain. The disk is categorized by its storage media and whether it is encrypted or not. <ul style="list-style-type: none"> <li>● SSD</li> <li>● SSD-SED</li> <li>● SAS</li> <li>● SAS-SED</li> <li>● NL-SAS</li> <li>● NL-SAS-SED</li> </ul> <b>NOTE</b> Self-encrypting drives (SED) means encrypted disk.	[Example] SSD
Total Capacity	Total capacity of a disk domain.	[Example] 2.00 TB
Allocated Capacity	Allocated capacity of a disk domain.	[Example] 100.00 MB
Free Capacity	Free capacity of a disk domain.	[Example] 500 GB
Anti-Wear Leveling Disk ID	If the wear degree of any disk is high, the system enters the anti-wear leveling mode, and the ID of the disk with the highest wear degree is displayed.	[Example] —

 **NOTE**

The following operations can improve your efficiency:

- Click  in the upper right part of the function pane and set the parameters to be displayed.
- In the search bar in the upper right corner of the **Disk Domain** page, enter a keyword to search for required information.

**Step 4** In the lower left area of the function pane, view capacity, owning storage pool, and disk information about the disk domain. You can delete or expand the owning storage pool.

----End

## 6.4.2 Viewing Data Distribution in a Disk Domain

This operation enables you to view data distribution in a disk domain.

### Prerequisites

A disk domain has been created in the system.

### Procedure

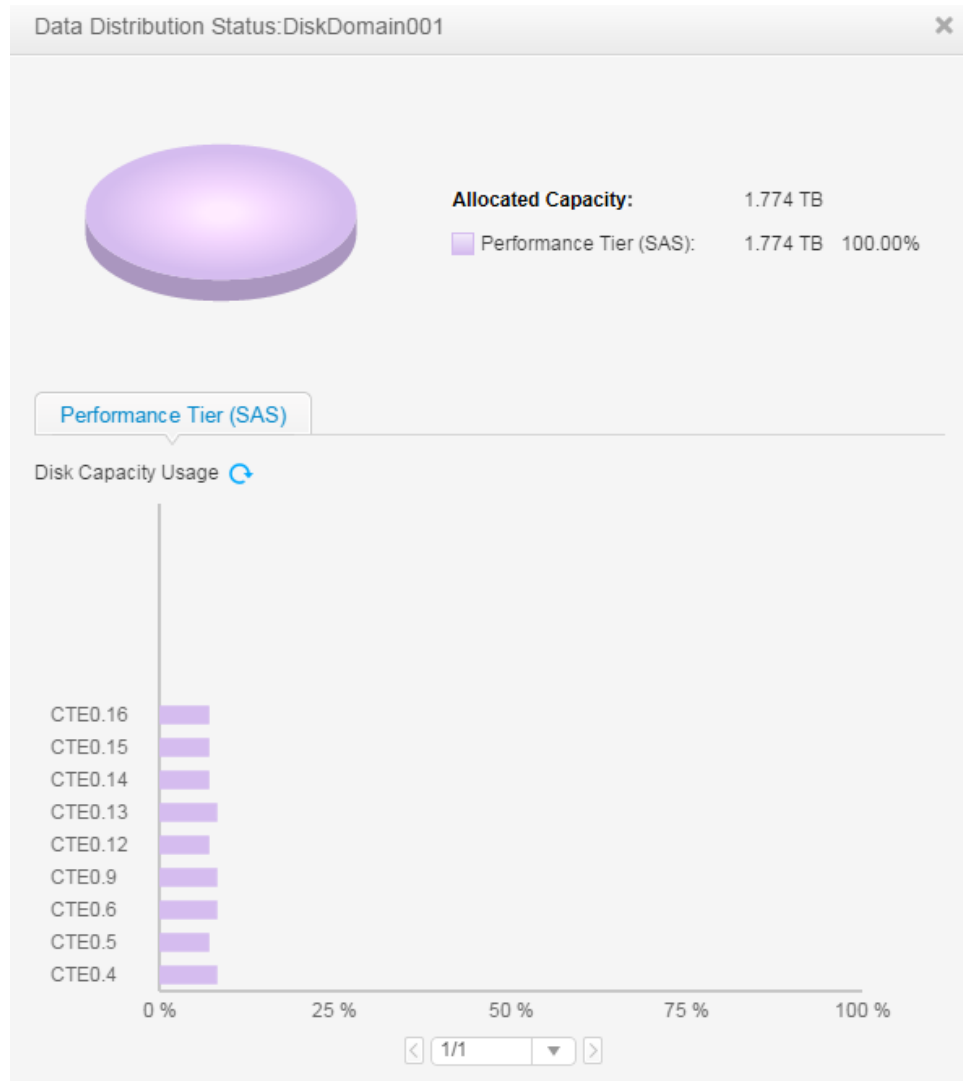
**Step 1** Log in to DeviceManager.

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

**Step 3** Select the disk domain you want to view.

**Step 4** Click **Data Distribution Status**.


The **Data Distribution Status** page is displayed.



**Step 5** View data distribution in a disk domain.

- Click **Properties** to view the used capacity and the percentage of the used capacity in each tier.
- Click **Data Distribution Status**, in the lower part, the storage tier tabs allow you to view the percentage of used disk capacity of each storage tier to the total disk capacity.

**NOTE**

The system refreshes disk capacity usage in each tier every 15 seconds. You can also click  to manually refresh the information.

---End

### 6.4.3 Deleting an Unencrypted Disk Domain

This operation enables you to delete a disk domain that is no longer needed.

#### Prerequisites

The storage pools in the disk domain have been deleted.



## Procedure

**Step 1** Log in to DeviceManager.

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

**Step 3** Delete a disk domain.

1. Select the disk domain you want to delete and click **Delete**.  
The security alert dialog box is displayed.
2. Click **OK**.  
A message is displayed, indicating that the operation succeeded.
3. Click **OK**.

---End

### 6.4.4 Deleting an Encrypted Disk Domain

This operation enables you to delete a disk domain that is no longer needed.

#### Prerequisites

The storage pools in the disk domain have been deleted.

## Procedure

**Step 1** Log in to DeviceManager.

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

**Step 3** Delete a disk domain.

1. Select the encrypted disk domain you want to delete and click **Delete**.  
The **Delete Disk Domain** dialog box is displayed.
2. **Optional:** Select **Data Erase**.

#### **NOTE**

- If **Data Erase** is selected, the system will first delete data from encrypted disks within the disk domain and then delete the disk domain. You must select **I have read and understand the consequences associated with performing this operation.** to complete the disk domain deletion.
- If **Data Erase** is not selected, the system will only delete the disk domain.

3. Click **OK**.  
A message is displayed, indicating that the operation succeeded.
4. Click **OK**.

---End

### 6.4.5 Modifying the Hot Spare Policy of a Disk Domain

This operation enables you to modify the hot spare policy of a disk domain.

## Precautions

Note the following if you want to modify the hot spare policy of a disk domain:

- If the hot spare policy needs to be modified from **None** to **Low**, or from **Low** to **High**, the remaining capacity of the disk domain cannot be smaller than 10% of the disk domain's total capacity.
- If the hot spare policy needs to be modified from **None** to **High**, the remaining capacity of the disk domain cannot be smaller than 20% of the disk domain's total capacity.

A hot spare policy cannot be modified if the disk domain remaining capacity does not meet the previously described requirements. To modify the hot spare policy successfully, expand the disk domain.

## Procedure

**Step 1** Log in to DeviceManager.

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

**Step 3** Modify the properties of a disk domain.

1. Select the disk domain you want to modify and click **Properties**.  
The **Properties of Disk Domain** dialog box is displayed.
2. Click **Hot Spare Policy** tab.
3. Modify the hot spare policy in the disk domain.
4. Click **OK**.

The security alert dialog box is displayed.

### **NOTE**

Only when the level of a hot spare policy is modified from high to low, a **Danger** dialog box is displayed indicating risky operations.

5. Read the content carefully and select **I have read and understand the consequences associated with performing this operation**, and click **OK**.

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

6. Click **Close**.

----End

## 6.4.6 Expanding a Disk Domain

This operation allows you to increase the capacity of a disk domain.

### Prerequisites

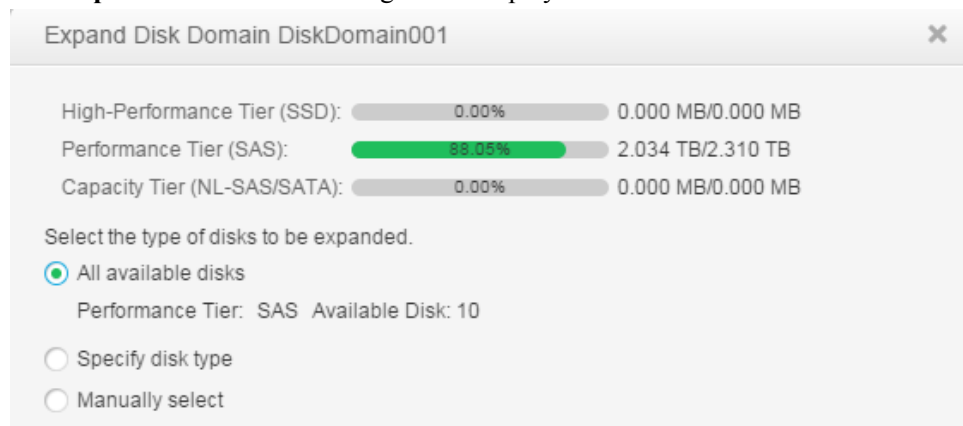
Disks used for capacity expansion are available.

### Procedure

**Step 1** Log in to DeviceManager.

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

- Step 3** Select the disk domain you want to expand and click **Expand**.  
The **Expand Disk Domain** dialog box is displayed.



- Step 4** Select an expansion method.

The following expansion methods are available:

- Select **All available disks** to add all available disks to the disk domain.
- Select **Specify disk type**.
- Select **Manually Select** and click **Select...**. On the **Select Disks** page, add disks from **Available Disks** to **Selected Disks** and click **OK**.

- Step 5** Confirm the expansion of the disk domain.

1. Click **OK**.  
The security alert dialog box is displayed.
2. Confirm the 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** to finish expanding.

---End

## 6.4.7 Updating Key of Encrypted Disk Domain

You can periodically update keys for encrypted disk domains to improve data access security.

### Prerequisites

- Disk domains have been encrypted.
- The encryption server is running normally.

### Procedure

- Step 1** Log in to DeviceManager.

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

- Step 3** Select the disk domain whose key you want to update and click **Rekey**.

The system automatically updates the key.

----End

## 6.5 Managing Storage Pools

This function enables you to consolidate the storage resources provided by different types of hard disks into storage pools as well as centrally manage the storage resources.

### 6.5.1 Viewing Storage Pool Information

This operation enables you to view the information about all the storage pools on a storage system.

#### Prerequisites

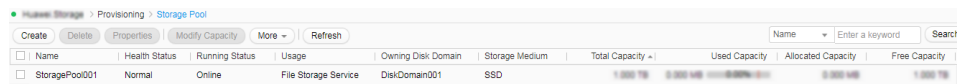
At least one storage pool has been created on the storage system.

#### Procedure

**Step 1** Log in to DeviceManager.

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

**Step 3** View storage pool information. [Table 6-13](#) describes storage pool parameters.



**Table 6-13** Storage pool parameters

Parameter	Description	Setting
Name	Name of a storage pool.	[Example] <b>storagepool1</b>
ID	ID of a storage pool.	[Example] <b>1</b>
Health Status	Health status of a storage pool.	[Example] <b>Normal</b>
Running Status	Running status of a storage pool.	[Example] <b>Online</b>
Usage	Usage of a storage pool. The usages include: <ul style="list-style-type: none"> <li>● <b>Block Storage Service:</b> for creating LUNs.</li> <li>● <b>File Storage Service:</b> for creating file systems.</li> </ul>	[Example] <b>Block Storage Service</b>

Parameter	Description	Setting
Owning Disk Domain	Name of the disk domain that a storage pool corresponds to.	[Example] <b>DiskDomain001</b>
Storage Medium	Disk types in a storage pool.	[Example] <b>SSD</b>
Total Capacity	Total capacity of a storage pool.	[Example] <b>2.000 TB</b>
Used Capacity	Sum of the allocated capacity and data protection capacity in the storage pool, that is, Used Capacity = Allocated Capacity + Data Protection Capacity. The percentage of <b>Used Capacity to Total Capacity</b> is displayed on DeviceManager.	[Example] <b>30.293 GB</b> <b>70.23%</b>
Allocated Capacity	Capacity actually allocated by a storage pool to LUNs or file systems	[Example] <b>100.000 MB</b>
Free Capacity	Free capacity of a storage pool.	[Example] <b>500 GB</b>
Data Protection Capacity	Capacity allocated by a storage pool for data protection. <b>NOTE</b> For example, the snapshots are created for LUNs or file systems within a storage pool. The storage space these snapshots occupy is data protection capacity.	[Example] <b>30.000 GB</b>
Migration Triggering Mode	Mode of data migration among storage tiers in a storage pool. <b>NOTE</b> This parameter is only applicable for storage pool with <b>Block Storage Service</b> .	[Example] <b>Manual</b>
Total Subscribed Capacity	Sum of the preset capacities of all the LUNs and capacities of all the LUNs' activated snapshots in the storage pool.	[Example] 46.000 GB (0.15%)

Parameter	Description	Setting
Capacity Saved by SmartDedupe	Size of storage space saved by the deduplication of data written to the LUN.	[Example] 40.959 GB (50%)
Capacity Saved by SmartCompression	Size of storage space saved by the compression of data written to the LUN.	[Example] 40.959 GB (50%)
Capacity Saved by SmartDedupe and SmartCompression	Total storage space saved after data written to LUNs is deduplicated and compressed.	[Example] 81.919 GB (50%)

**Step 4** Select a storage pool, and in the area below, view the LUN or file system information.

----End

## 6.5.2 Viewing General Information About a Storage Pool

This operation enables you to view the general properties of a storage pool.

### Prerequisites

At least one storage pool has been created on the storage system.

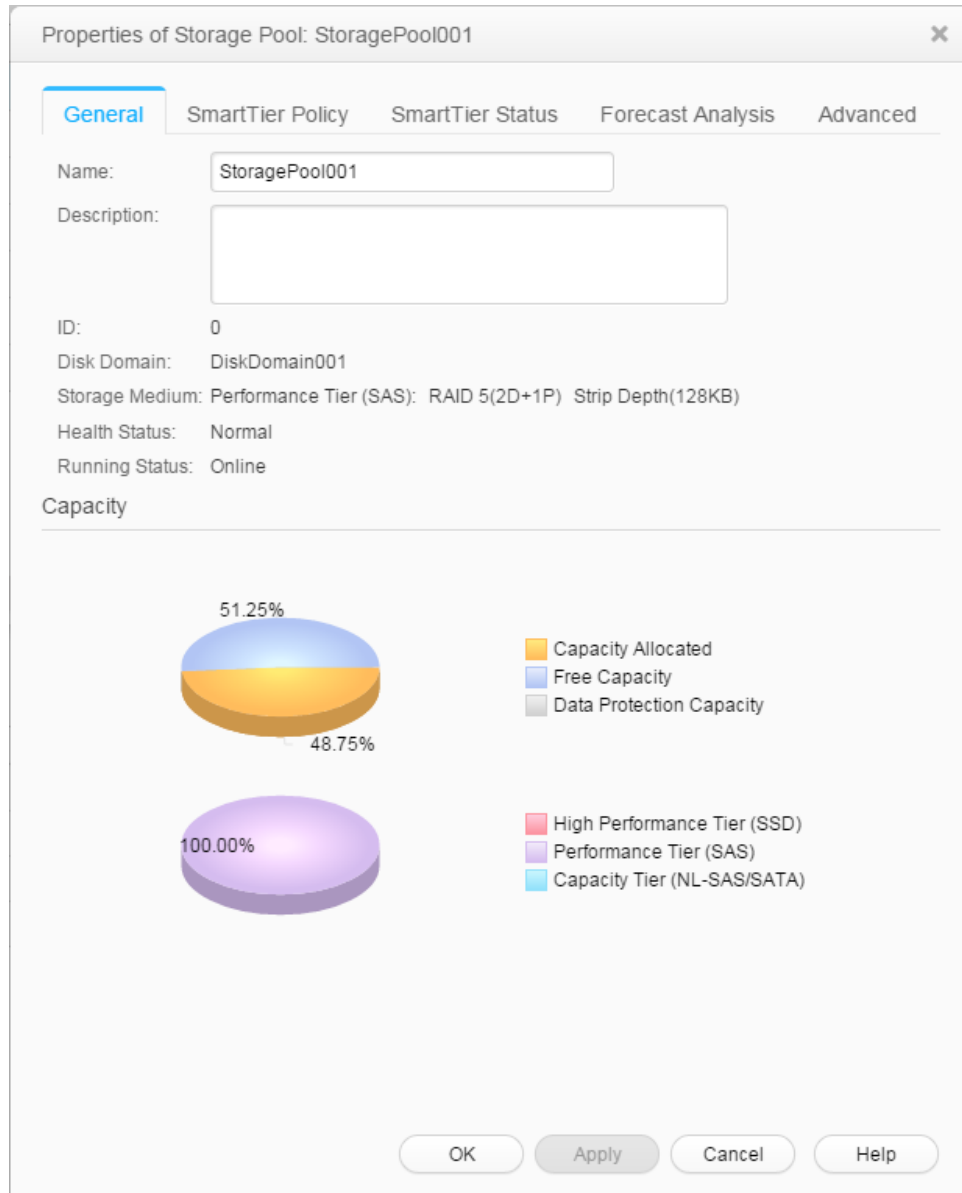
### Procedure

**Step 1** Log in to DeviceManager.

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

**Step 3** Select the storage pool whose information you want to view and click **Properties**.  
 The **Storage Pool Properties** dialog box is displayed.

**Step 4** View the general properties of the storage pool. [Table 6-14](#) describes storage pool general parameters parameters.



**Table 6-14** Storage pool general parameters

Parameter	Description	Setting
Name	Name of a storage pool.	[Example] <b>StoragePool001</b>
Description	Description of a storage pool.	[Example] -
ID	ID of a storage pool.	[Example] <b>2</b>
Disk Domain	Name of the disk domain that a storage pool corresponds to.	[Example] <b>DiskDomain001</b>

Parameter	Description	Setting
Storage Medium	Storage tier information about a storage pool, such as disk type, RAID level, and strip depth.	[Example] <b>Performance Tier (SAS): RAID 5(4D+1P) Strip Depth(128KB)</b>
Health Status	Health status of a storage pool.	[Example] <b>Normal</b>
Running Status	Running status of a storage pool.	[Example] <b>Online</b>
Saved Capacity after Deduplication	Size of storage space saved by the deduplication of data written to the LUN.	[Example] 40.959 GB (50%)
Saved Capacity after Compression	Size of storage space saved by the compression of data written to the LUN.	[Example] 40.959 GB (50%)
Total capacity saved by Deduplication and Compression	Total storage space saved after data written to LUNs is deduplicated and compressed.	[Example] 81.919 GB (50%)
Total Subscribed Capacity Ratio	Ratio of the actual capacity occupied by LUNs to the total subscribed capacity.	[Example] 0.15% (46.000 GB)
Capacity	Storage pool capacity distribution.	[Example] -

 **NOTE**

The name and description of a storage pool can be changed.

----End

### 6.5.3 Modifying a SmartTier Policy

This operation enables you to modify the data relocation mode of a storage pool to improve storage performance.



#### Prerequisites

At least one storage pool has been created and the storage pool has at least two storage tiers.

#### Procedure

**Step 1** Log in to DeviceManager.



- Step 2** Choose  **Provisioning** >  **Storage Pool**.
- Step 3** Select the storage pool whose properties you want to modify and click **Properties**.  
 The **Storage Pool Properties** dialog box is displayed.
- Step 4** Modify the SmartTier policy.
1. Click the **SmartTier Policy** tab.
  2. Modify the SmartTier policy of the storage pool. [Table 6-15](#) lists related parameters.

**Table 6-15** SmartTier policy of the storage pool

Parameter	Description	Setting
Cache Mode	<p>Select <b>Enable</b> to enable SSD caching. In this mode, the data analysis period is shortened, and at the same time, the storage pool is monitored around the clock. As a result, hotspot data can be quickly identified and migrated, accelerating access to hotspot data.</p> <p><b>NOTE</b>                      This parameter is displayed only when the system has the SmartTier license. Before enabling cache mode, check that the following conditions are met:</p> <ul style="list-style-type: none"> <li>– The SmartTier license does not expire.</li> <li>– The storage pool has a high performance tier.</li> <li>– The data migration plan is set to <b>Periodical</b>.</li> <li>– The <b>Usage</b> of the storage pool is <b>Block Storage Service</b>.</li> </ul>	<p>[Example]  <b>Enable</b></p>

Parameter	Description	Setting
Service Monitoring Period	<p>Period of time during which the service is monitored and hotspot statistics is collected after you select <b>Enable I/O monitoring</b>. The statistics serves as guidance for data to migrate among different storage tiers.</p> <p>You can specify the monitoring period by selecting days, and setting <b>Start Time</b> or <b>Duration</b>.</p>	<p>[Example]  <b>Enabling I/O monitoring</b></p>
Data Migration Plan	<p>The trigger policy of data relocation between the storage layers in a storage pool. The policies include:</p> <ul style="list-style-type: none"> <li>- Manual: You must manually trigger the data relocation among storage tiers. The data relocation process is transparent to application servers. Manual data relocation can be performed anytime.</li> <li>- Periodical: You must specify the start time and duration of data relocation for the storage system to perform data relocation automatically at the specified time. This reduces the management cost and complexity. The data relocation process is transparent to application servers. Automatic data relocation is performed only at the specified time.</li> </ul>	<p>[Example]  <b>Periodical</b></p>

 **NOTE**

- If **Data Migration Plan** is set to **Periodical**, I/Os are monitored on a 7x24 basis by default.
- SmartTier policy is only applicable when **Usage** of a storage pool is configured as **Block Storage Service**.

**Step 5** Confirm the modification of the SmartTier policy.

1. Click **OK**.

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

2. Click **Close**.

----End

## 6.5.4 Viewing SmartTier Status

This operation enables you to view the status of a storage layer in a storage pool.

### Prerequisites

- At least one storage pool has been created on the storage system.
- The **Usage** of the storage pool is **Block Storage Service**.

### Procedure

**Step 1** Log in to DeviceManager.

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

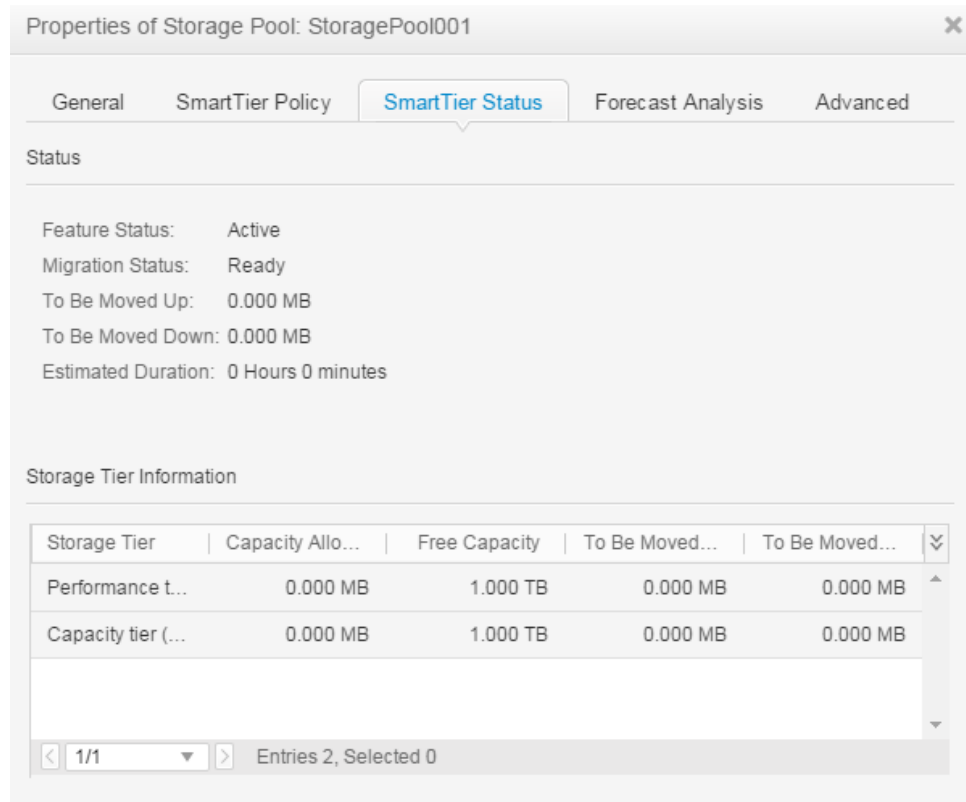
**Step 3** Select the storage pool that you want to modify and click **Properties**.

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

**Step 4** View the status and details of the storage tier.

1. Click the **SmartTier Status** tab.

2. View the **Status** and **Storage Tier Information** of the storage pool. [Table 6-16](#) describes storage tier parameters.



**Table 6-16** Storage tier parameters

Parameter	Description	Setting
Feature Status	<p>The feature status of SmartTier includes <b>Active</b> and <b>Inactive</b>.</p> <ul style="list-style-type: none"> <li>- When <b>Feature Status</b> is <b>Active</b>, you can use SmartTier feature.</li> <li>- When <b>Feature Status</b> is <b>Inactive</b>, you cannot use SmartTier feature.</li> </ul>	<p>[Example]  <b>Active</b></p>

Parameter	Description	Setting
Migration Status	<p>The data migration status of SmartTier includes <b>Ready</b>, <b>Migrating</b> and <b>Suspended</b>. You can manage data migration by starting, stopping, suspending or continuing it.</p> <ul style="list-style-type: none"> <li>- Ready means a storage pool has multiple storage tiers. You can start data migration automatically or manually.</li> <li>- Migrating means a storage pool is migrating data.</li> <li>- Suspended means a storage pool has stopped an ongoing data migration or a not-start data migration.</li> </ul>	<p>[Example]  <b>Ready</b></p>
Estimated Duration	Estimated time that will be spent migrating data.	<p>[Example]  <b>30 minutes</b></p>
To Be Moved Up	Amount of data to be migrated from a storage tier to a higher-performance storage tier.	<p>[Example]  <b>512.000 MB</b></p>
To Be Moved Down	Amount of data to be migrated from a storage tier to a lower-performance storage tier.	<p>[Example]  <b>512.000 MB</b></p>
Storage Tier	Type of a storage tier, such as high-performance tier, performance tier, or capacity tier.	<p>[Example]  <b>High-performance tier</b></p>
Allocated Capacity	Total used capacity of a storage tier.	<p>[Example]  <b>2.000 TB</b></p>
Free Capacity	Total free capacity of a storage tier.	<p>[Example]  <b>50.000 GB</b></p>

----End

## 6.5.5 Forecasting Storage Pool Performance

This operation allows the storage system to provide a recommended capacity ratio for a storage pool based on its configuration of hard disks and RAID policy.

### Prerequisites

- At least a LUN whose relocation policy is **Automatic relocation** is available.
- The I/O monitoring of the storage pool has been enabled.
- LUNs have been accessed after the I/O monitoring is enabled.
- The **Usage** of the storage pool is **Block Storage Service**.

### Procedure

**Step 1** Log in to DeviceManager.

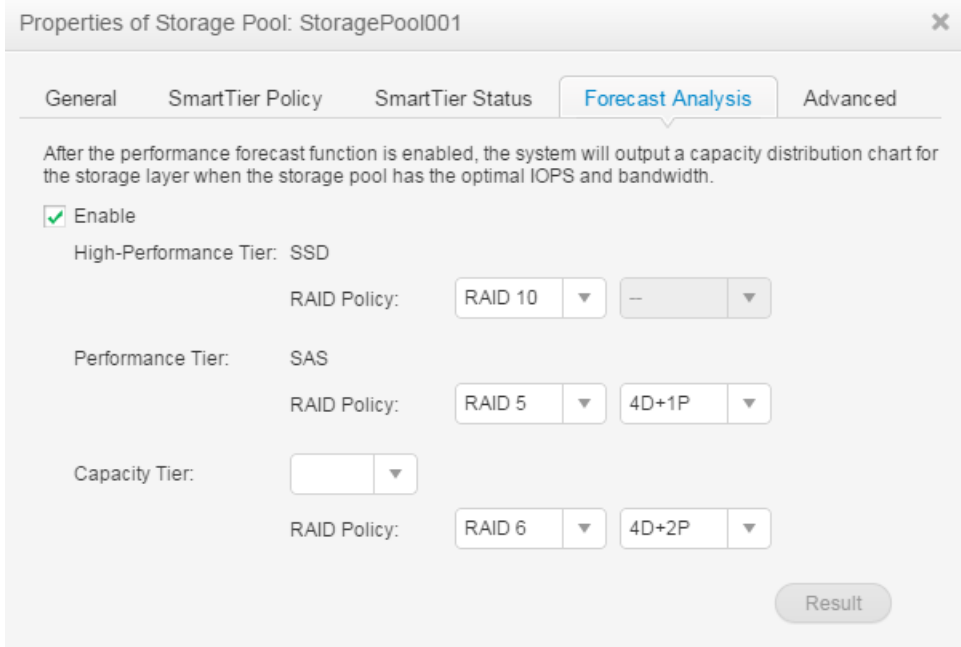
**Step 2** Choose  **Provisioning** >  **Storage Pool**.

**Step 3** Select the storage pool whose properties you want to forecast performance and click **Properties**.

The **Properties of Storage Pool** dialog box is displayed.

**Step 4** Enable the performance forecasting function. If the forecast analysis function has been enabled, skip this step.

1. Click the **Forecast Analysis** tab.



Properties of Storage Pool: StoragePool001

General SmartTier Policy SmartTier Status **Forecast Analysis** Advanced

After the performance forecast function is enabled, the system will output a capacity distribution chart for the storage layer when the storage pool has the optimal IOPS and bandwidth.

Enable

High-Performance Tier: SSD

RAID Policy: RAID 10 --

Performance Tier: SAS

RAID Policy: RAID 5 4D+1P

Capacity Tier:

RAID Policy: RAID 6 4D+2P

Result

2. Select **Enable** to enable the performance forecasting function.
3. Click **Apply**.

The **Execution Result** dialog box is displayed indicating that the function is enabled successfully.

4. Click **Close**.

**Step 5** Configure the performance forecasting function.

1. Click the **Forecast Analysis** tab.
2. From each of the **High-performance Tier**, **Performance Tier**, and **Capacity Tier** drop-down lists, select the type of hard disks and RAID policy.

**Step 6** Viewing the forecast analysis results.

1. Click **Result**.

The **Result** dialog box is displayed, and the following information can be viewed.

- Recommended capacity ratio configuration of each storage tier
- IOPS in the recommended capacity ratio configuration
- Bandwidth in the recommended capacity ratio configuration

---End

## 6.5.6 Modifying the Advanced Properties of a Storage Pool

This operation enables you to modify the advanced properties of a storage pool.

### Procedure

**Step 1** Log in to DeviceManager.

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

**Step 3** Select the storage pool whose properties you want to modify and click **Properties**.  
The **Properties of Storage Pool** dialog box is displayed.

**Step 4** Set advanced properties for the storage pool.

1. In the **Properties of Storage Pool** dialog box, click the **Advanced** tab.

[Table 6-17](#) describes the related parameters.

**Table 6-17** Storage pool advanced parameters

Parameter	Description	Setting
Used Capacity Alarm Threshold (%)	<p>If the storage pool contains a LUN with value-added service, or a file system with value-added service, or a thin LUN, or a thin file system, when the percentage of the used capacity of the storage pool to the total capacity of the storage pool (the used capacity for short as below) reaches the used capacity alarm threshold, the system generates an alarm. The alarm is generated in 3 circumstances:</p> <ul style="list-style-type: none"> <li>- When the used capacity reaches the used capacity alarm threshold, the system generates an alarm informing that the capacity of storage pool is insufficient.</li> <li>- When the used capacity alarm threshold is no greater than 88 and the used capacity reaches 90%, the system generates an alarm informing that the storage pool is running out.</li> <li>- When the used capacity alarm threshold is greater than 88 and the used capacity reaches (used capacity alarm threshold +2)%, the system generates an alarm informing that the storage pool is running out.</li> </ul> <p><b>NOTE</b> If the used capacity alarm threshold is set as 85, when the used capacity reaches 85%, the system generates an alarm informing that the capacity of storage pool is insufficient, and when the used capacity reaches 90%, the system generates an alarm informing that the storage pool is running out. If the used capacity alarm threshold is set as 91, when the used capacity reaches 93%, the system generates an alarm informing that the storage pool is running out.</p> <p>A proper used capacity alarm threshold helps you monitor the capacity usage of a storage pool.</p>	<p>[Value range] 1 to 95 [Default Value] <b>80</b></p>
Data Protection Capacity Alarm Threshold (%)	<p>When ratio the data protection capacity of the storage pool to the total capacity of the storage pool exceeds the capacity alarm threshold, the system generates an alarm.</p>	<p>[Value range] 1 to 100 [Default Value] <b>100</b></p>



2. Click **OK**.  
The **Execution Result** dialog box is displayed indicating that the operation succeeded.
3. Click **Close**.

----End

## 6.5.7 Modifying Capacity of a Storage Pool

When the storage pool capacity is insufficient, you can expand it to meet actual needs. When the storage pool is with surplus capacity, you can reduce it to release storage space.

### Prerequisites

- The **Health Status** of the storage pool is **Normal**.
- The disk domain has available storage space for capacity expansion of the storage pool.
- The reduced capacity must be smaller than maximum capacity for reduction.

### Procedure

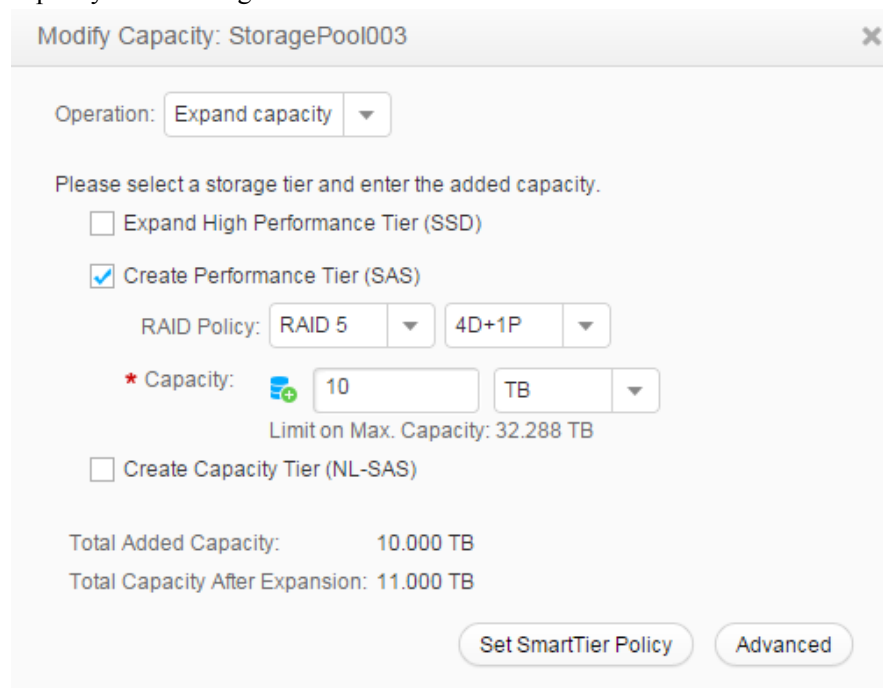
**Step 1** Log in to DeviceManager.

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

**Step 3** Select the storage pool you want to expand and click **Modify Capacity**.  
The **Modify Capacity** dialog box is displayed.

**Step 4** In **Operation**, select the mode of modifying capacity. The modes are **Expand capacity** and **Reduce capacity**.

- Expand the capacity of a storage pool.
  - a. Select the storage tier you want to expand or create.
  - b. To create a storage tier, configure the RAID policy and in **Capacity**, enter the capacity of the storage tier.



Modify Capacity: StoragePool003

Operation: Expand capacity

Please select a storage tier and enter the added capacity.

Expand High Performance Tier (SSD)

Create Performance Tier (SAS)

RAID Policy: RAID 5 4D+1P

\* Capacity: 10 TB

Limit on Max. Capacity: 32.288 TB

Create Capacity Tier (NL-SAS)

Total Added Capacity: 10.000 TB

Total Capacity After Expansion: 11.000 TB

Set SmartTier Policy Advanced

**Table 6-18** Storage tier parameters

Parameter	Description	Setting
RAID Policy	<p>RAID level. The system supports RAID 0, RAID 1, RAID 10, RAID 3, RAID 5, RAID 50, and RAID 6.</p> <p><b>NOTE</b>                      RAID 0 only supports configuration in CLI mode. For details, see the <i>Command Reference</i> of the corresponding product model.</p>	<p>Select a RAID policy based on the planned solution.</p> <p>The default RAID policy of a storage tier varies with the number of disks allocated to the storage tier.</p> <ul style="list-style-type: none"> <li>■ If the number of disks allocated to a storage tier is smaller than 10:                             <ul style="list-style-type: none"> <li>○ Default RAID policy of the high performance tier: RAID 10</li> <li>○ Default RAID policy of the performance tier: RAID 5 (4D+1P)</li> <li>○ Default RAID policy of the capacity tier: RAID 6 (4D+2P)</li> </ul> </li> <li>■ If the number of disks allocated to a storage tier is equal to 10:                             <ul style="list-style-type: none"> <li>○ Default RAID policy of the high performance tier: RAID 10</li> <li>○ Default RAID policy of the performance tier: RAID 5 (8D+1P)</li> <li>○ Default RAID policy of the capacity tier: RAID 6 (4D+2P)</li> </ul> </li> <li>■ If the number of disks allocated to a storage tier is greater than 10:                             <ul style="list-style-type: none"> <li>○ Default RAID policy of the high</li> </ul> </li> </ul>

Parameter	Description	Setting
		performance tier: RAID 10 ○ Default RAID policy of the performance tier: RAID 5 (8D+1P) ○ Default RAID policy of the capacity tier: RAID 6 (8D+2P) <b>NOTE</b> If the number of SSDs in a disk domain is two or three, you are advised to configure the corresponding high-performance tier to RAID 1 (2D).
Capacity	The capacity that the storage tier provides for the storage pool. Two capacity levels are provided: TB, GB. <b>NOTE</b> Select <b>Use all available capacity</b> , and then you can allocate all available capacity in this storage layer to the storage pool you want to expand.	The capacity must be not larger than the available capacity of the storage tier.

- c. To expand a storage tier, in **Added Capacity**, enter the added capacity of the storage tier.

The screenshot shows a dialog box titled "Modify Capacity: StoragePool003". The "Operation" dropdown is set to "Expand capacity". Below this, a message says "Please select a storage tier and enter the added capacity." There are three options: "Expand High Performance Tier (SSD)" (checked), "Create Performance Tier (SAS)" (unchecked), and "Create Capacity Tier (NL-SAS)" (unchecked). For the selected option, the RAID Policy is "RAID 10 (2D+2D)" and the Current Capacity is "1.000 TB". The "Added Capacity" is set to "10" TB, with a "Max. Added Capacity" of "21.174 TB". At the bottom, it shows "Total Added Capacity: 10.000 TB" and "Total Capacity After Expansion: 11.000 TB". There are two buttons: "Set SmartTier Policy" and "Advanced".

- Reduce the capacity of a storage pool.
  - a. Select the storage tier you want to reduce.
  - b. In **Reduction Capacity**, enter the capacity of the storage tier to be reduced.

The screenshot shows a dialog box titled "Modify Capacity: StoragePool003". The "Operation" dropdown is set to "Reduce capacity". Below this, a message says "Select a storage tier and enter the capacity that you want to reduce." The selected option is "Capacity Reduction High Performance Tier (SSD)". The RAID Policy is "RAID 10 (2D+2D)" and the Current Capacity is "1.000 TB". The "Reduction Capacity" is set to "10" GB, with a "Max. capacity for reduction" of "1023.000 GB". At the bottom, it shows "Reduced Capacity: 10.000 GB" and "Total Capacity After Reduction: 1014.000 GB". There is one button: "Advanced".

**NOTE**

- You can create a new storage tier or expand the existing storage tier to expand storage pools.
- You can configure RAID policy only for new created storage tier. For the storage tier already exists in the storage pool, you cannot modify its RAID policy.
- The number of RAID data disks of different storage pool tiers must be a multiple of 1, 2, 4, or 8.

**Step 5 Optional:** If there are multiple storage tiers, you are advised to set a SmartTier policy. The policy enables data to migrate among different types of disks, optimizing storage performance distribution. [Table 6-19](#) lists SmartTier policies of a storage pool.

**Table 6-19** SmartTier policy of the storage pool

Parameter	Description	Setting
Service Monitoring Period	<p>Period of time during which the service is monitored and hotspot statistics is collected after you select <b>Enable I/O monitoring</b>. The statistics serves as guidance for data to migrate among different storage tiers.</p> <p>You can specify the period by setting days, <b>Start Time</b>, and <b>Duration</b>.</p>	<p>[Default value]  <b>I/O monitoring disabled</b></p>
Data Migration Plan	<p>The trigger policy of data relocation between the storage layers in a storage pool. The policies include:</p> <ul style="list-style-type: none"> <li>● <b>Manual:</b> You must manually trigger the data relocation among storage tiers. The data relocation process is transparent to application servers. Manual data relocation can be performed anytime.</li> <li>● <b>Periodical:</b> You must specify the start time and duration of data relocation for the storage system to perform data relocation automatically at the specified time. This reduces the management cost and complexity. The data relocation process is transparent to application servers. Automatic data relocation is performed only at the specified time.</li> </ul>	<p>[Default value]  <b>Manual</b></p>

 **NOTE**

- If **Data Migration Plan** is set to **Periodical**, I/Os are monitored on a 7x24 basis by default.
- SmartTier policy is only applicable when **Usage** of a storage pool is configured as **Block Storage Service**.
- If the remaining capacity in a storage pool is equal to or smaller than 10% of the total capacity, data does not migrate in the storage pool.

**Step 6 Optional:** If there are multiple storage tiers, click **Advanced** to set the stripe depth.

Click **Advanced**, The **Modify Capacity** dialog box is displayed. [Table 6-20](#) lists related parameters.

**Table 6-20** Modify Capacity

Parameter	Description	Setting
Strip Depth	<p>Strip refers to continuous data that is divided into data blocks of the same size and data blocks are distributed on different disks of storage devices. In this way, I/O loads are balanced among disks, improving read/write performance.</p> <p>Strip depth refers to strip size, indicating the size of data blocks on each disk. Smaller strip size indicates smaller data blocks. These data blocks are distributed on more disks, improving transmission performance. However, more time is required to find different data blocks, decreasing disk locating performance. On the contrary, fewer data blocks indicate lower transmission performance but higher disk locating performance.</p> <p>The value of this parameter can be:</p> <ul style="list-style-type: none"> <li>● System auto select The system selects the optimal strip depth based on the RAID policy of the storage tier and data migration granularity.</li> <li>● 32 KB</li> <li>● 64 KB</li> <li>● 128 KB 128 KB is recommended for random read/write services (such as in database scenarios).</li> <li>● 256 KB</li> <li>● 512KB 512 KB is recommended for sequential read/write services (such as media asset scenarios)</li> </ul>	<p>[Default value] System auto select</p>

Parameter	Description	Setting
	<b>NOTE</b> The parameter value cannot be changed after being determined.	

**Step 7** Confirm the capacity modification of the storage pool.

1. Click **OK**.  
The security alert dialog box is displayed.
2. Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation..**
3. Click **OK**.  
The **Execution Result** dialog box is displayed indicating that the operation succeeded.
4. Click **Close**.

---End

## 6.5.8 Deleting a Storage Pool

This operation enables you to delete an unwanted storage pool.

### Prerequisites

Before deleting a storage pool, ensure that LUNs in the storage pool have been deleted.

### Procedure

**Step 1** Log in to DeviceManager.

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

**Step 3** Delete a storage pool.

1. Select the storage pool you want to delete and click **Delete**.  
The security alert dialog box is displayed.
2. Click **OK**.  
The **Success** dialog box is displayed, indicating that the operation succeeded.
3. Click **OK**.

---End

## 6.6 Managing LUNs

LUNs are provided by a storage system to enable the application servers to make full use of the storage resources.

### 6.6.1 Viewing LUN Information

This operation enables you to view the information about all the LUNs on a storage system.



## Prerequisites

At least one LUN has been created on the storage system.

## Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **LUN**.

**Step 3** View information about the LUNs in the list. [Table 6-21](#) describes related parameters.









Name	ID	Health	Running Status	Type	Use Type	Capacity	Sectors	Capaci...	Ownin...	Mapping	Data P...	WWN	Remot...	Ownin...	Smart...	Masqu...
LUN001	1	Normal	Online	thick LUN	Internal	1,000 GB	2097152	1,187 GB	Storage...	Unmap...		68038b...	--	CTED A	No relo...	--
LUN002	2	Normal	Online	thick LUN	Internal	1,000 GB	2097152	1,187 GB	Storage...	Unmap...		68038b...	--	CTED B	No relo...	--

**Table 6-21** LUN parameters

Parameter	Description	Setting
Name	Name of a LUN.	[Example] LUN001
ID	ID of a LUN.	[Example] 1
Health Status	Indicates whether a LUN is normal.	[Example] Normal
Running Status	Running status of a LUN.	[Example] Online
Type	Type of a LUN. The types include: <ul style="list-style-type: none"> <li>● thick LUN</li> <li>● thin LUN</li> </ul>	[Example] thick LUN

Parameter	Description	Setting
Use Type	<p>Use type of a LUN. The use types include:</p> <ul style="list-style-type: none"> <li>● <b>Internal:</b> Common LUN created in local storage device.</li> <li>● <b>External:</b> eDevLUN created for taking over LUN in remote storage device.</li> <li>● <b>PE LUN:</b> PE (Protocol Endpoint) LUN is applied for VVol LUN in VMware software defined storage only. PE is used as an I/O demultiplexer to simplify the connection between VMs and VVol LUNs. When there is a VM operation I/O, I/O is sent to the corresponding VVol LUN through PE LUN.</li> <li>● <b>VVol LUN:</b> provides storage space for VMware VMs.</li> </ul>	<p>[Example] Internal</p>
Capacity	Capacity of a LUN. A user specifies the capacity when creating a LUN.	<p>[Example] 1.000 GB</p>
Sectors	Number of the sectors in a LUN.	<p>[Example] 2097152</p>
Capacity Allocated	Storage pool capacity allocated to a LUN. The capacity includes the data capacity and metadata capacity of the LUN (excluding data protection capacity). The metadata capacity occupies about 1% of the LUN data capacity and LUN data protection capacity.	<p>[Example] 1.187 GB</p>
Owning Storage Pool	Storage pool to which a LUN belongs.	<p>[Example] storagepool1</p>

Parameter	Description	Setting
Mapping	Mapping status of a LUN, indicating a LUN is mapped to a host or not.	[Example] Unmapped
Data Protection	Data protection method of a LUN. The protection methods include: <ul style="list-style-type: none"> <li>●  Snapshot</li> <li>●  Remote Replication</li> <li>●  Clone</li> <li>●  LUN Copy</li> <li>●  HyperMirror</li> <li>●  HyperMetro</li> </ul>	[Example] Clone
WWN	WWN of a LUN.	[Example] 60022a1100037eca45ae3b6 100000019
Remote WWN	WWN of a remote LUN.	[Example] —
Takeover LUN WWN	WWN of the eDevLUN after takeover.	[Example] —
Owning Controller	The controller that owns the LUN. <b>NOTE</b> <ul style="list-style-type: none"> <li>● This parameter may not be displayed due to a configuration difference for a particular scene.</li> <li>● This parameter applies only to V3R6C00.</li> </ul>	[Example] CTE0.A

Parameter	Description	Setting
SmartTier Policy	<p>The data migration policies include:</p> <ul style="list-style-type: none"> <li>● Automatic relocation                      Automatically relocate data based on the ranking order of data blocks and activity levels of LUNs in a storage pool. Automatic relocation relies on the analysis result from the I/O monitoring. Thus I/O monitoring must be enabled and the service monitoring period must be set before automatic relocation.</li> <li>● Relocation to high-performance tier                      The relocation to high-performance tier policy is recommended for the applications (such as OLTP databases) sensitive to response time, IOPS, and bandwidth. This policy preferentially promotes data blocks to the high performance tier and the performance tier. If the capacity of the data blocks to be relocated is larger than the capacity of the high performance tier (or performance tier), only data blocks with the most activities are promoted to the high performance tier (or the performance tier).</li> <li>● Relocation to low-performance tier                      The relocation to low-performance tier policy is recommended for applications (such as file sharing) insensitive to</li> </ul>	<p>[Example]                      Automatic relocation</p>

Parameter	Description	Setting
	<p>performance requirements. This policy preferentially demotes data blocks to the performance tier and the capacity tier, regardless of the activity levels of these data blocks.</p> <ul style="list-style-type: none"> <li>● No relocation</li> </ul> <p>The no relocation policy does not relocate data blocks among storage tiers, and data can be relocated only when the data relocation policy is changed.</p>	
Masquerading Status	<p>Masquerading status can be:</p> <ul style="list-style-type: none"> <li>● No Masquerading</li> <li>● Basic Masquerading Applies to eDevLUNs, used for replacing the basic LUN information such as VID, PID, and LUN WWN.</li> <li>● Extended Masquerading Applies to eDevLUNs, used for replacing the basic LUN information and extended LUN information such as SCSI protocol version, owning controller, and working controller.</li> <li>● Inherited Masquerading Applies to local LUNs, used for inheriting the remote LUN information such as VID, PID, and SCSI protocol version.</li> <li>● Third-party Applies to eDevLUNs, used for taking over heterogeneous storage systems from third-party vendors online.</li> </ul>	<p>[Example] No Masquerading</p>

Parameter	Description	Setting
vStore Name	Name of the vStore where the LUN belongs.	[Example] —
vStore ID	ID of the vStore where the LUN belongs.	[Example] —

----End

## 6.6.2 Viewing Owing LUN Group Information

This operation enables you to view information about a LUN's owning LUN group.

### Prerequisites

A LUN has been created and added to a LUN group.

### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **LUN**.

**Step 3** Select the LUN whose properties you want to view and click **Properties**.  
The **Properties of LUN** dialog box is displayed.

**Step 4** View information about an owning LUN group.

1. In the **Properties of LUN** dialog box, click the **Owning LUN Group** tab.
2. View information about an owning LUN group. [Table 6-22](#) describes related parameters.

**Table 6-22** Owning LUN group parameters

Parameter	Description	Setting
Name	Name of an owning LUN group.	[Example] LUNgroup001
ID	ID of an owning LUN group.	[Example] 233
Total Capacity of LUNs	Total capacity of all LUNs in LUN groups, excluding snapshot capacity.	[Example] 682.000GB

----End

## 6.6.3 Modifying the General Properties of a LUN

This operation enables you to view or modify the general properties of a LUN.

## Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **LUN**.

**Step 3** Select the LUN that you want to view or modify and click **Properties**.  
The **Properties of LUN** dialog box is displayed.

**Step 4** Modify the general properties of the LUN.

1. In the **Properties of LUN** dialog box, click the **General** tab.
2. In the **Name** text box, enter a new name for the LUN.

 **NOTE**

Name a LUN in accordance with the following rules so that the LUN is available to host applications.

- The name must be unique.
  - The name can contain only letters, digits, periods (.), underscores (\_), and hyphens (-).
  - The value contains 1 to 31 characters.
3. **Optional:** In the **Description** text box, describe the LUN.

**Step 5** Confirm your operation.

1. Click **OK**.  
The **Execution Result** dialog box is displayed, indicating that the operation succeeded.
2. Click **Close**.

---End

## 6.6.4 Modifying the Advanced Properties of a LUN

This operation enables you to configure the prefetch policy and cache policy of a LUN.

### Prerequisites

At least one LUN has been created on the storage system.

## Procedure

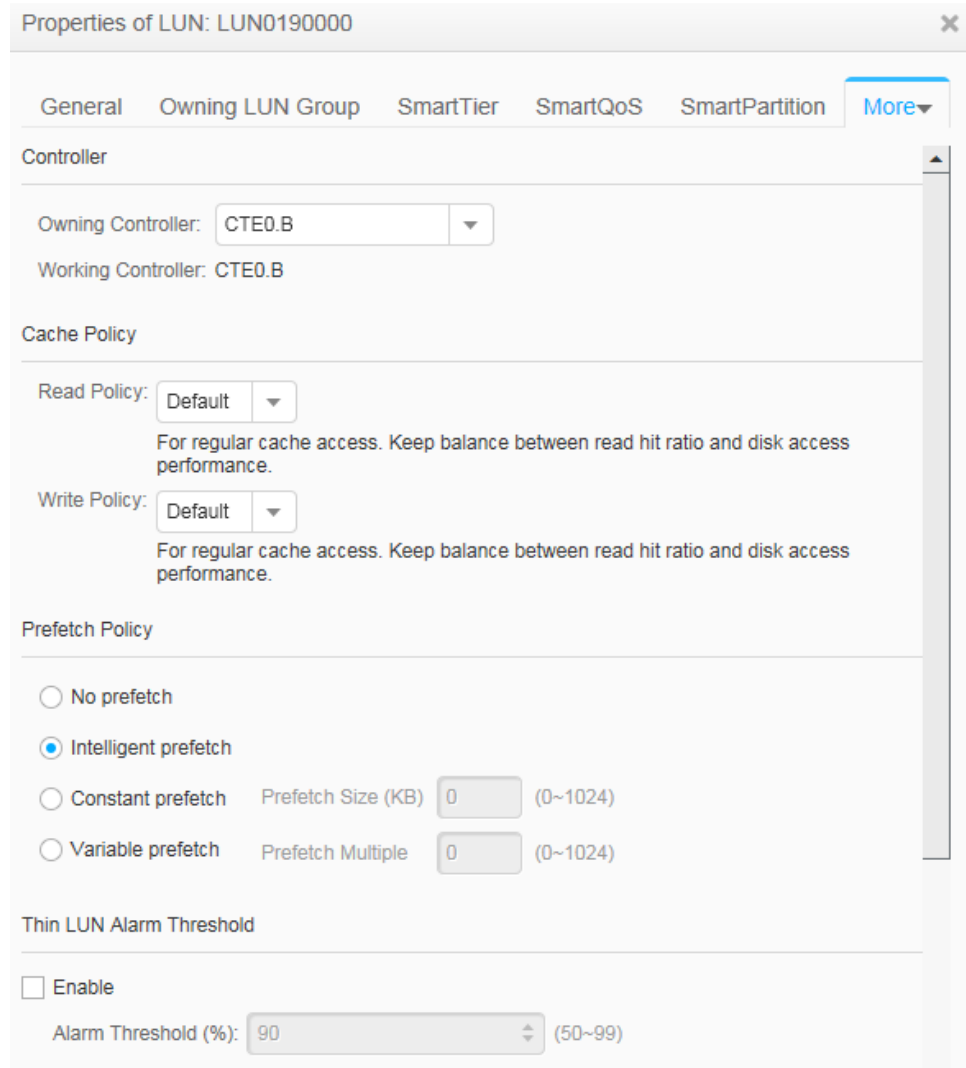
**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **LUN**.

**Step 3** Select the LUN whose properties you want to modify and click **Properties**.  
The **Properties of LUN** dialog box is displayed.

**Step 4** Configure the advanced properties of the LUN.

1. Click the **More > Advanced**.
2. Configure the advanced properties of the LUN. [Table 6-23](#) lists related parameters.



**Table 6-23** Advanced properties of the LUN parameters

Parameter	Description	Setting
Owning Controller	Owning controller of a LUN. You are advised to allocate LUNs to both controllers for load balancing.	If you are not sure about the owning controller, select <b>Auto select</b> . The storage system will automatically select the owning controller for the LUN. [Example] <b>Auto select</b>



Parameter	Description	Setting
Working Controller	Working controller of a LUN. Controller that is used to process read/write requests of LUNs and provide services. Only the working controller can process I/Os on LUNs. If hosts send I/Os to a non-working controller, the I/Os are forwarded to the working controller for processing.	[Example] <b>XXX0.B</b>
Read Policy	Data read policy of a cache. The system supports the following read policies. <ul style="list-style-type: none"> <li>- <b>Resident:</b> For random cache access. Data is retained in cache the longest to improve the read hit ratio.</li> <li>- <b>Default:</b> For regular cache access. Keep balance between read hit ratio and disk access performance.</li> <li>- <b>Recycle:</b> For sequential cache access. The idle cache resources are released for other access requests.</li> </ul>	[Example] Recycle [Default value] Default
Write Policy	Data write policy of a cache. The system supports the following write policies. <ul style="list-style-type: none"> <li>- <b>Resident:</b> For random cache access. Data is retained in cache the longest to improve the write hit ratio.</li> <li>- <b>Default:</b> For regular cache access. Keep balance between write hit ratio and disk access performance.</li> <li>- <b>Recycle:</b> For sequential cache access. The idle cache resources are released for other access requests.</li> </ul>	[Example] Recycle [Default value] Default

Parameter	Description	Setting
Prefetch Policy	<p>Data read mode of a LUN. Before reading data from a LUN, the storage system reads the data from the hard disks to the cache based on the preset policy. The policies include:</p> <ul style="list-style-type: none"> <li>- No prefetch: The storage system reads data based on the read length specified in the I/O request. As a low read hit ratio may lead to performance degradation, <b>No prefetch</b> is recommended for random read services.</li> <li>- Intelligent prefetch: Smart prefetch analyzes whether the requested data is sequential. If it is, the data following the currently requested data is prefetched from hard disks to the cache to improve the cache hit ratio. If they are not, the data is read directly from hard disks.</li> <li>- Constant prefetch: A constant length of data (user-definable, ranging from 0 to 1024 KB) is read from hard disks every time when the cache reads data from the disks.</li> <li>- Variable prefetch: The cache reads data from disks based on a multiple (user-definable, ranging from 0 to 1024) of the read length specified in the I/O request.</li> </ul>	<p>[Example]                      Intelligent prefetch</p>

Parameter	Description	Setting
Thin LUN Alarm Threshold	<p>This parameter is only valid when the selected LUN is a thin LUN and the operating system of the application server that owns the LUN is <b>Windows Server 2012</b>.</p> <p>Once this parameter is enabled, the application server will receive a threshold alarm when the ratio of the used capacity to total capacity of the LUN exceeds the configured <b>Alarm Threshold (%)</b>.</p>	<p>[Value range] 50 to 99</p> <p>[Default value] 90</p>
LUN Write Policy	<p>The LUN write policy can be:</p> <ul style="list-style-type: none"> <li>- <b>Write back</b>: Data is written onto the cache. The cache schedules the data and writes the data to disks.</li> <li>- <b>Write through</b>: Data is directly written onto disks without passing the cache.</li> </ul> <p><b>NOTE</b> Writing data onto the cache is fast. Therefore, write back delivers better write performance than write through.</p>	<p>[Example] Write back</p> <p>[Default value]</p> <ul style="list-style-type: none"> <li>- The default value of eDevLUN is write through.</li> <li>- The default value of local LUN is write back.</li> </ul> <p><b>NOTE</b> After a masqueraded eDevLUN created, you cannot modify its LUN write policy. You can modify the policy after you manually take over the masqueraded eDevLUN through CLI.</p>

Parameter	Description	Setting
Masquerading	<p>Masquerading replaces identification information of the LUN on local device with that on heterogeneous remote device so that heterogeneous remote LUNs can take over online.</p> <p>Masquerading types can be:</p> <ul style="list-style-type: none"> <li>- <b>No masquerading</b></li> <li>- <b>Basic masquerading</b>                      Applies to eDevLUNs, used for replacing the basic LUN information such as VID, PID, and LUN WWN.</li> <li>- <b>Extended masquerading</b>                      Applies to eDevLUNs, used for replacing the basic LUN information and extended LUN information such as SCSI protocol version, owning controller, and working controller.</li> <li>- <b>Inherited masquerading</b>                      Applies to local LUNs, used for inheriting remote LUN information such as VID, PID, and SCSI protocol version.</li> <li>- <b>Third-party</b>                      Applies to eDevLUNs, used for taking over heterogeneous storage systems from third-party vendors online.</li> </ul>	<p>[Example]</p> <p>Inherited masquerading</p> <p>[Default value]</p> <p>No masquerading</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>- If you select <b>Inherited masquerading</b>, <b>Remote Device</b> must be specified.</li> <li>- The masquerading type of LUNs that have been mapped to hosts cannot be changed.</li> <li>- If you want to change the masquerading type, change the current masquerading type to <b>No masquerading</b> and change the type.</li> </ul>
Takeover LUN WWN	WWN of the eDevLUN after takeover.	<p>[Example]</p> <p>—</p>

**Step 5** Confirm the configuration of the advanced properties of a LUN.

1. Click **OK**.

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

2. Click **Close**.

----**End**

## 6.6.5 Expanding a LUN on a Storage System

This operation enables you expand the capacity of a LUN to meet service requirements.

### Prerequisites

- The storage system has at least one formatted LUN.
- You cannot expand LUNs for which Snapshot, Remote Replication, Clone, LUN Copy, SmartMigration, HyperMetro, or HyperMirror has been configured.

### Precautions

To ensure data integrity, stop services on the LUN before LUN expansion.

When LUNs of different types are expanded, the capacity that can be expanded is restricted. Specific conditions are as follows:

- The capacity of a thin LUN is restricted by its specifications but not confined to the remaining capacity of the storage pool.
- The capacity of a thick LUN is restricted by its specifications. It cannot be larger than the remaining capacity of the storage pool.

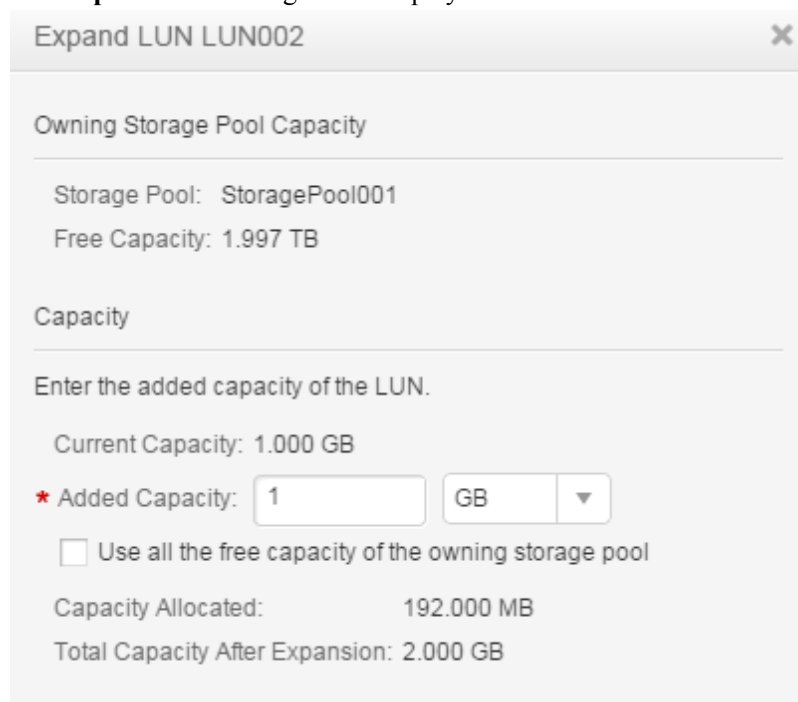
Rescan for the LUN on the server side after the capacity expansion.

### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **LUN**.

**Step 3** Select the LUN that you want to expand and click **Expand**.  
The **Expand LUN** dialog box is displayed.



Expand LUN LUN002

Owning Storage Pool Capacity

Storage Pool: StoragePool001  
Free Capacity: 1.997 TB

Capacity

Enter the added capacity of the LUN.

Current Capacity: 1.000 GB

\* Added Capacity:

Use all the free capacity of the owning storage pool

Capacity Allocated: 192.000 MB  
Total Capacity After Expansion: 2.000 GB

**Step 4** Set the parameters for expanding the LUN.

1. In the **Added Capacity** text box, enter the added capacity of the LUN after expansion.

 **NOTE**

- The total capacity of the thick LUN after expansion must be smaller than the available capacity of the storage pool.
  - The total capacity of the thin LUN after expansion must be smaller than its specifications.
  - Alternatively, you can select **Use all the free capacity of the owning storage pool** to expand the LUN.
2. Select a capacity unit from the drop-down list on the right of **Added Capacity**. Possible values are **Blocks**, **MB**, **GB**, or **TB**.

**Step 5** Confirm the LUN expansion.

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

---End

## 6.6.6 Expanding a LUN on an Application Server

When a LUN's capacity is insufficient to meet service need, expand the LUN on its storage system. After that, configure the application server so that the application server can identify and use the expanded storage space.

### 6.6.6.1 Expanding a LUN on a Windows-Based Application Server

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-based application server as an administrator.

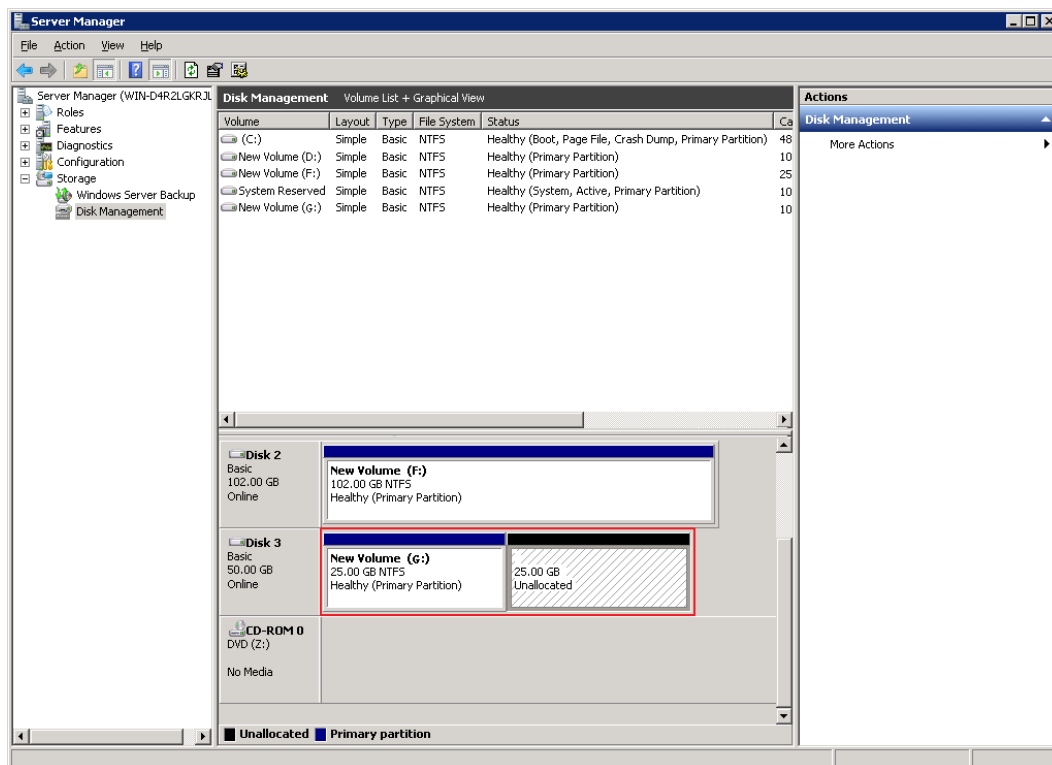
**Step 2** On the Windows desktop, click **Start** and choose **Administrative Tools > Server Manager** from the shortcut menu.

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 6-1**. On the right of disk G, the capacity of the partition to be expanded is displayed.

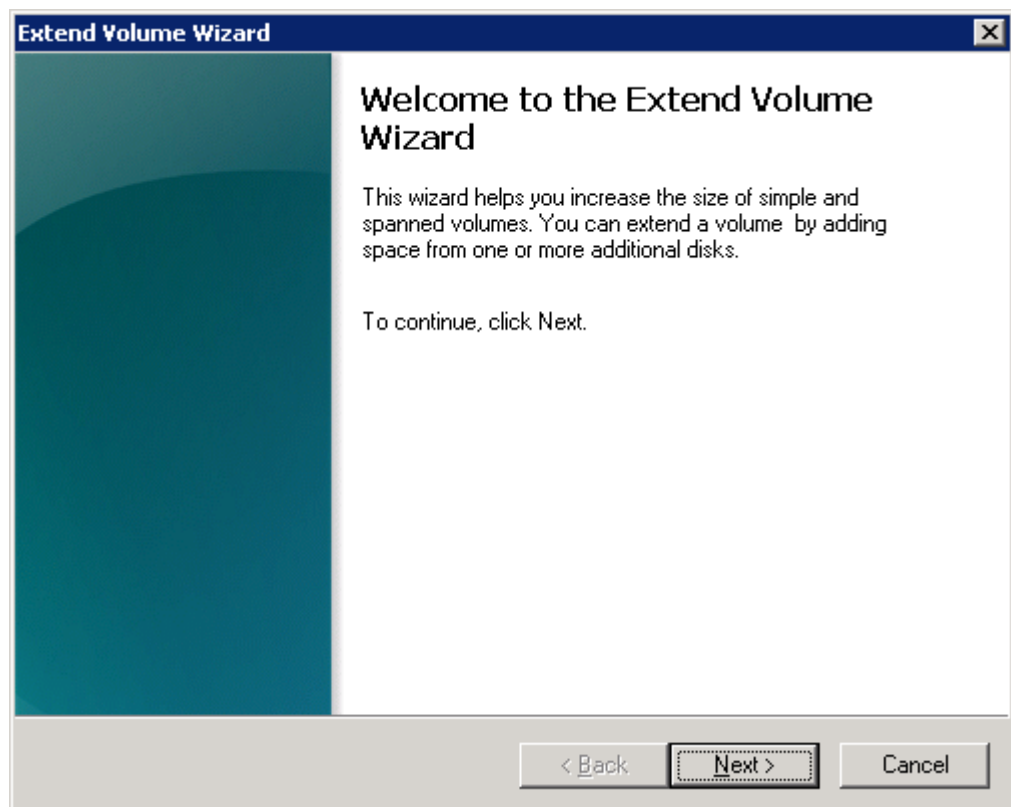
**Figure 6-1** Disk scanning result



**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 6-2**.

**Figure 6-2** Extend Volume Wizard

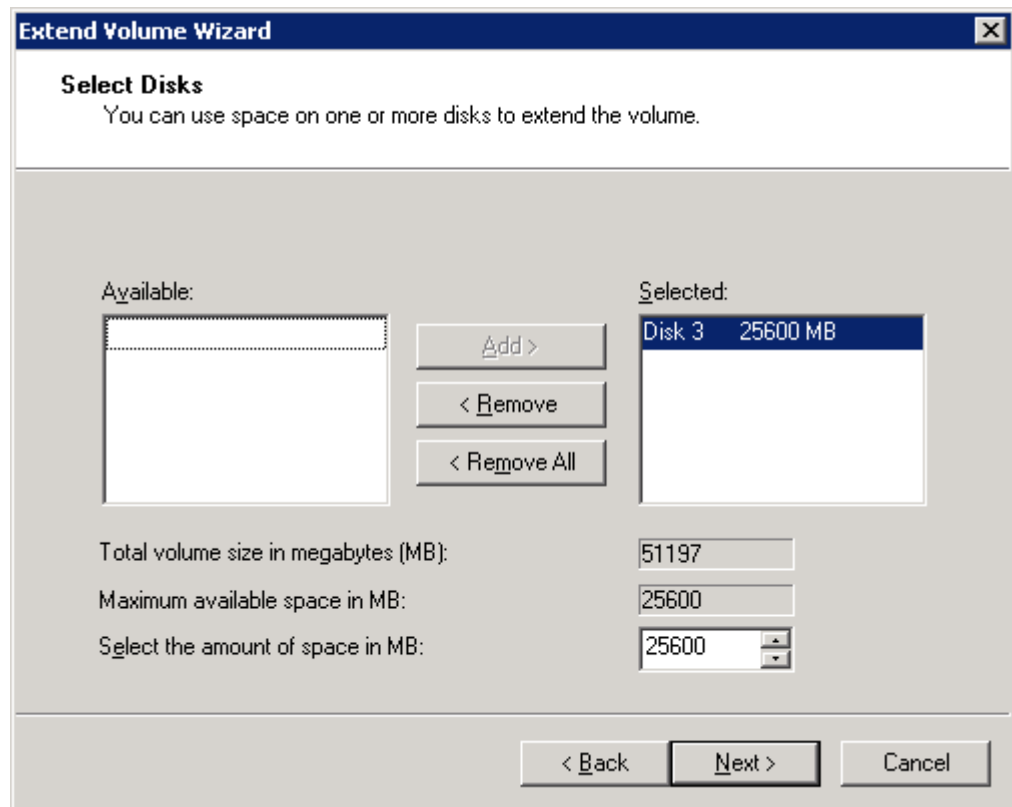


**Step 5** Click **Next**.

The **Select Disks** page is displayed, as shown in [Figure 6-3](#).



Figure 6-3 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**.

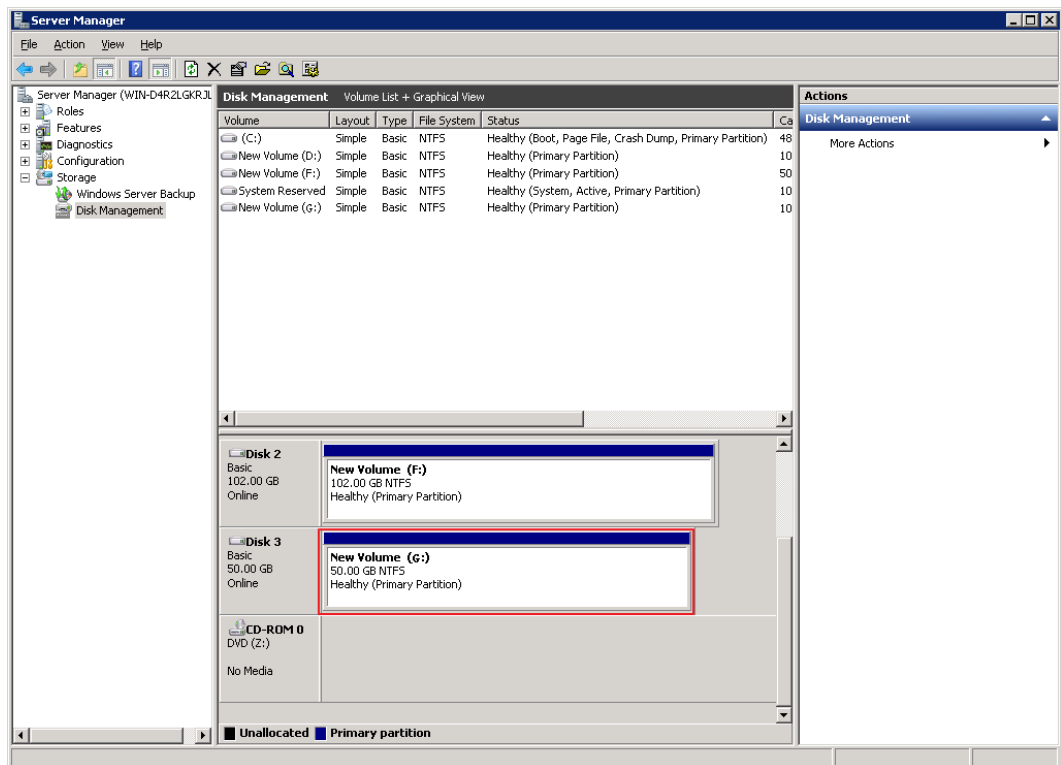
The **Server Manager** dialog box is displayed. You have completed configuring LUN expansion on the application server.

----**End**

## Result

In the **Server Manager** dialog box, view the capacity of disk G after expansion, as shown in [Figure 6-4](#).

Figure 6-4 Operation result



### 6.6.6.2 Expanding a LUN on a SUSE-Based Application Server

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**.

#### Procedure

**Step 1** Scan for disks on the SUSE-based 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** 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.

- ii. Run **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 **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

### 6.6.6.3 Expanding a LUN on a RedHat-Based Application Server

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 RedHat 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 RedHat-based 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 **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 **echo 1 > /sys/block/sdh/device/rescan** command to rescan for disks.

After the scanning is complete, the disk capacity becomes 50 GB.

### 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

### 6.6.6.4 Expanding a LUN on a Solaris-based Application Server

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. cl0t5d0 <drive type unknown>
    /pci@400/pci@2/pci@0/pci@a/SUNW,qlc@0/fp@0,0/ssd@w20080022a10bc14f,0
  3. cl0t5d1 <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 cl0t5d1
[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
swap                  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

### 6.6.6.5 Expanding a LUN on an AIX-based Application Server

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 example of the section, 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-based 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, 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 **cfgmgr -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 PPs per PV:      2032          MAX PVs:         64
LTG size (Dynamic):  256 kilobyte(s)  AUTO SYNC:       no
HOT SPARE:           no           BB POLICY:       relocatable
```

In the command output, pay attention to the **PP SIZE** parameter. 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
INTRA-POLICY:      middle                 UPPER BOUND:       128
MOUNT POINT:       /mnt/lv1              LABEL:             /mnt/lv1
MIRROR WRITE CONSISTENCY: on/ACTIVE
EACH LP COPY ON A SEPARATE PV ?: yes
Serialize IO ?:    NO
    
```

**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            +

```

- 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).

- After modifying the parameter, press **Enter**.

```

COMMAND STATUS

Command: OK          stdout: no          stderr: no

Before command completion, additional instructions may appear below.

```

- Press **Esc+0** to exit the logical volume configuration interface.

**Step 10** Expand the file system on the **lv1** logical volume.

- 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.

- Run **mount /mnt/lv1** to mount the file system again.

----End

### 6.6.6.6 Expanding a LUN on an HP-UX-based Application Server

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-based 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

### 6.6.6.7 Expanding a LUN on a VMware ESX-Based Application Server

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 this 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

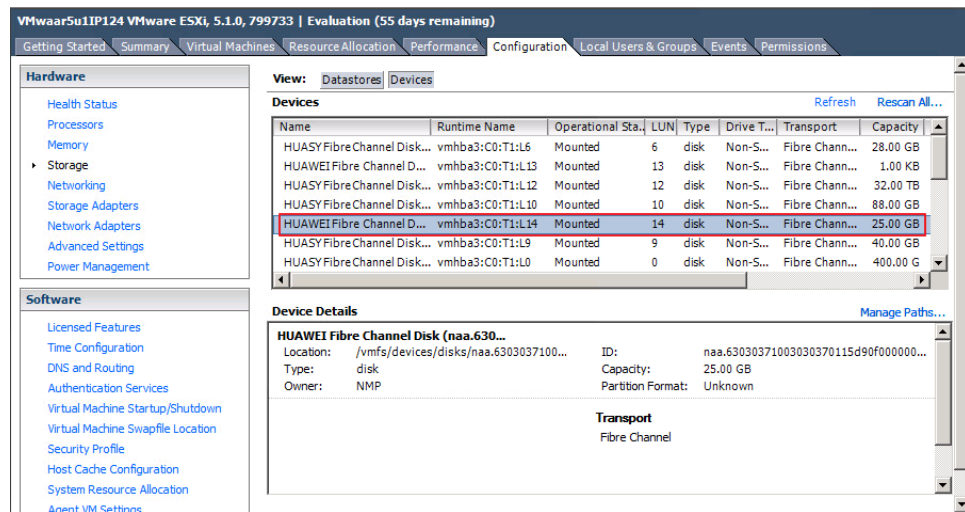
**Step 1** In vSphere Client, click the **Configuration** tab.

**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 6-5](#).

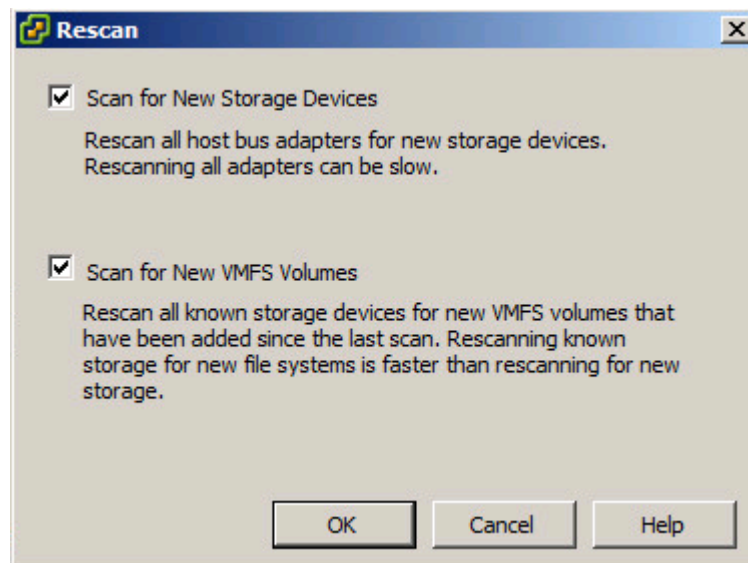
Figure 6-5 Device mapped from the LUN to be expanded on the application server



Step 4 On the **Devices** page, click **Rescan All**.

The **Rescan** dialog box is displayed, as shown in Figure 6-6.

Figure 6-6 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 6-7, the scanning is ongoing.

**Figure 6-7** Scanning ongoing

Name	Target	Status	Details	Initiated by	vCenter Server	Requested Start Time	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 6-8**, the scanning is completed.

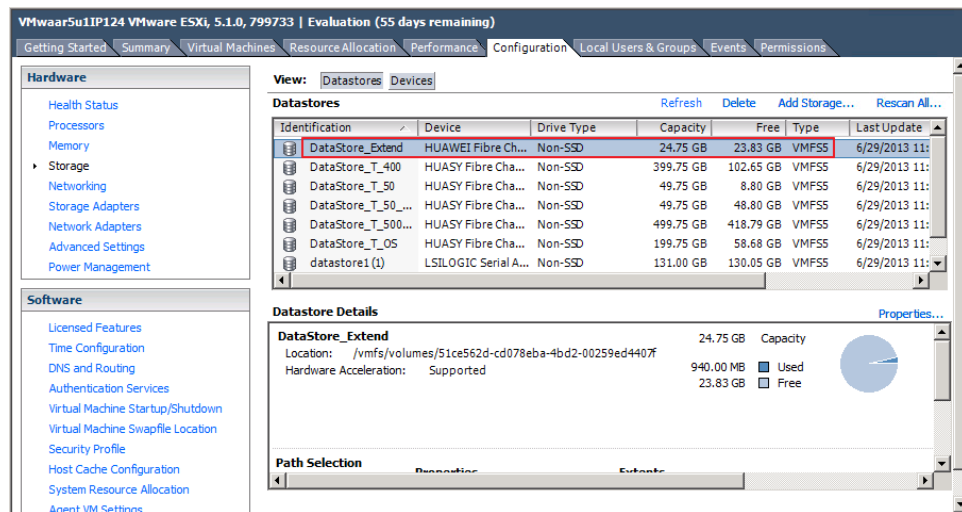
**Figure 6-8** Scanning completed

Name	Target	Status	Details	Initiated by	vCenter Server	Requested Start Time	Start Time	Completed Time
Rescan VMFS		Completed		Administrator	win232.zcyunhvs...	8/19/2013 6:47:46 PM	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...	

**Step 6** On the **Storage** page, click the **Datstores** tab.

On the **Datstores** page, view the datastore mapped from the LUN to be expanded on the application server, as shown in **Figure 6-9**.

**Figure 6-9** Device mapped from the LUN to be expanded on the application server

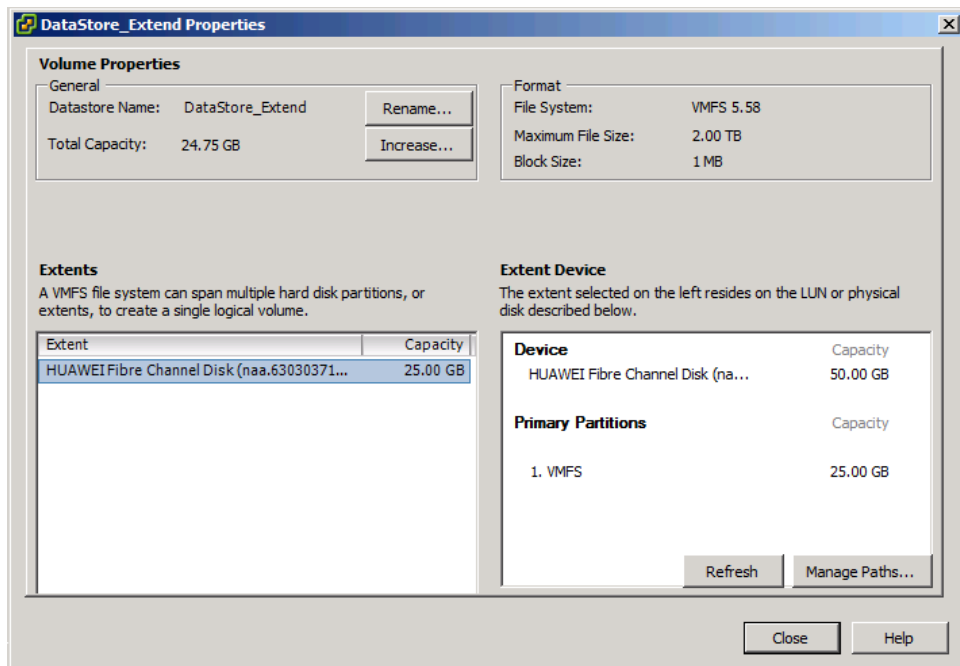


**Step 7** Right-click the datastore corresponding to the LUN to be expanded, and choose **Properties** from the shortcut menu.

The **DataStore\_Extend Properties** dialog box is displayed, as shown in **Figure 6-10**.



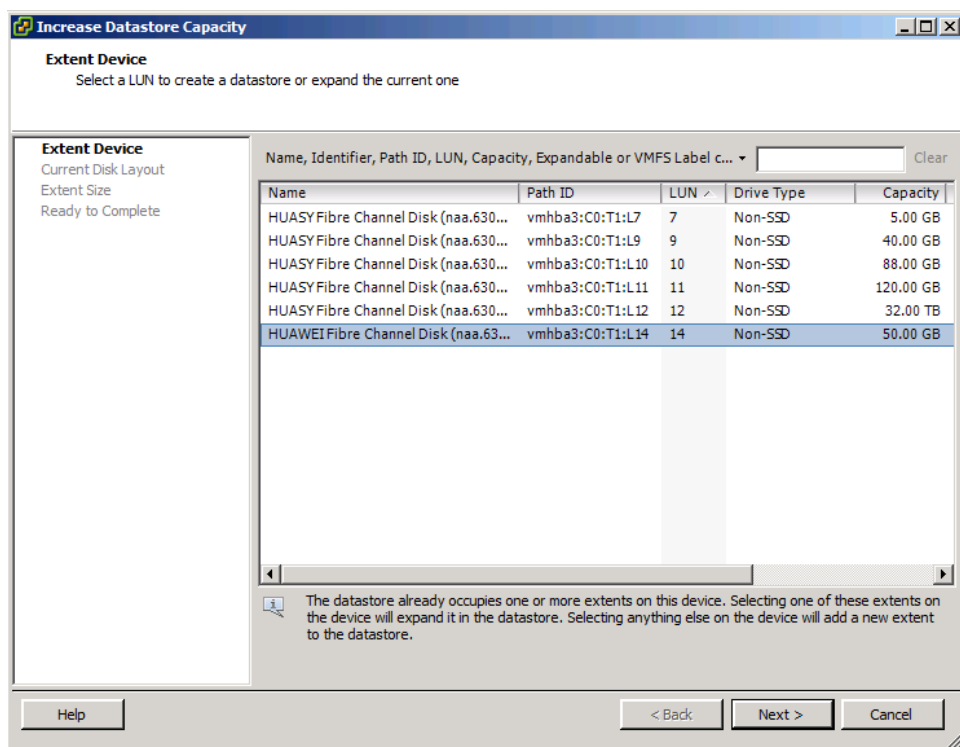
Figure 6-10 DataStore\_Extend Properties dialog box



**Step 8** In the **Volume Properties** area, click **Increase**.

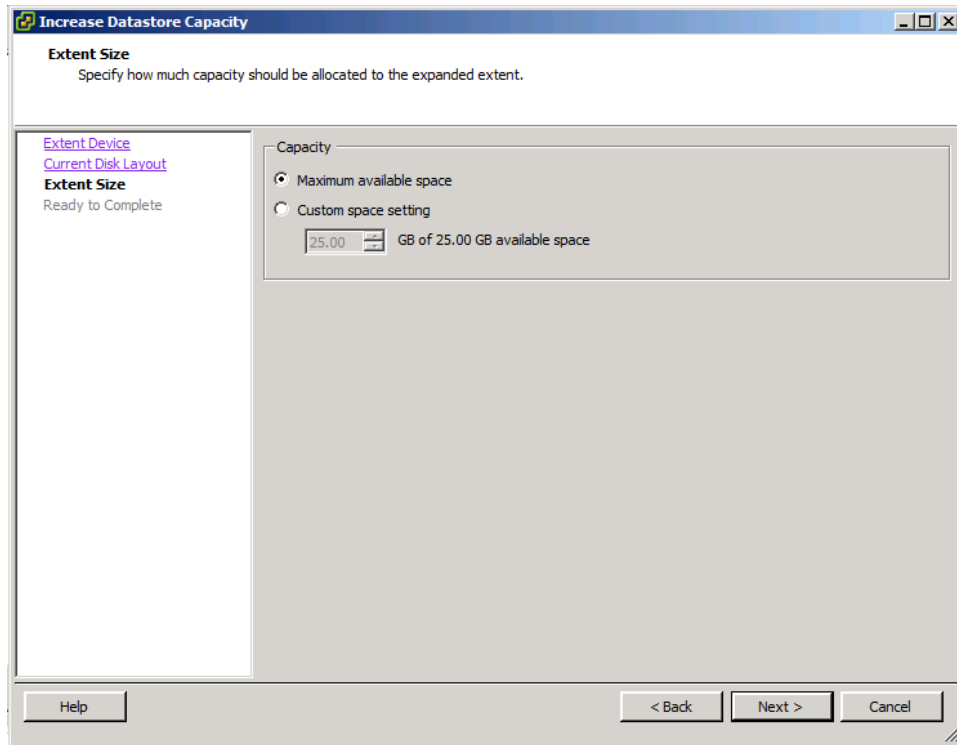
The **Increase Datastore Capacity** dialog box is displayed, as shown in [Figure 6-11](#).

Figure 6-11 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 6-12](#). Click **Next**.

**Figure 6-12** Setting the size of the expansion data area



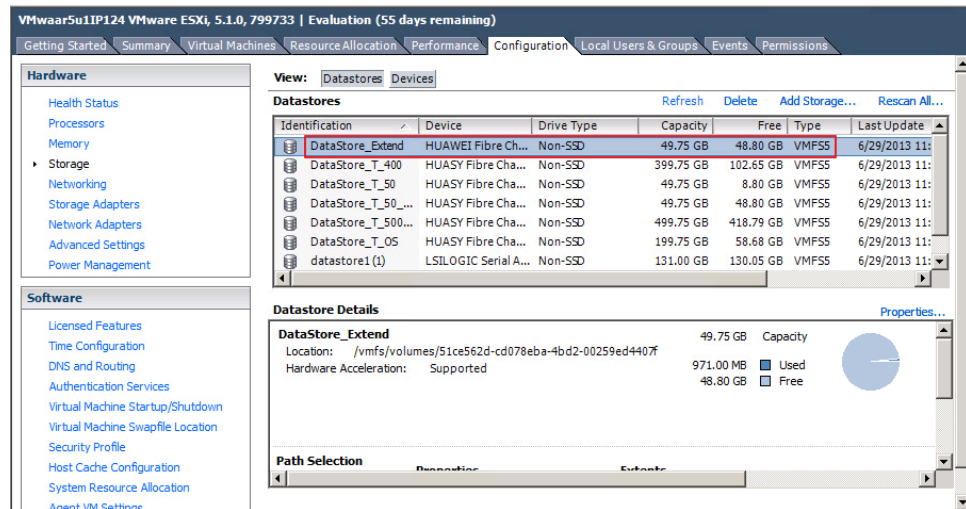
- Step 12** Click **Finish**.  
The **DataStore\_Extend Properties** dialog box is displayed.
- Step 13** Click **Close**.

----End

## Result

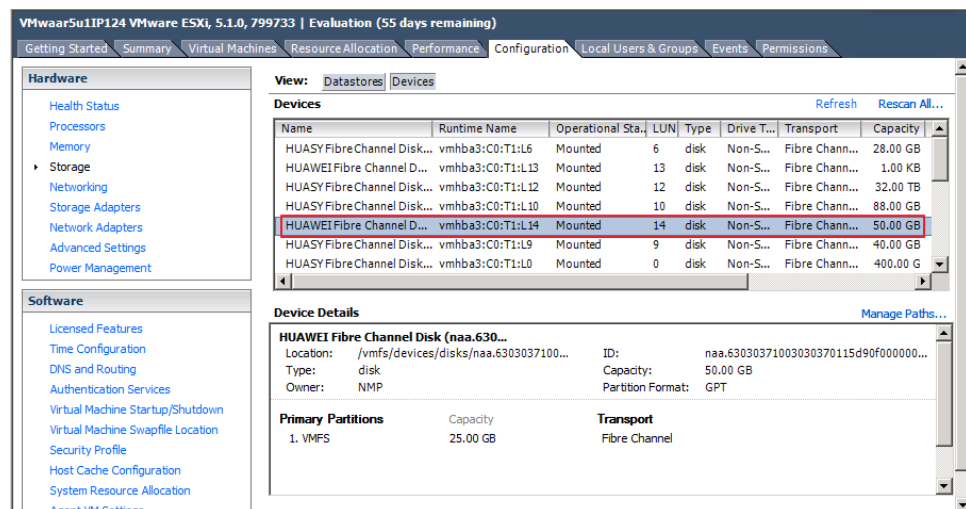
- On the **Datastores** tab of **Storage** page, view the expanded datastore, as shown in [Figure 6-13](#).

**Figure 6-13** 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 6-14**.

**Figure 6-14** Device mapped from the expanded LUN on the application server



## 6.6.7 Deleting a LUN

This operation enables you to remove unwanted objects to reclaim the storage resources.

### Prerequisites

- Services on the LUN have been stopped, no supported value-added functions on the LUN.
- The LUN is not added to any LUN group.

## Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **LUN**.

**Step 3** Select the LUN you want to delete and click **Delete**.  
The security alert dialog box is displayed.

**Step 4** Confirm the LUN deletion.

1. Carefully read the content of the dialog box. Then click the check box next to the statement **I have read and understand the consequences associated with performing this operation.** to confirm the information.
2. Click **OK**.  
The **Execution Result** dialog box is displayed, indicating that the operation succeeded.
3. Click **Close**.

---End

## Follow-up Procedure

After deleting a LUN, rescan for LUN information on the host to prevent the impact of residual LUN information on the host.

## 6.7 Managing LUN Groups

For easy management of multiple LUNs, logically add the LUNs to a LUN group.

### 6.7.1 Viewing LUN Group Information

This operation enables you to view basic information about all LUN groups.

## Prerequisites

At least one LUN group has been created.

## Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **LUN** > **LUN Group**.

**Step 3** In the function pane, view the LUN group information. [Table 6-24](#) describes related parameters.



Name	ID	Total LUN Capacity
LUNGroup001	1	2,000 GB

**Table 6-24** LUN group parameters

Parameter	Description	Setting
Name	Name of a LUN group.	[Example] <b>LUNgroup001</b>
ID	ID of a LUN group.	[Example] <b>1</b>
Total Capacity of LUNs	Total capacity of all LUNs in LUN groups, excluding snapshot capacity.	[Example] <b>2.000GB</b>

**Step 4** In the details area, information about the LUN or snapshot you have added is displayed.

----End

## 6.7.2 Modifying the General Properties of a LUN Group

This operation enables you to view or modify basic information about a LUN group.

### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **LUN** > **LUN Group**.

**Step 3** Select the LUN group that you want to modify and click **Properties**.  
The **Properties of LUN Group** dialog box is displayed.

**Step 4** Modify the general properties of LUN group.

1. In the **Properties of LUN Group** dialog box, click the **General** tab.
2. In the **Name** text box, enter a new name for the LUN group.

 **NOTE**

Name a LUN group in accordance with the following rules so that the LUN group is available to host applications.

- The name must be unique.
- The name can contain only letters, digits, periods (.), underscores (\_), and hyphens (-).
- The value contains 1 to 31 characters.

3. **Optional:** In the **Description** text box, describe the LUN group.

**Step 5** Confirm your operation.

1. Click **OK**.

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

2. Click **Close**.

----End

## 6.7.3 Viewing an Owing Mapping View of a LUN Group

This operation enables you to view information about the owing mapping view of a LUN group.

### Prerequisites

A LUN has been created and added to a LUN group.

### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **LUN** > **LUN Group**.

**Step 3** Select the LUN group you want to view and click **Properties**.  
The **Properties of LUN Group** dialog box is displayed.

**Step 4** View information about the owing mapping view of a host group.

1. In the **Properties of LUN Group** dialog box, click the **Owing Mapping View** tab.
2. View information about an owing mapping view. [Table 6-25](#) describes related parameters.

**Table 6-25** Owing mapping view parameters

Parameter	Description	Setting
Name	Name of an owing mapping view.	[Example] LUNmapping001
ID	ID of an owing mapping view.	[Example] 1

----End

## 6.7.4 Adding an Object

This operation enables you to add a LUN or snapshot for a LUN group to expand the LUN's storage space. A LUN group can be added with a maximum of 4096 LUNs. A LUN can be added to a maximum of 8 LUN groups.

### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **LUN** > **LUN Group**.

**Step 3** Select the LUN group you want to modify and click **Add Object**.  
The **Add Object** dialog box is displayed.

**Step 4** Select the LUN or snapshot you want to add to the LUN group.

 **NOTE**

To facilitate locating the LUN, select **Shows only the LUNs that do not belong to any LUN group** in the lower left corner of the dialog box.

**Step 5** Click  and add a LUN or snapshot to **Selected LUNs** or **Selected Snapshots**.

**Step 6** Confirm your operation.

1. Click **OK**.

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

2. Click **Close**.

----End

## 6.7.5 Removing Object

This operation enables you to remove a LUN or snapshot from a LUN group when the LUN or snapshot is not needed.

### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **LUN** > **LUN Group**.

**Step 3** Select the LUN group you want to modify and click **Remove Object**.

The **Remove Object** dialog box is displayed.

**Step 4** Select the LUN or snapshot you want to remove from the LUN group.

**Step 5** Click  and add a LUN or snapshot to **Selected LUNs** or **Selected Snapshots**.

**Step 6** Confirm the operation.

1. Click **OK**.

The security alert dialog box is displayed.

2. Carefully read the content in the dialog box. Then select **I have read and understand the consequences associated with performing this operation** for confirmation.

3. Click **OK**.

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

4. Click **Close**.

----End

## 6.7.6 Deleting a LUN Group

This operation enables you to delete a LUN group when it is not needed.

## Prerequisites

The LUN group to be deleted does not belong to any mapping view.

## Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **LUN** > **LUN Group**.

**Step 3** Select the LUN group you want to delete.

**Step 4** Delete the LUN group.

1. Click **Delete**.  
The security alert dialog box is displayed.
2. Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation**.
3. Click **OK**.  
The **Execution Result** dialog box is displayed, indicating that the operation succeeded.
4. Click **Close**.

---End

## 6.8 Managing Hosts

This function allows you to manage hosts so that the hosts can obtain and use the storage resources allocated by the storage system.

### 6.8.1 Viewing Host Information

This operation enables you to view the information about all the hosts.

## Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Host**.

**Step 3** View the information about the hosts in the list. [Table 6-26](#) describes related parameters.

**Table 6-26** Host parameters

Parameter	Description	Setting
Name	Name of a host.	[Example] host1
ID	ID of a host.	[Example] 1



Parameter	Description	Setting
Status	Status of a host.	[Example] Normal
OS	Operating system used by a host.	[Example] Windows
IP Address	IP address of a host.	[Example] 192.168.1.100
Added to Host Group	Whether a host is added to the host group.	[Example] Yes
Number of Initiators	The number of initiators that a host contains.	[Example] 1

**Step 4** Select a host and view the information of initiator, mapped LUN mapped snapshot or path in the lower part.



**Host LUN ID** indicates the identity mapped from the host system to the host's LUN or snapshot.

---End

## 6.8.2 Modifying Host Properties

This operation enables you to modify the general properties of a host.

### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Host**.

**Step 3** Select the host whose properties you want to modify and click **Properties**.  
The **Host Properties** dialog box is displayed.

The screenshot shows a dialog box titled "Properties of Host: Host001". It has two tabs: "General" (selected) and "Owning Host Group". The "General" tab contains the following fields:

- Name: Host001
- Description: (empty text box)
- ID: 0
- OS: Windows (dropdown menu)
- IP Address: 192.168.1.100
- Device Location: (empty text box)

**Step 4** Modify the general properties of the host.

1. Click **General** tab.
2. In the **Name** text box, enter a new name for the host.

 **NOTE**

Name a host in accordance with the following rules so that the host is available to host applications.

- The name must be unique.
- The name contains only letters, digits, periods (.), underscores (\_), and hyphens (-).
- The name contains 1 to 63 characters.

3. **Optional:** In the **Description** text box, enter new description for the host.
4. From the **OS** drop-down list, select an operating system for the host.
5. **Optional:** In the **IP address** text box, enter the IP address of the host.
6. **Optional:** In the **Location** text box, enter the location of the host.

**Step 5** Click **Owning Host Group** to view information about the host group that the host belongs to.

**Step 6** Confirm the modification of the host's general properties.

1. Click **OK**.  
The **Execution Result** dialog box is displayed indicating that the operation succeeded.
2. Click **Close**.

----End

## 6.8.3 Creating an Initiator

This operation enables you to create an initiator for a storage device. A host can be added with a maximum of 32 initiators.

## Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Host** > **Initiator**.

**Step 3** Click **Create**.

The **Create Initiator** dialog box is displayed.

**Step 4** In **Type**, select an initiator type.

 **NOTE**

The initiator types include:

- iSCSI
- FC
- IB
- vHBA

The vHBA initiator applies to some storage device models only and only the alias of the initiator can be changed.

**Step 5** Set the properties of the initiator based on the initiator type.

If you select FC or IB, the related parameters are shown in [Table 6-27](#).

**Table 6-27** FC or IB initiator parameter

Parameter	Description	Setting
WWPN	The unique identifier of an initiator.	[Example] 2000000743ab cdff
Alias	Alias of an initiator.	[Example] FC1_ALIAS
Uses third-party multipath software	<ul style="list-style-type: none"> <li>● This parameter is only available after the initiator is added to host successfully.</li> <li>● If LUNs have been mapped to the host before you enable or disable <b>Uses third-party multipath software</b>, restart the host after reconfiguration.</li> <li>● If the host has installed UltraPath, do not need to enable <b>Uses third-party multipath software</b>.</li> </ul>	[Example] Uses third-party multipath software

Parameter	Description	Setting
Switchover Mode	<p>Patch switchover mode. The system supports the following four modes:</p> <ul style="list-style-type: none"> <li>● <b>early-version ALUA:</b> This mode is selected when an earlier version is upgraded to the current version.                          Requirements:                         <ul style="list-style-type: none"> <li>- The storage system is upgraded from V300R003C10 and earlier to V300R003C20/V300R006C00SPC100 or later or from V300R005 to V300R006C00SPC100 and later.</li> <li>- Before the upgrade, the storage system has dual controllers and has enabled ALUA.</li> </ul> </li> <li>● <b>common ALUA:</b> This mode is selected when a storage system is in V300R003C20, V300R006C00SPC100 and later versions.                          Requirements:                         <ul style="list-style-type: none"> <li>- The storage system is in V300R003C20, V300R006C00SPC100 and later versions</li> <li>- The storage system has dual or multiple controllers.</li> <li>- The storage system connects to a host running SUSE, Red Hat 6.X, Windows Server 2012 (Emulex HBA), Windows Server 2008 (Emulex HBA), and HP-UX 11i V3.</li> </ul> </li> <li>● <b>ALUA not used:</b> This mode is selected when a host such as HP-UX 11i V2 does not support ALUA or the actual application scenario does not need ALUA.</li> <li>● <b>Special mode:</b> This mode is selected when a host is in V300R003C20, V300R006C00SPC100 and later versions and connects to a host running an operating system not supported by common ALUA.                          Requirements:                         <ul style="list-style-type: none"> <li>- The storage system is in V300R003C20, V300R006C00SPC100, and later versions</li> <li>- The storage system has dual or multiple controllers.</li> <li>- The storage system connects to a host running VMware, AIX, Red Hat 7.X, Windows Server 2012 (QLogic HBA), and Windows Server 2008 (Qlogic HBA).</li> </ul> </li> </ul> <p><b>NOTICE</b>                      When configuring the path switchover mode of an initiator, perform the operations with the guidance of Huawei technical support engineers and follow the requirements of relevant host connectivity guides. For example, <i>HUAWEI SAN Storage Host Connectivity Guide for Windows</i>.</p>	[Example] common ALUA

Parameter	Description	Setting
	<p><b>NOTE</b></p> <p>Asymmetric logical unit access (ALUA) is a multitarget port access model. In a multipathing state, the ALUA model provides a way of presenting active/passive LUNs to a host, and offers a port status switching interface to switch over the working controller. For example, when a host multipathing program supporting the ALUA detects a port status change on a controller that becomes faulty, the program will automatically switch subsequent I/Os to the other controller.</p>	
<p>Special mode type</p>	<p>The parameter applies to V300R003C20, V300R006C00SPC100, and later, and needs to be configured when you select <b>Special mode type</b> for <b>Switchover Mode</b>. The detailed requirements are as follows:</p> <ul style="list-style-type: none"> <li>● <b>Mode 0:</b> <ul style="list-style-type: none"> <li>- The host and storage system must be connected using a Fibre Channel network.</li> <li>- The OS of the host that connects to the storage system is Red Hat 7.X, Windows Server 2012 (using QLogic HBAs), or Windows Server 2008 (using QLogic HBAs).</li> </ul> </li> <li>● <b>Mode 1:</b> <ul style="list-style-type: none"> <li>- The OS of the host that connects to the storage system is AIX or VMware.</li> <li>- HyperMetro works in load balancing mode.</li> </ul> </li> <li>● <b>Mode 2:</b> <ul style="list-style-type: none"> <li>- The OS of the host that connects to the storage system is AIX or VMware.</li> <li>- HyperMetro works in local preferred mode.</li> </ul> </li> </ul> <p><b>NOTICE</b></p> <p>Perform the operations with the guidance of Huawei technical support engineers and follow the requirements of relevant host connectivity guides. For example, <i>HUAWEI SAN Storage Host Connectivity Guide for Windows</i>.</p>	<p>[Example]                      Mode 0</p>

Parameter	Description	Setting
Path Type	<p>The storage system supports two path switchover modes: <b>Optimal Path</b> and <b>Non-Optimal Path</b>.</p> <ul style="list-style-type: none"> <li>● When HyperMetro works in load balancing mode, set the <b>Path Type</b> for the initiators of both the local and remote storage arrays to <b>Optimal Path</b>. Enable ALUA on both the host and storage arrays. If the host uses the <b>round-robin</b> multipathing policy, it delivers I/Os to both storage arrays in round-robin mode.</li> <li>● When HyperMetro works in local preferred mode, set the <b>Path Type</b> for the initiator of the local storage array to <b>Optimal Path</b>, and that of the remote storage array to <b>Non-Optimal Path</b>. Enable ALUA on both the host and storage arrays. The host delivers I/Os to the local storage array preferentially.</li> </ul>	<p>[Example] Optimal Path</p>

If you select iSCSI, the related parameters are shown in [Table 6-28](#).

**Table 6-28** iSCSI initiator parameters

Parameter	Description	Setting
IQN	<p>iSCSI Qualified Name (IQN) of an iSCSI initiator.</p> <p><b>NOTE</b> The IQN of initiator must be the same as the one on application server. The IQN of a initiator must be unique, and do not configure the initiators of multiple application servers with the same IQN.</p>	<p>[Example] iqn. 1991-05.com. microsoft:host- name</p>
Alias	Alias of an iSCSI initiator.	<p>[Example] -</p>
Uses third-party multipath software	<ul style="list-style-type: none"> <li>● This parameter is only available after the initiator is added to host successfully.</li> <li>● If LUNs have been mapped to the host before you enable or disable <b>Uses third-party multipath software</b>, restart the host after reconfiguration.</li> <li>● If the host has installed UltraPath, do not need to enable <b>Uses third-party multipath software</b>.</li> </ul>	<p>[Example] Uses third-party multipath software</p>

Parameter	Description	Setting
<p>Switchover Mode</p>	<p>Patch switchover mode. The system supports the following four modes:</p> <ul style="list-style-type: none"> <li>● <b>early-version ALUA:</b> This mode is selected when an earlier version is upgraded to the current version. Requirements: <ul style="list-style-type: none"> <li>- The storage system is upgraded from V300R003C10 and earlier to V300R003C20/V300R006C00SPC100 or later or from V300R005 to V300R006C00SPC100 and later.</li> <li>- Before the upgrade, the storage system has dual controllers and has enabled ALUA.</li> </ul> </li> <li>● <b>common ALUA:</b> This mode is selected when a storage system is in V300R003C20, V300R006C00SPC100 and later versions. Requirements: <ul style="list-style-type: none"> <li>- The storage system is in V300R003C20, V300R006C00SPC100 and later versions</li> <li>- The storage system has dual or multiple controllers.</li> <li>- The storage system connects to a host running SUSE, Red Hat 6.X, Windows Server 2012 (Emulex HBA), Windows Server 2008 (Emulex HBA), and HP-UX 11i V3.</li> </ul> </li> <li>● <b>ALUA not used:</b> This mode is selected when a host such as HP-UX 11i V2 does not support ALUA or the actual application scenario does not need ALUA.</li> <li>● <b>Special mode:</b> This mode is selected when a host is in V300R003C20, V300R006C00SPC100 and later versions and connects to a host running an operating system not supported by common ALUA. Requirements: <ul style="list-style-type: none"> <li>- The storage system is in V300R003C20, V300R006C00SPC100, and later versions</li> <li>- The storage system has dual or multiple controllers.</li> <li>- The storage system connects to a host running VMware, AIX, Red Hat 7.X, Windows Server 2012 (QLogic HBA), and Windows Server 2008 (QLogic HBA).</li> </ul> </li> </ul> <p><b>NOTICE</b> When configuring the path switchover mode of an initiator, perform the operations with the guidance of Huawei technical support engineers and follow the requirements of relevant host connectivity guides. For example, <i>HUAWEI SAN Storage Host Connectivity Guide for Windows</i>.</p>	<p>[Example] common ALUA</p>

Parameter	Description	Setting
	<p><b>NOTE</b></p> <p>Asymmetric logical unit access (ALUA) is a multitarget port access model. In a multipathing state, the ALUA model provides a way of presenting active/passive LUNs to a host, and offers a port status switching interface to switch over the working controller. For example, when a host multipathing program supporting the ALUA detects a port status change on a controller that becomes faulty, the program will automatically switch subsequent I/Os to the other controller.</p>	
<p>Special mode type</p>	<p>The parameter applies to V300R003C20, V300R006C00SPC100, and later, and needs to be configured when you select <b>Special mode type</b> for <b>Switchover Mode</b>. The detailed requirements are as follows:</p> <ul style="list-style-type: none"> <li>● <b>Mode 0:</b> <ul style="list-style-type: none"> <li>- The host and storage system must be connected using a Fibre Channel network.</li> <li>- The OS of the host that connects to the storage system is Red Hat 7.X, Windows Server 2012 (using QLogic HBAs), or Windows Server 2008 (using QLogic HBAs).</li> </ul> </li> <li>● <b>Mode 1:</b> <ul style="list-style-type: none"> <li>- The OS of the host that connects to the storage system is AIX or VMware.</li> <li>- HyperMetro works in load balancing mode.</li> </ul> </li> <li>● <b>Mode 2:</b> <ul style="list-style-type: none"> <li>- The OS of the host that connects to the storage system is AIX or VMware.</li> <li>- HyperMetro works in local preferred mode.</li> </ul> </li> </ul> <p><b>NOTICE</b></p> <p>Perform the operations with the guidance of Huawei technical support engineers and follow the requirements of relevant host connectivity guides. For example, <i>HUAWEI SAN Storage Host Connectivity Guide for Windows</i>.</p>	<p>[Example]                      Mode 0</p>



Parameter	Description	Setting
Path Type	<p>The storage system supports two path switchover modes: <b>Optimal Path</b> and <b>Non-Optimal Path</b>.</p> <ul style="list-style-type: none"> <li>● When HyperMetro works in load balancing mode, set the <b>Path Type</b> for the initiators of both the local and remote storage arrays to <b>Optimal Path</b>. Enable ALUA on both the host and storage arrays. If the host uses the <b>round-robin</b> multipathing policy, it delivers I/Os to both storage arrays in round-robin mode.</li> <li>● When HyperMetro works in local preferred mode, set the <b>Path Type</b> for the initiator of the local storage array to <b>Optimal Path</b>, and that of the remote storage array to <b>Non-Optimal Path</b>. Enable ALUA on both the host and storage arrays. The host delivers I/Os to the local storage array preferentially.</li> </ul>	<p>[Example] Optimal Path</p>
Enable CHAP authentication	<p>CHAP authentication includes Discovery and Normal authentication.</p> <ul style="list-style-type: none"> <li>● If <b>Enable CHAP authentication</b> is selected, you must set <b>CHAP name</b> and <b>Password</b> for the storage system. In addition, you must set <b>CHAP name</b> and <b>Password</b> on the application server for it to access the storage system.</li> <li>● If <b>Enable CHAP authentication</b> is not selected, you do not need to set <b>CHAP name</b> and <b>Password</b> for the storage system.</li> </ul>	<p>[Example] -</p>
Normal Authentication	<p>Normal authentication is the process during with the target and initiator transmit data between each other after connections are set up. Authentication includes:</p> <ul style="list-style-type: none"> <li>● No authentication</li> <li>● Unidirectional authentication Target authenticates initiator.</li> <li>● Bidirectional authentication Target and initiator authenticates each other.</li> </ul>	<p>[Default Value] Unidirectional authentication</p>
Discovery Authentication	<p>Discovery authentication is a process during which the target and initiator set up connections. Authentication includes:</p> <ul style="list-style-type: none"> <li>● No authentication</li> <li>● Unidirectional authentication Target authenticates initiator.</li> <li>● Bidirectional authentication Target and initiator authenticates each other.</li> </ul>	<p>[Default Value] No authentication</p>

Parameter	Description	Setting
CHAP name	User name for CHAP authentication.	[Value range] The name contains 4 to 25 characters. <ul style="list-style-type: none"> <li>● The name contains 4 to 223 characters.</li> <li>● The name only contains letters, digits or special characters. Special characters are:                          !"#&amp;%()*                          +,-./:;&lt;=&gt;?                          @[ ] ^ _ ` {                            } ~</li> <li>● The first character must be letter or digit.</li> </ul> [Example] admin

Parameter	Description	Setting
Password	Password for CHAP authentication.	<p>[Value range]</p> <ul style="list-style-type: none"> <li>● The password contains 12 to 16 characters.</li> <li>● The password must contain three of the following four types of characters:                             <ul style="list-style-type: none"> <li>- Upper case letters</li> <li>- Lower case letters</li> <li>- Digits</li> <li>- Special characters (including space) !"#&amp;%()*+,-./:;&lt;=&gt;?@[]^_`{ }~</li> </ul> </li> <li>● The password cannot be the same as the account or mirror writing of the account.</li> </ul> <p>[Example]                      Admin@123456789</p>

Parameter	Description	Setting
Confirm password	Password for CHAP authentication.	[Value range] The value of <b>Confirm password</b> must be consistent with that of <b>Password</b> . [Example] -

**Step 6** Click **OK**.

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

**Step 7** Select the initiator that you want to add, select a host that you want to associate with the initiator, and click **Associate Host**.

**Step 8** Click **OK**.

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

---End

## 6.8.4 Modifying an Initiator

This operation enables you to modify the properties of an initiator.

### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Host** > **Initiator**.

**Step 3** Select the initiator whose properties you want to modify and click **Properties**.  
The **Initiator Properties** dialog box is displayed.

**Step 4** Modify the properties of the initiator. If the iSCSI initiator does not enable CHAP authentication, [Table 6-29](#) lists related parameters. If the iSCSI initiator has enabled CHAP authentication, [Table 6-30](#) lists related parameters. For non-iSCSI initiators, [Table 6-31](#) lists related parameters.

**Table 6-29** iSCSI initiator parameters (CHAP authentication not enabled)

Parameter	Description	Setting
Alias	The alias of initiator.	[Example] Initiator01
Uses third-party multipath software	<ul style="list-style-type: none"> <li>This parameter is only available after the initiator is added to host successfully.</li> <li>If LUNs have been mapped to the host before you enable or disable <b>Uses third-party multipath software</b>, restart the host after reconfiguration.</li> <li>If the host has installed UltraPath, do not need to enable <b>Uses third-party multipath software</b>.</li> </ul>	[Example] Uses third-party multipath software

Parameter	Description	Setting
Switchover Mode	<p>Patch switchover mode. The system supports the following four modes:</p> <ul style="list-style-type: none"> <li>● <b>early-version ALUA</b>: This mode is selected when an earlier version is upgraded to the current version.                          Requirements:                         <ul style="list-style-type: none"> <li>- The storage system is upgraded from V300R003C10 and earlier to V300R003C20/V300R006C00SPC100 or later or from V300R005 to V300R006C00SPC100 and later.</li> <li>- Before the upgrade, the storage system has dual controllers and has enabled ALUA.</li> </ul> </li> <li>● <b>common ALUA</b>: This mode is selected when a storage system is in V300R003C20, V300R006C00SPC100 and later versions.                          Requirements:                         <ul style="list-style-type: none"> <li>- The storage system is in V300R003C20, V300R006C00SPC100 and later versions</li> <li>- The storage system has dual or multiple controllers.</li> <li>- The storage system connects to a host running SUSE, Red Hat 6.X, Windows Server 2012 (Emulex HBA), Windows Server 2008 (Emulex HBA), and HP-UX 11i V3.</li> </ul> </li> <li>● <b>ALUA not used</b>: This mode is selected when a host such as HP-UX 11i V2 does not support ALUA or the actual application scenario does not need ALUA.</li> <li>● <b>Special mode</b>: This mode is selected when a host is in V300R003C20, V300R006C00SPC100 and later versions and connects to a host running an operating system not supported by common ALUA.                          Requirements:                         <ul style="list-style-type: none"> <li>- The storage system is in V300R003C20, V300R006C00SPC100, and later versions</li> <li>- The storage system has dual or multiple controllers.</li> <li>- The storage system connects to a host running VMware, AIX, Red Hat 7.X, Windows Server 2012 (QLogic HBA), and Windows Server 2008 (Qlogic HBA).</li> </ul> </li> </ul> <p><b>NOTICE</b>                      When configuring the path switchover mode of an initiator, perform the operations with the guidance of Huawei technical support engineers and follow the requirements of relevant host connectivity guides. For example, <i>HUAWEI SAN Storage Host Connectivity Guide for Windows</i>.</p>	[Example] common ALUA

Parameter	Description	Setting
	<p><b>NOTE</b></p> <p>Asymmetric logical unit access (ALUA) is a multitarget port access model. In a multipathing state, the ALUA model provides a way of presenting active/passive LUNs to a host, and offers a port status switching interface to switch over the working controller. For example, when a host multipathing program supporting the ALUA detects a port status change on a controller that becomes faulty, the program will automatically switch subsequent I/Os to the other controller.</p>	
<p>Special mode type</p>	<p>The parameter applies to V300R003C20, V300R006C00SPC100, and later, and needs to be configured when you select <b>Special mode type</b> for <b>Switchover Mode</b>. The detailed requirements are as follows:</p> <ul style="list-style-type: none"> <li>● <b>Mode 0:</b> <ul style="list-style-type: none"> <li>- The host and storage system must be connected using a Fibre Channel network.</li> <li>- The OS of the host that connects to the storage system is Red Hat 7.X, Windows Server 2012 (using QLogic HBAs), or Windows Server 2008 (using QLogic HBAs).</li> </ul> </li> <li>● <b>Mode 1:</b> <ul style="list-style-type: none"> <li>- The OS of the host that connects to the storage system is AIX or VMware.</li> <li>- HyperMetro works in load balancing mode.</li> </ul> </li> <li>● <b>Mode 2:</b> <ul style="list-style-type: none"> <li>- The OS of the host that connects to the storage system is AIX or VMware.</li> <li>- HyperMetro works in local preferred mode.</li> </ul> </li> </ul> <p><b>NOTICE</b></p> <p>Perform the operations with the guidance of Huawei technical support engineers and follow the requirements of relevant host connectivity guides. For example, <i>HUAWEI SAN Storage Host Connectivity Guide for Windows</i>.</p>	<p>[Example]                      Mode 0</p>

Parameter	Description	Setting
Path Type	<p>The storage system supports two path switchover modes: <b>Optimal Path</b> and <b>Non-Optimal Path</b>.</p> <ul style="list-style-type: none"> <li>● When HyperMetro works in load balancing mode, set the <b>Path Type</b> for the initiators of both the local and remote storage arrays to <b>Optimal Path</b>. Enable ALUA on both the host and storage arrays. If the host uses the <b>round-robin</b> multipathing policy, it delivers I/Os to both storage arrays in round-robin mode.</li> <li>● When HyperMetro works in local preferred mode, set the <b>Path Type</b> for the initiator of the local storage array to <b>Optimal Path</b>, and that of the remote storage array to <b>Non-Optimal Path</b>. Enable ALUA on both the host and storage arrays. The host delivers I/Os to the local storage array preferentially.</li> </ul>	[Example] Optimal Path
Enable CHAP authentication	<p>CHAP authentication includes Discovery and Normal authentication.</p> <ul style="list-style-type: none"> <li>● If <b>Enable CHAP authentication</b> is selected, you must set <b>CHAP name</b> and <b>Password</b> for the storage system. In addition, you must set <b>CHAP name</b> and <b>Password</b> on the application server for it to access the storage system.</li> <li>● If <b>Enable CHAP authentication</b> is not selected, you do not need to set <b>CHAP name</b> and <b>Password</b> for the storage system.</li> </ul> <p><b>NOTE</b> The CHAP authentication parameters are valid when the type of the initiator is iSCSI.</p>	[Example] -

**Table 6-30** iSCSI initiator parameters (CHAP authentication enabled)

Parameter	Description	Setting
Alias	The alias of initiator.	[Example] Initiator01
Uses third-party multipath software	<ul style="list-style-type: none"> <li>● This parameter is only available after the initiator is added to host successfully.</li> <li>● If LUNs have been mapped to the host before you enable or disable <b>Uses third-party multipath software</b>, restart the host after reconfiguration.</li> <li>● If the host has installed UltraPath, do not need to enable <b>Uses third-party multipath software</b>.</li> </ul>	[Example] Uses third-party multipath software



Parameter	Description	Setting
Switchover Mode	<p>Patch switchover mode. The system supports the following four modes:</p> <ul style="list-style-type: none"> <li>● <b>early-version ALUA</b>: This mode is selected when an earlier version is upgraded to the current version.                          Requirements:                         <ul style="list-style-type: none"> <li>- The storage system is upgraded from V300R003C10 and earlier to V300R003C20/V300R006C00SPC100 or later or from V300R005 to V300R006C00SPC100 and later.</li> <li>- Before the upgrade, the storage system has dual controllers and has enabled ALUA.</li> </ul> </li> <li>● <b>common ALUA</b>: This mode is selected when a storage system is in V300R003C20, V300R006C00SPC100 and later versions.                          Requirements:                         <ul style="list-style-type: none"> <li>- The storage system is in V300R003C20, V300R006C00SPC100 and later versions</li> <li>- The storage system has dual or multiple controllers.</li> <li>- The storage system connects to a host running SUSE, Red Hat 6.X, Windows Server 2012 (Emulex HBA), Windows Server 2008 (Emulex HBA), and HP-UX 11i V3.</li> </ul> </li> <li>● <b>ALUA not used</b>: This mode is selected when a host such as HP-UX 11i V2 does not support ALUA or the actual application scenario does not need ALUA.</li> <li>● <b>Special mode</b>: This mode is selected when a host is in V300R003C20, V300R006C00SPC100 and later versions and connects to a host running an operating system not supported by common ALUA.                          Requirements:                         <ul style="list-style-type: none"> <li>- The storage system is in V300R003C20, V300R006C00SPC100, and later versions</li> <li>- The storage system has dual or multiple controllers.</li> <li>- The storage system connects to a host running VMware, AIX, Red Hat 7.X, Windows Server 2012 (QLogic HBA), and Windows Server 2008 (Qlogic HBA).</li> </ul> </li> </ul> <p><b>NOTICE</b>                      When configuring the path switchover mode of an initiator, perform the operations with the guidance of Huawei technical support engineers and follow the requirements of relevant host connectivity guides. For example, <i>HUAWEI SAN Storage Host Connectivity Guide for Windows</i>.</p>	[Example] common ALUA

Parameter	Description	Setting
	<p><b>NOTE</b></p> <p>Asymmetric logical unit access (ALUA) is a multitarget port access model. In a multipathing state, the ALUA model provides a way of presenting active/passive LUNs to a host, and offers a port status switching interface to switch over the working controller. For example, when a host multipathing program supporting the ALUA detects a port status change on a controller that becomes faulty, the program will automatically switch subsequent I/Os to the other controller.</p>	
<p>Special mode type</p>	<p>The parameter applies to V300R003C20, V300R006C00SPC100, and later, and needs to be configured when you select <b>Special mode type</b> for <b>Switchover Mode</b>. The detailed requirements are as follows:</p> <ul style="list-style-type: none"> <li>● <b>Mode 0:</b> <ul style="list-style-type: none"> <li>- The host and storage system must be connected using a Fibre Channel network.</li> <li>- The OS of the host that connects to the storage system is Red Hat 7.X, Windows Server 2012 (using QLogic HBAs), or Windows Server 2008 (using QLogic HBAs).</li> </ul> </li> <li>● <b>Mode 1:</b> <ul style="list-style-type: none"> <li>- The OS of the host that connects to the storage system is AIX or VMware.</li> <li>- HyperMetro works in load balancing mode.</li> </ul> </li> <li>● <b>Mode 2:</b> <ul style="list-style-type: none"> <li>- The OS of the host that connects to the storage system is AIX or VMware.</li> <li>- HyperMetro works in local preferred mode.</li> </ul> </li> </ul> <p><b>NOTICE</b></p> <p>Perform the operations with the guidance of Huawei technical support engineers and follow the requirements of relevant host connectivity guides. For example, <i>HUAWEI SAN Storage Host Connectivity Guide for Windows</i>.</p>	<p>[Example]                      Mode 0</p>

Parameter	Description	Setting
Path Type	<p>The storage system supports two path switchover modes: <b>Optimal Path</b> and <b>Non-Optimal Path</b>.</p> <ul style="list-style-type: none"> <li>● When HyperMetro works in load balancing mode, set the <b>Path Type</b> for the initiators of both the local and remote storage arrays to <b>Optimal Path</b>. Enable ALUA on both the host and storage arrays. If the host uses the <b>round-robin</b> multipathing policy, it delivers I/Os to both storage arrays in round-robin mode.</li> <li>● When HyperMetro works in local preferred mode, set the <b>Path Type</b> for the initiator of the local storage array to <b>Optimal Path</b>, and that of the remote storage array to <b>Non-Optimal Path</b>. Enable ALUA on both the host and storage arrays. The host delivers I/Os to the local storage array preferentially.</li> </ul>	[Example] Optimal Path
Enable CHAP authentication	<p>CHAP authentication includes Discovery and Normal authentication.</p> <ul style="list-style-type: none"> <li>● If <b>Enable CHAP authentication</b> is selected, you must set <b>CHAP name</b> and <b>Password</b> for the storage system. In addition, you must set <b>CHAP name</b> and <b>Password</b> on the application server for it to access the storage system.</li> <li>● If <b>Enable CHAP authentication</b> is not selected, you do not need to set <b>CHAP name</b> and <b>Password</b> for the storage system.</li> </ul> <p><b>NOTE</b> The CHAP authentication parameters are valid when the type of the initiator is iSCSI.</p>	[Example] -
Normal Authentication	<p>Normal authentication is the process during with the target and initiator transmit data between each other after connections are set up. Authentication includes:</p> <ul style="list-style-type: none"> <li>● No authentication</li> <li>● Unidirectional authentication Target authenticates initiator.</li> <li>● Bidirectional authentication Target and initiator authenticates each other.</li> </ul>	[Default Value] Unidirectional authentication
Discovery Authentication	<p>Discovery authentication is a process during which the target and initiator set up connections. Authentication includes:</p> <ul style="list-style-type: none"> <li>● No authentication</li> <li>● Unidirectional authentication Target authenticates initiator.</li> <li>● Bidirectional authentication Target and initiator authenticates each other.</li> </ul>	[Default Value] No authentication

Parameter	Description	Setting
Old Password	Old password for CHAP authentication <b>NOTE</b> Click <b>Modify</b> next to <b>Password</b> to modify the CHAP authentication password.	[Example] -

Parameter	Description	Setting
New Password	New Password for CHAP authentication.	<p>[Value range]</p> <ul style="list-style-type: none"> <li>● The password contains 12 to 16 characters.</li> <li>● The password must contain three of the following four types of characters:                             <ul style="list-style-type: none"> <li>- Uppercase letters</li> <li>- Lowercase letters</li> <li>- Digits</li> <li>- Special characters (including space)                                     <ul style="list-style-type: none"> <li>` ~ ! @ # \$ % ^ &amp; * ( ) - _ = + \   [ { } ] ; : ' " &lt; . &gt; / ?</li> </ul> </li> </ul> </li> <li>● The password cannot be the same as the account or mirror writing of the account.</li> </ul> <p>[Example]</p> <p>-</p>

Parameter	Description	Setting
Confirm Password	Password for CHAP authentication.	[Value range] The value of <b>Confirm Password</b> must be consistent with that of <b>New Password</b> . [Example] -

**Table 6-31** Non-iSCSI initiator parameters

Parameter	Description	Setting
Alias	The alias of initiator.	[Example] Initiator01
Uses third-party multipath software	<ul style="list-style-type: none"> <li>● This parameter is only available after the initiator is added to host successfully.</li> <li>● If LUNs have been mapped to the host before you enable or disable <b>Uses third-party multipath software</b>, restart the host after reconfiguration.</li> <li>● If the host has installed UltraPath, do not need to enable <b>Uses third-party multipath software</b>.</li> </ul>	[Example] Uses third-party multipath software

Parameter	Description	Setting
Switchover Mode	<p>Patch switchover mode. The system supports the following four modes:</p> <ul style="list-style-type: none"> <li>● <b>early-version ALUA</b>: This mode is selected when an earlier version is upgraded to the current version.                      Requirements:                     <ul style="list-style-type: none"> <li>- The storage system is upgraded from V300R003C10 and earlier to V300R003C20/V300R006C00SPC100 or later or from V300R005 to V300R006C00SPC100 and later.</li> <li>- Before the upgrade, the storage system has dual controllers and has enabled ALUA.</li> </ul> </li> <li>● <b>common ALUA</b>: This mode is selected when a storage system is in V300R003C20, V300R006C00SPC100 and later versions.                      Requirements:                     <ul style="list-style-type: none"> <li>- The storage system is in V300R003C20, V300R006C00SPC100 and later versions</li> <li>- The storage system has dual or multiple controllers.</li> <li>- The storage system connects to a host running SUSE, Red Hat 6.X, Windows Server 2012 (Emulex HBA), Windows Server 2008 (Emulex HBA), and HP-UX 11i V3.</li> </ul> </li> <li>● <b>ALUA not used</b>: This mode is selected when a host such as HP-UX 11i V2 does not support ALUA or the actual application scenario does not need ALUA.</li> <li>● <b>Special mode</b>: This mode is selected when a host is in V300R003C20, V300R006C00SPC100 and later versions and connects to a host running an operating system not supported by common ALUA.                      Requirements:                     <ul style="list-style-type: none"> <li>- The storage system is in V300R003C20, V300R006C00SPC100, and later versions</li> <li>- The storage system has dual or multiple controllers.</li> <li>- The storage system connects to a host running VMware, AIX, Red Hat 7.X, Windows Server 2012 (QLogic HBA), and Windows Server 2008 (Qlogic HBA).</li> </ul> </li> </ul> <p><b>NOTICE</b>                      When configuring the path switchover mode of an initiator, perform the operations with the guidance of Huawei technical support engineers and follow the requirements of relevant host connectivity guides. For example, <i>HUAWEI SAN Storage Host Connectivity Guide for Windows</i>.</p>	[Example] common ALUA

Parameter	Description	Setting
	<p><b>NOTE</b></p> <p>Asymmetric logical unit access (ALUA) is a multitarget port access model. In a multipathing state, the ALUA model provides a way of presenting active/passive LUNs to a host, and offers a port status switching interface to switch over the working controller. For example, when a host multipathing program supporting the ALUA detects a port status change on a controller that becomes faulty, the program will automatically switch subsequent I/Os to the other controller.</p>	
<p>Special mode type</p>	<p>The parameter applies to V300R003C20, V300R006C00SPC100, and later, and needs to be configured when you select <b>Special mode type</b> for <b>Switchover Mode</b>. The detailed requirements are as follows:</p> <ul style="list-style-type: none"> <li>● <b>Mode 0:</b> <ul style="list-style-type: none"> <li>- The host and storage system must be connected using a Fibre Channel network.</li> <li>- The OS of the host that connects to the storage system is Red Hat 7.X, Windows Server 2012 (using QLogic HBAs), or Windows Server 2008 (using QLogic HBAs).</li> </ul> </li> <li>● <b>Mode 1:</b> <ul style="list-style-type: none"> <li>- The OS of the host that connects to the storage system is AIX or VMware.</li> <li>- HyperMetro works in load balancing mode.</li> </ul> </li> <li>● <b>Mode 2:</b> <ul style="list-style-type: none"> <li>- The OS of the host that connects to the storage system is AIX or VMware.</li> <li>- HyperMetro works in local preferred mode.</li> </ul> </li> </ul> <p><b>NOTICE</b></p> <p>Perform the operations with the guidance of Huawei technical support engineers and follow the requirements of relevant host connectivity guides. For example, <i>HUAWEI SAN Storage Host Connectivity Guide for Windows</i>.</p>	<p>[Example]                      Mode 0</p>



Parameter	Description	Setting
Path Type	<p>The storage system supports two path switchover modes: <b>Optimal Path</b> and <b>Non-Optimal Path</b>.</p> <ul style="list-style-type: none"> <li>● When HyperMetro works in load balancing mode, set the <b>Path Type</b> for the initiators of both the local and remote storage arrays to <b>Optimal Path</b>. Enable ALUA on both the host and storage arrays. If the host uses the <b>round-robin</b> multipathing policy, it delivers I/Os to both storage arrays in round-robin mode.</li> <li>● When HyperMetro works in local preferred mode, set the <b>Path Type</b> for the initiator of the local storage array to <b>Optimal Path</b>, and that of the remote storage array to <b>Non-Optimal Path</b>. Enable ALUA on both the host and storage arrays. The host delivers I/Os to the local storage array preferentially.</li> </ul>	[Example] Optimal Path

**Step 5** Confirm the modification of the initiator's properties.

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

----End

## 6.8.5 Deleting an Initiator

This operation enables you to delete an initiator that is no longer used from a storage device.

### Prerequisites

The **Status** of the initiator must be **Offline**.

### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Host** > **Initiator**.

**Step 3 Optional:** Cancel host association.

1. Select the initiator you want to cancel host association and click **Cancel Host Association**.  
The **Danger** dialog box is displayed.
2. Click the check box next to the statement **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**.

**Step 4** Delete an initiator.

1. Select the initiator you want to delete and click **Delete**.  
The security alert dialog box is displayed.
2. Click **OK**.  
The **Execution Result** dialog box is displayed indicating that the operation succeeded.
3. Click **Close**.

----End

## 6.8.6 Adding an Initiator to a Host

This operation enables you to add an initiator to a host.

### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Host** > **Initiator**.

**Step 3** Select initiators to be added to a host based on service requirements.

**Step 4** Click **Associate Host** to add initiators to a host.  
The **Associate Host** dialog box is displayed.

**Step 5** Select a host and associate it with initiators. Then click **OK**.  
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 **Execution result** dialog box is displayed, indicating that the operation succeeded.

**Step 8** Click **Close**.

----End

## 6.8.7 Deleting a Host

After a host is deleted, the communication between LUNs on the host and the corresponding application server is interrupted.

### Prerequisites

The host to be deleted is not added to any host group.

### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Host**.

- Step 3** Select the host you want to delete and click **Delete**.  
The security alert dialog box is displayed.
- Step 4** Confirm the deleting of the host.
- Carefully read the content in the dialog box. Then select **I have read and understand the consequences associated with performing this operation.** for confirmation.
  - Click **OK**.  
The **Execution Result** dialog box is displayed indicating that the operation succeeded.
  - Click **Close**.
- End

## 6.9 Managing Host Groups

To centrally manage multiple hosts, you can aggregate hosts into a host group.



### 6.9.1 Viewing Host Group Information

This operation enables you to view basic information about a host group.

#### Prerequisites

At least one host group has been created.

#### Procedure

- Step 1** Log in to DeviceManager.
- Step 2** Choose  **Provisioning** >  **Host** > **Host Group**.
- Step 3** In the function pane, view the host group information. [Table 6-32](#) describes related parameters.

**Table 6-32** Host group parameters

Parameter	Description	Setting
Name	Name of a host group.	[Example] <b>HostGroup001</b>
ID	ID of a host group.	[Example] <b>1</b>

- Step 4** In the details area, information about the member hosts is displayed.
- End

### 6.9.2 Modifying Host Group Information

This operation enables you to view or modify basic information about a host group.

## Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Host** > **Host Group**.

**Step 3** Modify the general properties of the host group.

1. Select the host group you want to modify.
2. Click **Properties**.  
The **Properties of Host Group** dialog box is displayed.
3. In the **Properties of Host Group** dialog box, click the **General** tab.
4. In the **Name** text box, name the host group.

 **NOTE**

Name a host group in accordance with the following rules so that the host group is available to host applications.

- The name must be unique.
  - The name can contain only letters, digits, periods (.), underscores (\_), and hyphens (-).
  - The value contains 1 to 31 characters.
5. In the **Description** text box, describe the host group.

**Step 4** Confirm your operation.

1. Click **OK**.  
The **Execution Result** message box is displayed, indicating that the operation succeeded.
2. Click **Close**.

----End

## 6.9.3 Viewing an Owing Mapping View of a Host Group

This operation enables you to view information about the owing mapping view of a host group.

### Prerequisites

At least one host group has been created.

## Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Host** > **Host Group**.

**Step 3** Select the host group you want to view, and click **Properties**.  
The **Properties of Host Group** dialog box is displayed.

**Step 4** View information about the owing mapping view of a host group.

1. In the **Properties of Host Group** dialog box, click the **Owing Mapping View** tab.

2. View information about an owning mapping view. [Table 6-33](#) describes related parameters.

**Table 6-33** Owning mapping view parameters

Parameter	Description	Setting
Name	Name of a contained mapping view.	[Example] Hostgroupmapping001
ID	ID of a contained mapping view.	[Example] 1

----End

## 6.9.4 Adding a Host

This operation enables you to add a host. A host can be added to a maximum of 64 host groups. A host group can be added with a maximum of 64 hosts.

### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Host** > **Host Group**.

**Step 3** Add a host.

1. Select the host group that you want to add a host to.
2. Click **Add Host** to add a host.  
The **Add Host to Host Group** dialog box is displayed.
3. Select the host that you want to add.

 **NOTE**

If hosts to be added into the host group belong to different clusters, data access conflict may occur and cause data loss. Before this operation, you are advised to install cluster software to manage hosts.

4. Click  to add the host to the **Selected Hosts** list.

**Step 4** Confirm your operation.

1. Click **OK**.  
The **Execution Result** message box is displayed, indicating that the operation succeeded.
2. Click **Close**.

----End

## 6.9.5 Deleting a Host Group

This operation enables you to delete a host group when it is no longer needed.

## Prerequisites

The Host group to be deleted is not added to the mapping view.

## Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Host** > **Host Group**.

**Step 3** Delete the host group.

1. Select the host group you want to delete.
2. Click **Delete**.  
The security alert dialog box is displayed.
3. Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation**.
4. Click **OK**.  
The **Execution Result** message box is displayed, indicating that the operation succeeded.
5. Click **Close**.

----End

## 6.10 Managing a Port Group

This section describes how to manage a port group, including viewing information about the port group and the mapping view where the port group resides.

### 6.10.1 Viewing the Information About a Port Group

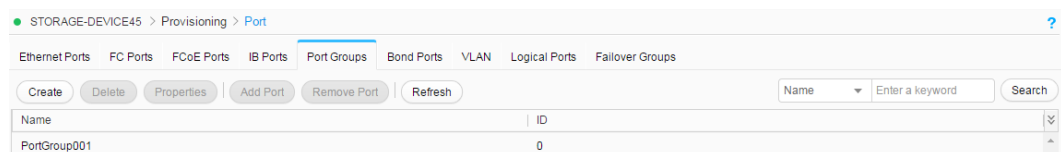
This operation enables you to view the information about a port group.

## Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Port** > **Port Groups**.

**Step 3** In the function pane in the upper area, view information about the port group.



**Table 6-34** Port group parameters

Parameter	Description	Value
Name	Name of a port group.	[Example] PortGroup001
ID	ID of a port group.	[Example] 1

**Step 4** In the function pane in the lower area, view information about ports contained by the port group.

**Table 6-35** Port parameters

Parameter	Description	Value
Type	Type of a port.	[Example] Ethernet port
Location	Location of a port.	[Example] CTE0.B0.P0
Health Status	Health status of a port.	[Example] Normal
Running Status	Running status of a port.	[Example] Link up

----End

## 6.10.2 Modifying the Properties of a Port Group

This operation enables you to modify the properties of a port group.

### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Port** > **Port Groups**.

**Step 3** Select the port group you want to modify and click **Properties**.  
The **Properties of Port Group** dialog box is displayed.

**Step 4** In the **Properties of Port Group** dialog box, click the **General** tab.  
In the function pane, view the port group information. [Table 6-36](#) describes related parameters.

**Table 6-36** Port group parameters

Parameter	Description	Value
Name	Name of a port group.	[Example] portGroup001
Description	Description of a port group.	[Example] -
ID	ID of a port group.	[Example] 1

**Step 5** Confirm your operation.

1. Click **OK**.

The **Execution result** message box is displayed, indicating that the operation succeeded.

2. Click **Close**.

----End

### 6.10.3 Viewing an Owing Mapping View

This operation enables you to view information about the owing mapping view of a port group.

#### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Port** > **Port Groups**.

**Step 3** Select the port group you want to modify and click **Properties**.  
The **Properties of Port Group** dialog box is displayed.

**Step 4** In the **Properties of Port Group** dialog box, click the **Owing Mapping View** tab.  
In the function pane, view the port group information. [Table 6-37](#) describes related parameters.

**Table 6-37** Port group parameters

Parameter	Description	Value
Name	Name of a contained mapping view.	[Example] portGroupMappingView001
ID	ID of a contained mapping view.	[Example] 1

----End



## 6.10.4 Deleting a Port Group

This operation enables you to delete a port group when it is no longer needed.

### Prerequisites

The port group is not added to any mapping view.

### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Port** > **Port Groups**.

**Step 3** Select the port group you want to delete.

1. Click **Delete**.  
The security alert dialog box is displayed.
2. Read the contents of the security alert dialog box carefully. Then click the check box next to the statement **I have read the previous information and understood subsequences of the operation** to confirm the information.
3. Click **OK**.  
The **Execution Result** message box is displayed, indicating that the operation succeeded.
4. Click **Close**.

----End

## 6.10.5 Adding a Port

This operation enables you to add a port.

### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Port** > **Port Groups**.

**Step 3** Select the port group whose port you want to add and click **Add Port**.  
The **Add Port** message box is displayed.

**Step 4** From the **Available Ports** list, select the ports you want to remove.

**Step 5** Click **Right Arrow** to move the ports to the **Selected Ports**.

**Step 6** Confirm your operation.

1. Click **OK**.  
The **Execution Result** message box is displayed, indicating that the operation succeeded.
2. Click **Close**.

----End

## 6.10.6 Removing a Port

This operation enables you to remove a port.

### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Port** > **Port Groups**.

**Step 3** Select the port group whose port you want to remove and Click **Remove Port**.  
The **Remove Port** dialog box is displayed.

**Step 4** From the **Added Ports** list, select the ports you want to remove.

**Step 5** Click **Right Arrow** to move the ports to the **Ports to Be Removed**.

**Step 6** Confirm your operation.

1. Click **OK**.  
The security alert dialog box is displayed.
2. Read the contents of the security alert dialog box carefully. Then click the check box next to the statement **I have read the previous information and understood subsequences of the operation** to confirm the information.
3. Click **OK**.  
The **Execution Result** message box is displayed, indicating that the operation succeeded.
4. Click **Close**.

----End

## 6.11 Managing Mapping Views

This function allows you to flexibly allocate storage resources to hosts using mapping views.

### 6.11.1 Viewing Mapping View Information

This operation enables you to view the basic information about all the mapping views on a storage system.

#### Prerequisites

At least one mapping view has been created on the storage system.

#### Procedure

**Step 1** Log in to DeviceManager.

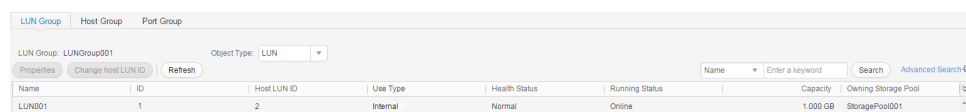
**Step 2** Choose  **Provisioning** >  **Mapping View**.

**Step 3** View the information about mapping views in the upper part of page. [Table 6-38](#) describes related parameters.

**Table 6-38** Mapping view parameters

Parameter	Description	Setting
Name	Name of a mapping view.	[Example] MappingView001
ID	ID of a mapping view.	[Example] 2

**Step 4** Select a mapping view. On the **LUN Group** tab page in the lower part of the function pane, view the information about the LUNs and snapshots in the mapping view. [Table 6-39](#), [Table 6-40](#) describes related parameters.









**Table 6-39** LUN parameters


Parameter	Description	Setting
Name	Name of a LUN.	[Example] LUN001
ID	ID of a LUN.	[Example] 2
Host LUN ID	For a LUN mapped to a host, the storage system assigns the ID for the LUN. <b>NOTE</b> This ID can be modified manually.	[Value Range] 0 to 511 [Example] 2
Use Type	Use type of a LUN. The use types include: <ul style="list-style-type: none"> <li>● <b>Internal:</b> Common LUN created in local storage device.</li> <li>● <b>External:</b> eDevLUN created for taking over LUN in remote storage device.</li> </ul>	[Example] Internal
Health Status	Indicates whether a LUN is normal.	[Example] Normal
Running Status	Indicates whether a LUN is working properly.	[Example] Online

Parameter	Description	Setting
Capacity	Capacity of a LUN.	[Example] 1 GB
Owning Storage Pool	The storage pool to which a LUN belongs.	[Example] storagepool1

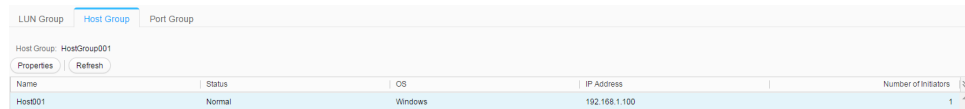
**Table 6-40** Snapshot parameters

Parameter	Description	Setting
Name	Name of a snapshot.	[Value range] <ul style="list-style-type: none"> <li>● The name must be unique.</li> <li>● The name contains letters, digits, underscores (_), periods (.), and hyphens (-).</li> <li>● The name contains 1 to 31 characters.</li> </ul> [Example] Snapshot001
ID	ID of a snapshot. <b>NOTE</b> After click  and choose this parameter, you can view this parameter in the snapshots list.	[Example] 2
Host LUN ID	For a LUN mapped to a host, the storage system assigns the ID for the LUN. <b>NOTE</b> This ID can be modified manually.	[Value Range] 0 to 511 [Example] 2
Health Status	Indicates whether a snapshot is normal. The possible value can be <b>Normal</b> or <b>Fault</b> .	[Example] Normal
Running Status	Indicates whether a snapshot is working properly. The possible value can be <b>Activated</b> , <b>Restore</b> , or <b>Deleting</b> , or <b>Modifying</b> , or <b>Inactive</b> .	[Example] Activated

Parameter	Description	Setting
Source LUN	Name of the source LUN of a snapshot. Source LUN is a LUN where source data resides.	[Example] lun005
Source LUN ID	ID of the source LUN of a snapshot. <b>NOTE</b> After click  and choose this parameter, you can view this parameter in the snapshots list.	[Example] 2
Snapshot Capacity	The same as the capacity of the source LUN of a snapshot.	[Example] 1.000 GB
Allocated Capacity	Storage pool capacity allocated to a snapshot. After the snapshot is activated, the capacity includes the data capacity and metadata capacity of the writable snapshot (excluding the data protection capacity of the source LUN). The metadata capacity occupies about 1% of the data capacity.	[Example] 256 MB
Activated At	Time when a snapshot is activated.	[Example] 2013-11-16 14:12:25 UTC +08:00
Mapping	Indicates whether a snapshot is mapped to a mapping view. The possible value can be <b>Mapped</b> or <b>Unmapped</b> .	[Example] Unmapped
WWN	World Wide Name (WWN) of a snapshot. <b>NOTE</b> After click  and choose this parameter, you can view this parameter in the snapshots list.	[Example] 210235G6LLZ0 B8000008
Rollback Start Time	Time when a snapshot rollback is started. <b>NOTE</b> After click  and choose this parameter, you can view this parameter in the snapshots list.	[Example] 2014-05-30 10:15:25 UTC +08:00
Rollback End Time	Time when a snapshot rollback is completed. <b>NOTE</b> After click  and choose this parameter, you can view this parameter in the snapshots list.	[Example] 2014-05-30 10:15:45 UTC +08:00
Rollback Progress	Progress of a snapshot rollback. <b>NOTE</b> After click  and choose this parameter, you can view this parameter in the snapshots list.	[Example] 50

Parameter	Description	Setting
Rollback Speed	<p>Rate at which a snapshot is rolled back. The possible value can be <b>Low</b>, <b>Medium</b>, <b>High</b>, or <b>Highest</b>.</p> <ul style="list-style-type: none"> <li>● When the service load on the storage system is heavy, set the rollback rate to <b>Low</b> or <b>Medium</b>.</li> <li>● When the service load on the storage system is light, set the rollback rate to <b>High</b> or <b>Highest</b>.</li> </ul> <p><b>NOTE</b></p> <p>After click  and choose this parameter, you can view this parameter in the snapshots list.</p>	[Example] High

**Step 5** On the **Host Group** tab page in the lower part of the function pane, view the information about the hosts in the mapping view. [Table 6-41](#) describes related parameters.



**Table 6-41** Host parameters

Parameter	Description	Setting
Name	Name of a host.	[Example] host11
ID	ID of a host.	[Example] 2
Status	Status of a host.	[Example] Normal
OS	Operating system used by the hosts in a mapping view. The value can be <b>Windows</b> , <b>Windows Server 2012</b> , <b>Linux</b> , <b>Solaris</b> , <b>HP-UX</b> , <b>AIX</b> , <b>XenServer</b> , <b>Mac OS X</b> , <b>VMware ESX</b> and <b>Windows Server 2012</b> .	[Example] Windows
IP Address	IP address of a host.	[Example] 192.168.1.100
Number of Initiators	The number of initiators that a host contains.	[Example] 1

**Step 6** On the **Port Group** tab page in the lower part of the function pane, view information about the ports in the mapping view. [Table 6-42](#) describes related parameters.

Location	Type	Health Status	Running Status
CTE0.A.IOM1.P0	Ethernet Port	Normal	Link down

**Table 6-42** Port parameters

Parameter	Description	Setting
Location	Location of a port.	Example CTE0.A.IO M1.P0
Type	Type of a port.	[Example] FC
Health Status	Health status of a port.	[Example] Normal
Running Status	Running status of a port.	[Example] Link Down

----End

## 6.11.2 Modifying the Properties of a Mapping View

This operation enables you to modify the name and description of a mapping view.

### Prerequisites

At least one mapping view has been created on the storage system.

### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Mapping View**.

**Step 3** Select the mapping view whose properties you want to modify and click **Properties**.  
The **Properties of Mapping View** dialog box is displayed.

**Step 4** Modify the properties of the mapping view.

1. In the **Name** text box, enter a new name for the mapping view.
2. **Optional:** In the **Description** text box, enter new description for the mapping view.

**Step 5** Confirm the modification of the mapping view's properties.

1. Click **OK**.  
The **Execution Result** dialog box is displayed indicating that the operation succeeded.
2. Click **Close**.

----End

## 6.11.3 Deleting a Mapping View

This operation enables you to delete a mapping view.

### Prerequisites

Before deleting a mapping view, ensure that all services on it have been stopped.

### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Mapping View**.

**Step 3** Select the mapping view you want to delete and click **Delete**.  
The security alert dialog box is displayed.

**Step 4** Confirm the information in the dialog box and select **I have read and understand the consequences associated with performing this operation..**

**Step 5** Click **OK**.  
The **Execution result** dialog box is displayed, indicating that the operation succeeded.

**Step 6** Click **Close**.

----End

## 6.11.4 Modifying a Host LUN ID

Host LUN ID is an ID allocated by the storage system to a LUN mapped to a host. This ID is visible on the host. You can manually change host LUN IDs based on site requirements.

### Prerequisites

- A mapping view has been created.
- LUN groups in the existing mapping view must contain LUNs.
- Host services running on the LUN have been stopped. In addition, the LUN's physical disks and virtual disks generated by the multipathing have been uninstalled.

### Context

- A host LUN ID is uniquely allocated to each LUN of a host.
- LUNs of different hosts can have the same host LUN ID.

### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Mapping View**.

**Step 3** Select a mapping view and click the **LUN Group** tab in the lower part of the left function pane.



**Step 4** In the LUN group list, select the LUN whose host LUN ID you want to change and click **Modify Host LUN ID**.

The **Modify Host LUN ID** dialog box is displayed.

**Step 5** Select a new host LUN ID and click **OK**.

**Step 6** Read the content of the dialog box carefully and select **I have read and understand the consequences associated with performing this operation..**

**Step 7** Click **OK**. The host LUN ID is successfully modified.

----End

# 7 Appendix OpenStack Cinder Driver Access Methods and Configuration Ideas

---

OpenStack Cinder Driver is a plug-in deployed on the OpenStack Cinder module. The plug-in can be used to provide functions such as logical volume configuration for virtual machines (VMs) in OpenStack. Cinder Driver supports iSCSI and FC protocols.

## Obtaining Cinder Driver

You can obtain OpenStack Cinder Driver by using either of the following methods:

- Obtain Cinder Driver from the OpenStack community warehouse: Since the Kilo version, Huawei has contributed all of its storage drivers to the OpenStack community. OpenStack integrates Huawei's storage drivers. Users can download OpenStack drivers contributed to the OpenStack community. After OpenStack of the specified version is installed, you can find Cinder Driver in `/Cinder/Cinder/share/drivers/huawei`.

### NOTE

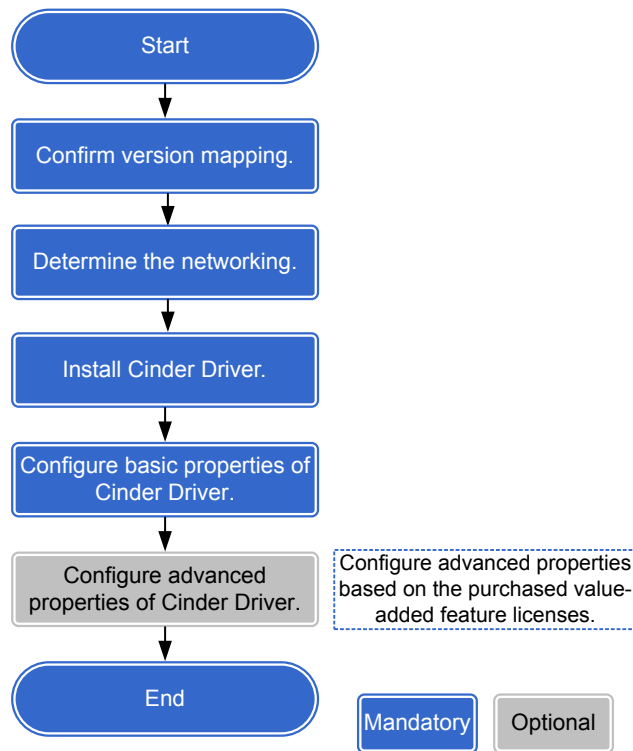
If you cannot find the installation file after installation, you can download the specified Cinder Driver from the OpenStack official website.

- Obtain Cinder Driver from Huawei's OpenStack driver warehouse: Go to [https://github.com/huaweistorage/OpenStack\\_Driver](https://github.com/huaweistorage/OpenStack_Driver). Then you can download Cinder Driver that matches the OpenStack version.

## Configuration Roadmap

[Figure 7-1](#) shows the configuration roadmap of Cinder Driver.

**Figure 7-1** Cinder Driver configuration roadmap



For the specific steps of configuring Cinder Driver, see the configuration guide released with Cinder Driver.

# 8 FAQ

---

## About This Chapter

This chapter describes FAQs related to the basic storage service configuration guide. You can also refer to this chapter when encountering faults during configurations or maintenance.

[8.1 In the SQL Server database scenario, how can I adjust parameters to reduce the I/O latency and achieve the optimal performance?](#)

[8.2 How to create AD domain users and groups on the AD domain controller?](#)

## 8.1 In the SQL Server database scenario, how can I adjust parameters to reduce the I/O latency and achieve the optimal performance?

### Question

In the SQL Server database scenario, how can I adjust parameters to reduce the I/O latency and achieve the optimal performance?

### Answer

You can set **target\_recovery\_time** to **60** according to the SQL official suggestion. For details, see <https://docs.microsoft.com/zh-cn/sql/relational-databases/logs/database-checkpoints-sql-server#IndirectChkpt>.

## 8.2 How to create AD domain users and groups on the AD domain controller?

### Question

How to create AD domain users and groups on the AD domain controller?

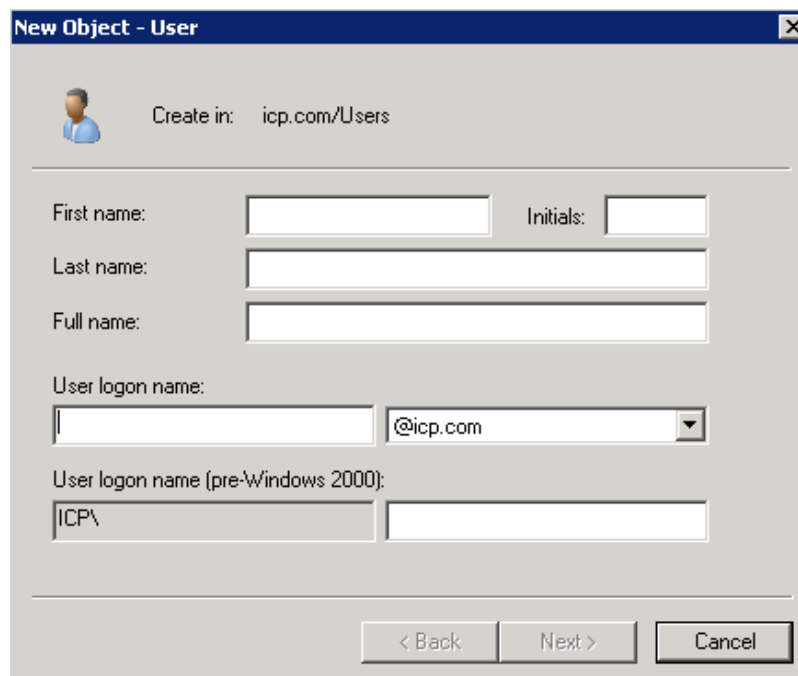
## Answer

- After the primary AD domain controller is configured, you need to create AD domain users and groups on the AD domain controller. An administrator can centrally manage domain users and groups and allocate them to different users.
- A user can log in to as a domain user to a client host in the AD domain and is authenticated by the primary AD domain controller.
- This section uses Windows Server 2008 R2 as an example to explain how to create AD domain users and groups on the AD domain controller.

**Step 1** Log in to the Windows AD domain server. Choose **Start > Administrative Tools > Active Directory Users and Computers**. The **Active Directory Users and Computers** software is displayed.

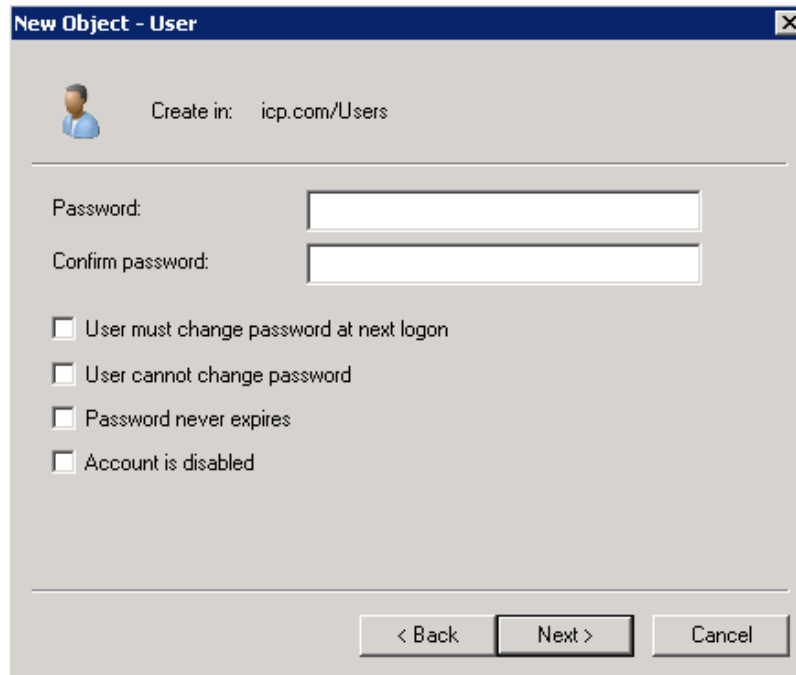
**Step 2** Create a user.

1. In the **Active Directory Users and Computers** dialog box, right-click **Users**.
2. Choose **New > User**.

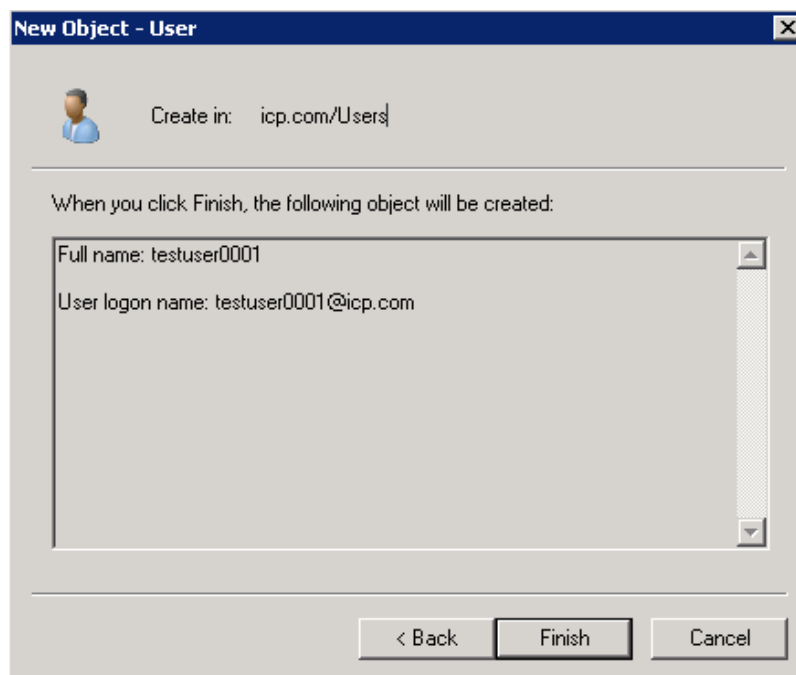


The screenshot shows the 'New Object - User' dialog box. At the top, it says 'Create in: icp.com/Users'. Below this are several input fields: 'First name:', 'Last name:', 'Full name:', 'User logon name:', and 'User logon name (pre-Windows 2000):'. The 'User logon name' field has a dropdown menu showing '@icp.com'. The 'User logon name (pre-Windows 2000)' field contains 'ICP\'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

3. Enter the domain user information.  
The user information includes **First name**, **Last name**, **Initials**, and **User logon name**. **User logon name** is used for AD domain login and authentication.
4. Click **Next** after the user information is configured.



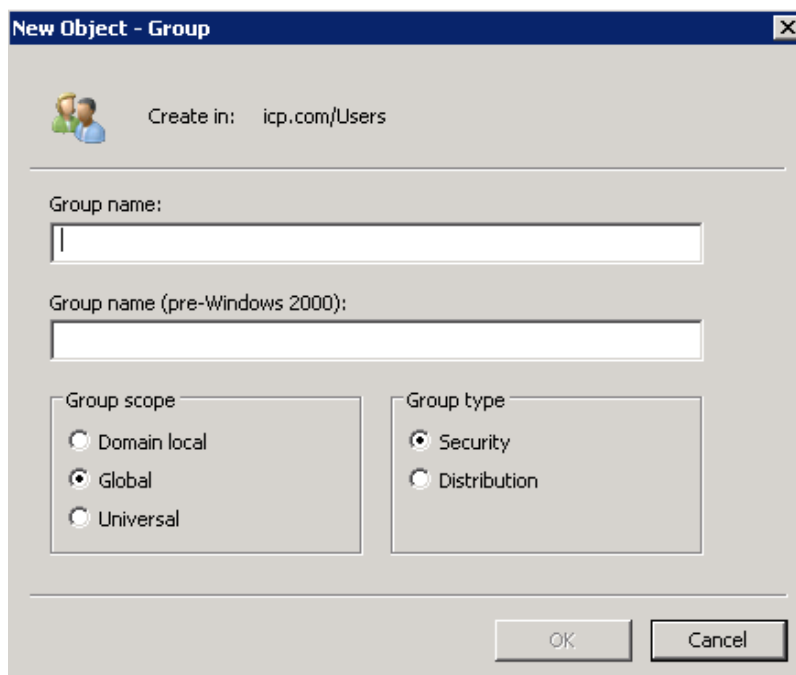
5. Enter and confirm the user password. Deselect **User must change password at next logon**. Click **Next**.



6. Click **Finish** after you confirm the user information.  
You are returned to the **Active Directory Users and Computers** dialog box.

**Step 3** Create a group.

1. In the **Active Directory Users and Computers** dialog box, right-click **Users**.
2. Choose **New > Group**.

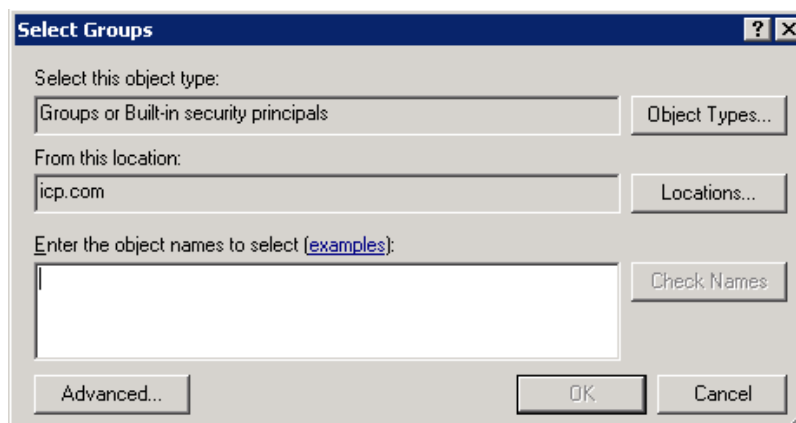


3. Enter **Group name**.
4. Set **Group scope** to **Global**.
5. Set **Group type** to **Security**.
6. Click **OK**.

You are returned to the **Active Directory Users and Computers** dialog box.

**Step 4** Add a user to a group.

1. In the **Active Directory Users and Computers** dialog box, right-click a user that you want to add to a group.
2. Select **Add to a group**.



3. In the **Enter the object name to select** text box, enter the name of the group to which the user is added.
4. Click **OK**.  
A message is displayed indicating that the operation succeeded.
5. Click **OK**.

----End

---

# A Managing Batch Configuration

---

You can import and execute a preset configuration file to batch create storage resources.

## [A.1 About Batch Configuration](#)

Batch configuration, a function provided by DeviceManager, employs configuration files to batch divide storage resources to simplify resource management, reduce management time, and significantly improve the storage resource configuration efficiency.

## [A.2 Configuration Process](#)

Before batch configuration, understand the process to ensure a smooth configuration.

## [A.3 Configuring Storage System with CLI Configuration File](#)

You can import and execute a preset configuration file to batch create storage resources. You are advised to download a configuration file template first, and then edit the template to import resources.

## [A.4 Configuring Storage System with Offline Configuration File](#)

You can import and execute a service configuration file to batch create storage resources. Service configuration file must be the .xml file generated using IT Visual Designer (ITVD).

## A.1 About Batch Configuration

Batch configuration, a function provided by DeviceManager, employs configuration files to batch divide storage resources to simplify resource management, reduce management time, and significantly improve the storage resource configuration efficiency.

- Only the super administrator can use batch configuration function. Read-only users and administrators cannot use this function.
- During Batch Configuration, CLI commands are used. You can obtain *Command Reference* of the related product to learn how to effectively use these commands.
- Currently, Batch Configuration does not support **change cli timeout=?** and **change cli silent\_enabled=no** commands.

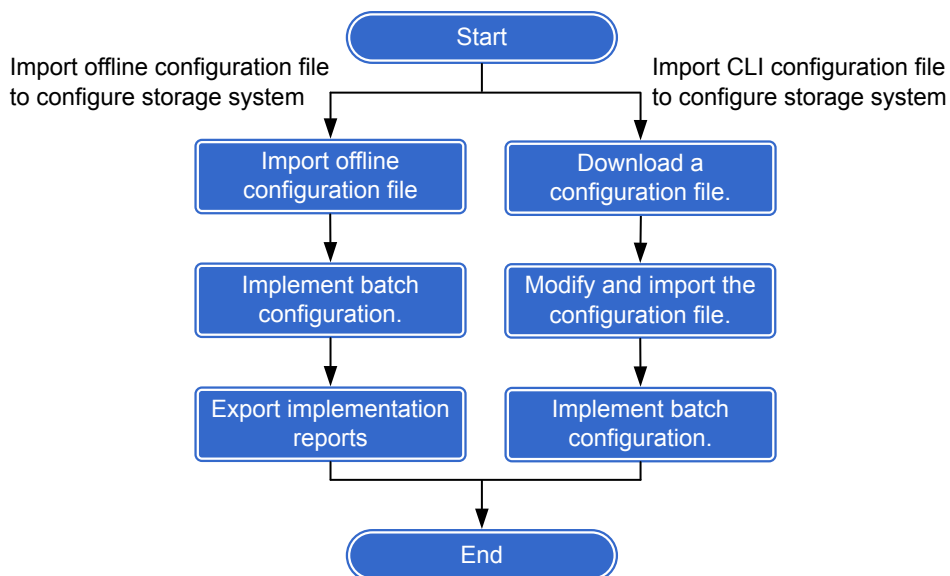
## A.2 Configuration Process

Before batch configuration, understand the process to ensure a smooth configuration.

[Figure A-1](#) shows the batch configuration process.



Figure A-1 Batch configuration process



## A.3 Configuring Storage System with CLI Configuration File

You can import and execute a preset configuration file to batch create storage resources. You are advised to download a configuration file template first, and then edit the template to import resources.

### A.3.1 Downloading a Configuration File

This operation enables you to obtain the default configuration file template.

#### Prerequisites

DeviceManager is correctly communicating with the storage device.

#### Context

The exported default configuration file template is named **Example.conf**.

#### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Batch Configuration** > **CLI**.

**Step 3** Download the configuration file.

1. Click **Configuration file template**.

If Windows Internet Explorer 8 is used, the **File Download** dialog box is displayed.

2. Click **Save**.  
The **Save As** dialog box is displayed.
3. Select the directory where you want to save the configuration file and click **Save**.

----End

## A.3.2 Importing a Configuration File

This operation enables you to batch import configuration files.

### Prerequisites

Only configuration files not being executed can be imported.

### Context

- If system check fails or is not executed during configuration file import, only the super administrator of the configuration file can import the configuration file.
- The latest imported configuration file will overwrite the earlier configuration file.
- The configuration file to be imported cannot be larger than 1 MB.

### Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Batch Configuration** > **CLI**.

**Step 3** Import the configuration files.

1. Click **Select**.  
The **Selected File to Be Loaded** dialog box is displayed.
2. Select the configuration file to be imported and click **Open**.  
The selected configuration file is displayed in the file selection area.
3. Click **Upload**.  
A message is displayed indicating that the upload succeeded.

----End

## A.3.3 Implementing Batch Configuration

This operation enables a storage system to automatically allocate storage resources based on the parameters in the configuration file to improve the storage resource configuration efficiency.

### Prerequisites

The configuration file has been imported.

### Context

- The offline configuration command can be executed only by the user who imports the configuration file.

- If the user logs out during the command execution, the storage system immediately stops the offline configuration.
- The storage system executes the commands included in the configuration file one by one.

## Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Batch Configuration** > **CLI**.

**Step 3** Click **Execute** to implement batch configuration.  
When the progress reaches 100%, the operation is successful.

----End

## A.3.4 Stopping Batch Configuration

This operation enables you to stop ongoing batch configuration at any time.

### Prerequisites

The storage system is implementing batch configuration.

### Context

Only the user who delivers the batch configuration command can stop batch configuration.

## Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Batch Configuration** > **CLI**.

**Step 3** Click **Stop**.  
The storage system stops batch configuration.

----End

## A.4 Configuring Storage System with Offline Configuration File

You can import and execute a service configuration file to batch create storage resources. Service configuration file must be the .xml file generated using IT Visual Designer (ITVD).

### A.4.1 Importing a Offline Configuration File

This operation enables you to import a service configuration file.

## Prerequisites

Only configuration files not being executed can be imported.

## Context

- If system check fails or is not executed during configuration file import, only the super administrator of the configuration file can import the configuration file.
- The latest imported configuration file will overwrite the earlier configuration file.
- The configuration file to be imported cannot be larger than 1 MB.

## Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Batch Configuration** > **Offline Configuration**.

**Step 3** Import the configuration files.

1. Click **Select**.  
The **Selected File to Be Loaded** dialog box is displayed.
2. Select the configuration file to be imported and click **Open**.  
The selected configuration file is displayed in the file selection area.
3. Click **Upload**.  
A message is displayed indicating that the upload succeeded.

---End

## A.4.2 Implementing Offline Configuration

This operation enables a storage system to automatically allocate storage resources based on the parameters in the configuration file to improve the storage resource configuration efficiency.

## Prerequisites

The configuration file has been imported.

## Context

- The offline configuration command can be executed only by the user who imports the configuration file.
- If the user logs out during the command execution, the storage system immediately stops the offline configuration.
- The storage system executes the commands included in the configuration file one by one.

## Procedure

**Step 1** Log in to DeviceManager.

**Step 2** Choose  **Provisioning** >  **Batch Configuration** > **Offline Configuration**.

- Step 3** Click **Execute** to implement offline configuration.  
When the progress reaches 100%, the operation is successful.
- End

### A.4.3 Exporting Implementation Reports

This operation enables you to stop ongoing batch configuration at any time.



#### Prerequisites

A offline configuration file has been imported and executed.

#### Context

Only the user who delivers the batch configuration command can stop batch configuration.

#### Procedure

- Step 1** Log in to DeviceManager.
- Step 2** Choose  **Provisioning** >  **Batch Configuration** > **Offline Configuration**.
- Step 3** Click **Stop**.  
The storage system stops batch configuration.
- End

# B Permission Matrix for Self-defined Roles

Functional Module	Function	Function Description	Role Group
pool	disk_domain	Creates, deletes, modifies, and queries disk domains.	System group <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
mapping_view	initiator	Creates, deletes, modifies, and queries initiators.	System group
	initiator_readonly	Query information about initiators.	System group

Functional Module	Function	Function Description	Role Group
	target	Creates, deletes, modifies, and queries targets.	System group
	target_readonly	Queries information about targets.	System group
	isns	Configures, deletes, and queries the IP address of an iSNS server.	System group
	isns_readonly	Queries the IP address of an iSNS server	System group
	mapping_view	Creates, deletes, modifies, and queries mapping views.	System group
	mapping_view_readonly	Queries information about mapping views.	System group
	lun_group	Creates, deletes, modifies, and queries LUN groups, as well as adds objects (LUNs and snapshots) to and removes objects from LUN groups.	System group
	lun_group_readonly	Queries information about LUN groups.	System group
	host_group	Creates, deletes, modifies, and queries host groups, as well adds hosts to or removes hosts from host groups.	System group
	host_group_readonly	Queries information about host groups.	System group
	host	Creates, deletes, modifies, and queries hosts, as well adds initiators to or removes initiators from hosts.	System group
	host_readonly	Queries information about hosts.	System group
	port_group	Creates, deletes, modifies, and queries port groups.	System group
	port_group_readonly	Queries information about port groups.	System group
file_system	file_system	Creates, deletes, modifies, and queries file systems.	System group, vStore group
	file_system_readonly	Query information about file systems.	System group, vStore group
quota	quota_tree	Creates, deletes, modifies, and queries quota trees in file systems.	System group, vStore group

Functional Module	Function	Function Description	Role Group
	quota_tree_readonly	Queries quota trees in file systems.	System group, vStore group
	quota	Creates, deletes, modifies, and queries quota in file systems.	System group, vStore group
	quota_readonly	Queries quota in file systems.	System group, vStore group
share	share	Creates, deletes, modifies, and queries shared services.	System group, vStore group
	share_readonly	Queries information about shared services.	System group, vStore group
file_storage_service	nfs_service	Configures and queries NFS service information.	System group, vStore group
	nfs_service_readonly	Queries NFS service information.	System group, vStore group
	cifs_service	Configures and queries CIFS service information.	System group, vStore group
	cifs_service_readonly	Queries CIFS service information.	System group, vStore group
	http_service	Configures and queries HTTP service information.	System group
	http_service_readonly	Queries HTTP service information.	System group
	ftp_service	Configures and queries FTP service information.	System group
	ftp_service_readonly	Queries FTP service information.	System group
resource_user	domain	Configures and queries domain authentication information.	System group, vStore group
	domain_readonly	Queries domain authentication information.	System group, vStore group
	resource_user	Creates, deletes, modifies, and queries authenticated users.	System group, vStore group
	resource_user_readonly	Queries information about authenticated users.	System group, vStore group
network	port	Adds, deletes, modifies, and queries ports.	System group



Functional Module	Function	Function Description	Role Group
	port_readonly	Queries information about ports.	System group, vStore group
	logical_port	Creates, deletes, modifies, and queries logical ports, as well as adds routes to or deletes routes from logical ports.	System group
	logical_port_readonly	Queries information about logical ports.	System group, vStore group
	vlan	Creates, deletes, modifies, and queries VLANs.	System group
	vlan_readonly	Queries information about VLANs.	System group, vStore group
	failover_group	Creates, modifies, deletes, and queries failover groups, as well as adds members to or removes members from failover groups.	System group
	failover_group_readonly	Queries information about failover groups.	System group, vStore group
	controller_readonly	Queries information about controllers.	System group
	interface_module_readonly	Queries information about interface modules.	System group
	dns_zone <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
local_data_protection	remote_device	Creates, deletes, modifies, and queries remote devices, as well as adds links to or deletes links from remote devices.	System group
	remote_device_readonly	Queries information about remote devices.	System group, vStore group
	remote_resource	Manages the query of remote resources (file systems and LUNs).	System group
	remote_resource_readonly	Queries remote resources (file systems and LUNs).	System group, vStore group

Functional Module	Function	Function Description	Role Group
	mirror_lun	Creates, deletes, modifies, and queries mirror LUNs, as well as adds mirror copies to or removes mirror copies from mirror LUNs.	System group
	mirror_lun_readonly	Queries information about mirror LUNs.	System group
	lun_snapshot	Creates, deletes, modifies, queries, activates, recreates, rolls back, cancels the rollback of, and creates copies for LUN snapshots.	System group
	lun_snapshot_readonly	Queries information about LUN snapshots.	System group
	lun_clone	Creates, deletes, modifies, queries, consistently splits, synchronizes, and reversely synchronizes clones, as well as adds pairs to or removes pairs from clones.	System group
	lun_clone_readonly	Queries information about clones.	System group
	fs_snapshot	Creates, deletes, modifies, queries, rolls back, and cancels the rollback of file system snapshots.	System group, vStore group
	fs_snapshot_readonly	Query information about file system snapshots.	System group, vStore group
	lun_copy	Creates, deletes, modifies, queries, suspends, continues, and stops LUN copy.	System group
	lun_copy_readonly	Queries information about LUN copy.	System group
remote_data_protection	remote_device	Creates, deletes, modifies, and queries remote devices, as well as adds links to or deletes links from remote devices.	System group
	remote_device_readonly	Queries information about remote devices.	System group, vStore group
	remote_resource	Manages the query of remote resources (file systems and LUNs).	System group
	remote_resource_readonly	Queries remote resources (file systems and LUNs).	System group, vStore group

Functional Module	Function	Function Description	Role Group
	hyper_vault	Creates, deletes, modifies, and queries HyperVault.	System group, vStore group
	hyper_vault_read only	Queries information about HyperVault.	System group, vStore group
	remote_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_pair	Creates, deletes, modifies, and queries HyperMetro vStore pairs, as well as configures consistency check for HyperMetro vStore pairs.	System group
	hyper_metro_vstore_pair_readonly	Queries information about HyperMetro vStore pairs.	System group, vStore group
	quorum_server	Creates, deletes, modifies, and queries quorum servers, as well as adds links to or removes links from quorum servers.	System group

Functional Module	Function	Function Description	Role Group
	quorum_server_readonly	Queries information about quorum servers.	System group, vStore group
resource_performance_tuning	smart_qos	Creates, modifies, deletes, and queries SmartQos policies, as well as adds objects (LUNs and file systems) to or removes objects from SmartQoS policies.	System group
	smart_qos_readonly	Queries information about SmartQoS policies.	System group
	smart_tier <sup>c</sup>	Configures and queries SmartTier polices (data migration policies or I/O monitoring policies).	System group
	smart_tier_readonly <sup>c</sup>	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 <sup>c</sup>	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 <sup>c</sup>	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
	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_read only	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>c: Function is not supported by 2000F, 5000F, 6000F, 18000F series storage systems.</p> <p>d: Function is supported by V300R006C10 storage systems.</p>			

# 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.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.

### [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.

### [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.

## 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 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

---

## A

**ASM** Automatic Storage Management

## C

**CPU** Central Processing Unit

## D

**DCL** Data Change Log

## F

**FC** Fiber Channel

## I

**ID** Identifier

**I/O** Input/Output

**IP** Internet Protocol

**iSCSI** Internet Small Computer Systems Interface

## L

**LM** LUN Migration

**LUN** Logical Unit Number

## N

<b>NL-SAS</b>	Near Line SAS
<b>R</b>	
<b>RAID</b>	Redundant Array of Independent Disks
<b>S</b>	
<b>SAN</b>	Storage Area Network
<b>SAS</b>	Serial Attached SCSI
<b>V</b>	
<b>VVol</b>	Virtual Volume
<b>W</b>	
<b>WWN</b>	World Wide Name