OceanStor S2600 Storage System

V100R001

Initial Configuration Guide

Issue 05

Date 2010-04-20

Huawei Technologies Co., Ltd. provides customers with comprehensive technical support and service. For any assistance, please 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://www.huawei.com

Email: support@huawei.com

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 the warranty of any kind, express or implied.

Contents

Figures

Tables

About This Document

Purpose

This document describes the initial configuration of the OceanStor S2600 storage system (hereinafter referred to as the S2600).

Related Versions

The following table lists the product versions related to this document.

Product Name	Version
OceanStor S2600 Storage System	V100R001

Intended Audience

This document is intended for:

- Technical support engineers
- Maintenance personnel

Organization

This document is organized as follows.

Chapter	Description
1 Process of the Initial Configuration	This chapter describes the procedure for and steps of the initial configuration of the S2600.
2 Setting up Management Environment	This chapter describes the preparations made when you set up the management environment for the S2600 and the networking.

Chapter	Description
3 Installation Configuration	This chapter describes the procedure for installing JRE and ISM.
4 Configuring the Storage System	This chapter describes the wizard, flow chart, and procedure for configuring the storage system.
5 Setting Additional Information	This chapter describes how to set the system information and alarm information.
A How to Obtain Help	This chapter describes preparations and ways of obtaining help from Huawei.
B Glossary	Lists the terms used in this document.
C Acronyms and Abbreviations	Lists the acronyms and abbreviations used in this document.

Conventions

Symbol Conventions

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

Symbol	Description
DANGER	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.
WARNING	Indicates a hazard with a medium or low level of risk, which if not avoided, could result in minor or moderate injury.
CAUTION	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
TIP	Indicates a tip that may help you solve a problem or save time.
NOTE	Provides additional information to emphasize or supplement important points of the main text.

General Conventions

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

Convention	Description
Times New Roman	Normal paragraphs are in Times New Roman.
Boldface	Names of files, directories, folders, and users are in **boldface**. For example, log in as user **root**.
Italic	Book titles are in *italics*.
`Courier New`	Examples of information displayed on the screen are in Courier New.

Command Conventions

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

Convention	Description
Boldface	The keywords of a command line are in **boldface**.
Italic	Command arguments are in *italics*.
[ ]	Items (keywords or arguments) in brackets [ ] are optional.
{ x | y | ... }	Optional items are grouped in braces and separated by vertical bars. One item is selected.
[x | y | ...]	Optional items are grouped in brackets and separated by vertical bars. One item is selected or no item is selected.
{ x | y | ... }*	Optional items are grouped in braces and separated by vertical bars. A minimum of one item or a maximum of all items can be selected.
[x | y | ...]*	Optional items are grouped in brackets and separated by vertical bars. Several items or no item can be selected.

GUI Conventions

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

Convention	Description
Boldface	Buttons, menus, parameters, tabs, window, and dialog titles are in **boldface**. For example, click **OK**.
>	Multi-level menus are in **boldface** and separated by the ">" signs. For example, choose **File** > **Create** > **Folder**.

Keyboard Operations

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

Format	Description
Key	Press the key. For example, press **Enter** and press **Tab**.
Key 1+**Key 2**	Press the keys concurrently. For example, pressing **Ctrl**+**Alt**+**A** means the three keys should be pressed concurrently.
Key 1, **Key 2**	Press the keys in turn. For example, pressing **Alt**, **A** means the two keys should be pressed in turn.

Mouse Operations

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

Action	Description
Click	Select and release the primary mouse button without moving the pointer.
Double-click	Press the primary mouse button twice continuously and quickly without moving the pointer.
Drag	Press and hold the primary mouse button and move the pointer to a certain position.

Update History

Updates between document issues are cumulative. Therefore, the latest document issue contains all updates made in previous issues.

Updates in Issue 05 (2010-04-20)

This is the fifth release. The updated contents are as follows:

Adding the description about downloading JRE of other version.

Adding the restriction description about modifying the same FC host port.

Updates in Issue 04 (2009-11-15)

This is the fourth release. The updated contents are as follows:

Bugs revised.

Updates in Issue 03 (2009-10-21)

This is the third release. The updated contents are as follows:

Chapter 4 Configuring the Storage System

Interface revised.

Updates in Issue 02 (2009-07-31)

This is the second release. The updated contents are as follows:

Chapter 1 Process of the Initial Configuration

Adding "Logging in to the CLI Through the Management Network Port".

Chapter 2 Installation Configuration

Added chapter.

Chapter 3 Configuring the Storage System

Adding related information on supporting disks larger than 2 TB.

Chapter 4 Setting Additional Information

Adding "Creating a Trap IP".

Deleting "Setting the Trap IP Address".

Bugs revised.

Updates in Issue 01 (2009-04-16)

This is the first release.

1 Process of the Initial Configuration

About This Chapter

This chapter describes the procedure for and steps of the initial configuration of the S2600.

1.1 Introduction to Initial Configuration
Initial configuration of a storage system is the basis for service running. This document provides the detailed procedure for initially configuring the S2600.

1.2 Planning the Networking
Introduction to the networking of S2600.

1.3 Installing and Checking the Hardware
Introduction to installing and checking the hardware of S2600.

1.4 Configuring the NICs or HBAs for the ASs
Introduction to configuring the NICs or HBAs for the ASs.

1.5 Setting up the Management Environment
Introduction to setting up the management environment of S2600.

1.6 Setting the IP Addresses of the Management Network Interfaces on the Controllers
Introduction to configuring the IP address of the management network interface on the S2600 controller.

1.7 Logging In to the OceanStor ISM
This section describes how to log in to the OceanStor ISM.

1.8 Discovering Array
Introduction to discovering array.

1.9 Configuring the Storage System
Introduction to configuring the S2600 storage system.

1.10 Setting Additional Information
Introduction to setting additional information for the S2600.

1.1 Introduction to Initial Configuration

Initial configuration of a storage system is the basis for service running. This document provides the detailed procedure for initially configuring the S2600.

The initial configuration consists of the following processes:

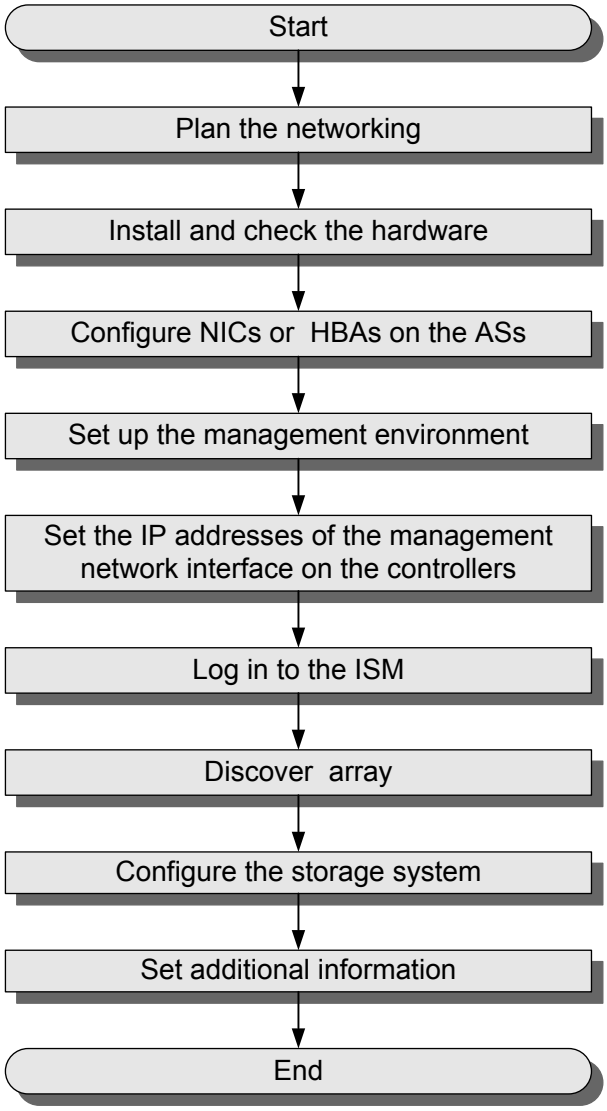
- Planning the networking
- Installing and checking the hardware
- Configuring the NICs or HBAs for the ASs
- Setting up the management environment
- Configuring the IP addresses of the management network interfaces on the controllers
- Logging in to the OceanStor ISM
- Discovering array
- Configuring the storage system
- Setting additional information

NOTE

- NIC: network interface card
- HBA: host bus adapter
- AS: application server
- IP: Internet Protocol
- ISM: Integrated Storage Management

Figure 1-1 shows the flow chart of the S2600 initial configuration.

Figure 1-1 Flow chart of the S2600 initial configuration



NOTE

The S2600 storage devices can be used for setting up the two-node system cluster environment. The cluster environment is configured in the "**1.3 Installing and Checking the Hardware**". For details, see the related documents.

NOTE

The two-node system cluster described in this document is a high available cluster. In the cluster, one node, as the primary mode, provides services; the other node, as the secondary node, runs idly or runs certain non-core applications.

1.2 Planning the Networking

Introduction to the networking of S2600.

The S2600 controller enclosures are classified into four types:

- S2600S

  The S2600S uses the Serial Attached SCSI (SAS) front-end host port.

- S2600F

  The S2600F uses the fiber channel (FC) front-end host port.

- S2600i

  The S2600i uses the Internet Small Computer Systems Interface (iSCSI) front-end host port.

- S2600C

  The S2600C uses the iSCSI and FC front-end host ports.

The S2600 is a storage system that uses a storage area network (SAN).

- The S2600S and ASs form a SAS SAN through the SAS protocol.
- The S2600F and ASs form an FC SAN through the FC protocol.
- The S2600i and ASs form an IP SAN through the iSCSI protocol.
- The S2600C and ASs form an FC SAN and an IP SAN through the FC protocol and the iSCSI protocol.

The controller of the S2600 has the following types of host ports:

- S2600S controller enclosure
  - Dual-controller

    The S2600 controller enclosure of this type is configured with two controllers. Each controller is configured with one SAS interface module. Each SAS interface module supports two SAS host ports; therefore, the S2600S controller enclosure with dual-controller is configured with four SAS host ports.
  - Single controller

    The S2600S controller enclosure of this type is configured with one controller. Each controller is configured with one SAS interface module. Each SAS interface module supports two SAS host ports; therefore, the S2600S controller enclosure with single controller is configured with two SAS host ports.
- S2600F controller enclosure
  - Dual-controller

    The S2600F controller enclosure of this type is configured with two controllers. Each controller is configured with one FC interface module. Each FC interface module supports four FC host ports. Therefore, the S2600F controller enclosure with dual-controller is configured with eight FC host ports.
  - Single controller

    The S2600F controller enclosure of this type is configured with one controller. Each controller is configured with one FC interface module. Each FC interface module supports four FC host ports. Therefore, the S2600F controller enclosure with single controller is configured with four FC host ports.
- S2600i controller enclosure
  - Dual-controller

    The S2600i controller enclosure of this type is configured with two controllers. Each controller is configured with one iSCSI interface module. Each iSCSI interface module supports four iSCSI host ports; therefore, the S2600i controller enclosure with dual-controller is configured with eight iSCSI host ports.

- Single controller

  The S2600i controller enclosure of this type is configured with one controller. Each controller is configured with one iSCSI interface module. Each iSCSI interface module supports four iSCSI host ports; therefore, the S2600i controller enclosure with single controller is configured with four iSCSI host ports.

- S2600C controller enclosure
  - Dual-controller

    The S2600C controller enclosure of this type is configured with two controllers. Each controller is configured with one Combo interface module. Each Combo interface module supports two FC host ports and two iSCSI host ports; therefore, the S2600C controller enclosure with dual-controller is configured with four FC host ports and four iSCSI host ports.
  - Single controller

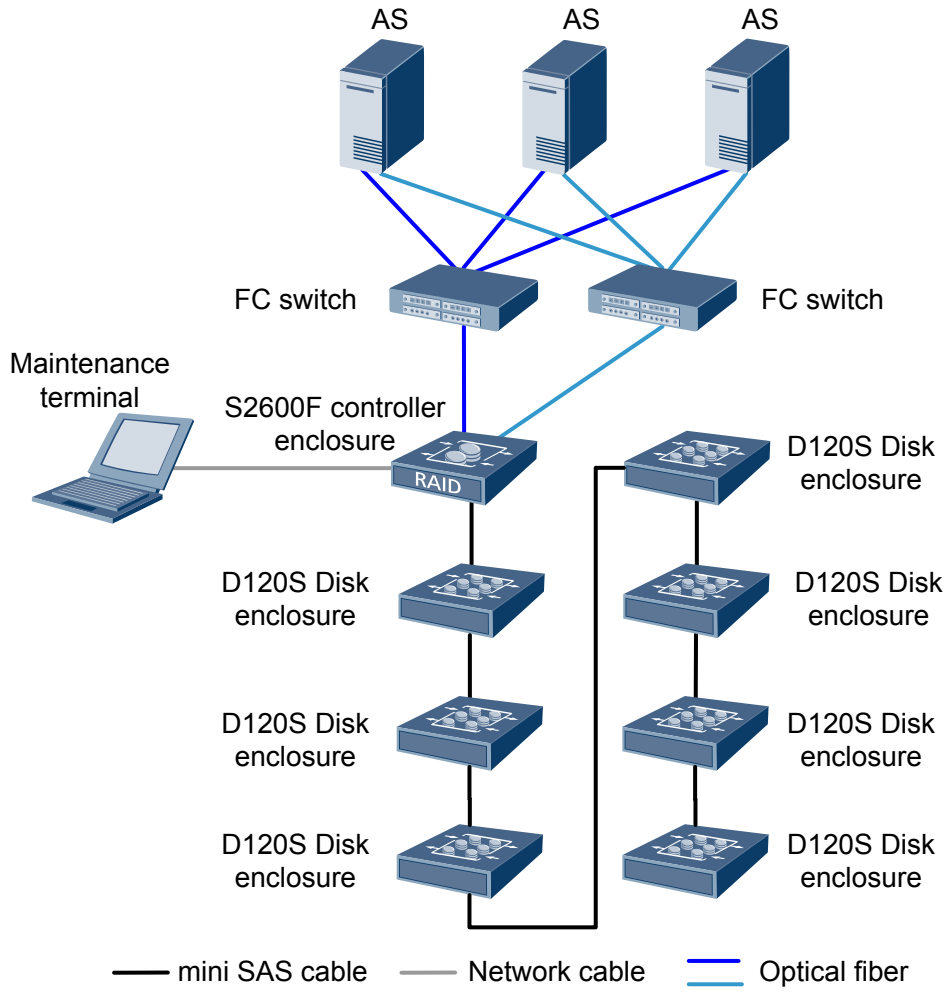
    The S2600C controller enclosure of this type is configured with one controller. Each controller is configured with one Combo interface module. Each Combo interface module supports two FC host ports and two iSCSI host ports; therefore, the S2600C controller enclosure with single controller is configured with two FC host ports and two iSCSI host ports.

NOTE

If one of the two controllers is faulty, the S2600 controller enclosure runs in single controller mode. In this case, only one controller (controller A or controller B) is present.

Figure 1-2 shows the typical networking of the S2600F configured with dual-controller.

Figure 1-2 Typical networking of the S2600F configured with dual-controller



NOTE

You can improve the service reliabilities by using the cluster in **Figure 1-2**.

The main elements shown in **Figure 1-2** are described as follows:

- S2600F controller enclosure with dual-controller
  - It provides a mature hardware platform, multiple backup protection mechanisms, global hot-spare disks, and a data verification mechanism. Besides, it supports the redundant configuration of functional modules. It can be installed in a standard 19-inch cabinet and provides the functions of performance monitoring and fault alarming.
  - With the modular design, this type of S2600F controller enclosure satisfies the requirements for system expansion.
- D120S disk enclosure

  The D120S disk enclosure works with the S2600F controller enclosure to build an intelligent storage system of high reliability, high performance, and high availability.
- AS

  The ASs such as the video surveillance AS, the streaming AS, and the data backup AS can gain access to and obtain storage resources from the S2600F.

- Maintenance terminal

  The maintenance terminal is used to log in to the management software to manage and maintain the storage resource of the S2600F.

- FC switch

  The FC switches enable more ASs to connect to the storage device.

1.3 Installing and Checking the Hardware

Introduction to installing and checking the hardware of S2600.

Installing the Hardware

CAUTION

When you install the support guide rails on the FC switch, ensure that the left and right guide rails are properly installed in correct positions. If the brackets cannot contact the FC switch properly and tightly, check whether the guide rails are installed on wrong sides. Reinstall the guide rails if they are not correctly installed.

Install the hardware in a cabinet:

- Install the S2600 controller enclosure
  - For details on how to install the S2600 controller enclosure and the uninterrupted power supply (UPS), see the *OceanStor S2600 Controller Enclosure User Guide*.
  - For details on how to install a disk enclosure, see the *OceanStor D120S Disk Enclosure User Guide*.
- Install a switch For details on how to install a switch, see the related product documents.
  - S2600F

    You need to install the FC switch.
  - S2600S

    You need to install the SAS switch or SAS switching board.
  - S2600i

    You need to install the Ethernet switch.
  - S2600C

    You need to install the FC switch and the Ethernet switch.
- Install the ASs
  - For details on how to install an AS, see the AS manual.
  - For details on how to install cluster software, see the related product documents.
- Install the maintenance terminal

  For details on how to install the maintenance terminal, see the maintenance terminal manual.

Checking the Hardware

DANGER

Before checking the correctness of the device installation and cable connection, cut off all the power supplies. This can avoid injury to your body and damage to the devices due to incorrect device installation or loose cable connection.

Check the correctness of the device installation based on the check items of device installation, as listed in **Table 1-1**.

Table 1-1 Check items of device installation

Check Item	Correct	Incorrect
S2600 controller enclosure	Placed stably at the right position	Slanted and loosened
D120S disk enclosure	Placed stably at the right position	Slanted and loosened
UPS tray	Placed stably at the right position	Slanted and loosened
Switch	Placed stably at the right position	Slanted and loosened
AS	Placed stably at the right position	Slanted and loosened
Maintenance terminal	Placed stably at the right position	Slanted and loosened

1.4 Configuring the NICs or HBAs for the ASs

Introduction to configuring the NICs or HBAs for the ASs.

Note the following items when configuring the NICs or HBAs for the ASs:

- To ensure the complete redundancy of the SAN, you are recommended to use two switches in the networking and configure two FC HBAs, two SAS HBAs, or two NICs for the ASs.
- The NICs installed on the same AS must be of the same model.
- When configuring the NIC on an AS, you need to set the IP address of the AS according to the network environment.
- When installing the driver of the FC HBA or SAS HBA, you need to choose a driver based on the compatibility list of the FC HBA or SAS HBA.

NOTE

After obtaining the information about the storage devices, OS, and system patch, you can determine the driver version according to the compatibility list of the FC HBA or SAS HBA.

CAUTION

- When the ASs are installed with the UltraPath software, you need to disable the multipath of the HBA if the multipath function is configured on the HBA. Otherwise, compatibility problems might occur.
- If you use the Qlogic FC HBA, you need to insert the optical fiber into the original host port after removing or replacing the optical fiber. Otherwise, the displayed results (such as I/O statistics in the path or the path status) that you query with the UpTools in the UltraPath may be not correct. This does not affect the communications between the ASs and the storage devices.

To configure the FC HBAs or NICs for the AS, do the follows:

- Checking compatible versions according to the OS.
- Configuring the FC HBAs, SAS HBAs, or NICs for the AS and related drivers.

1.5 Setting up the Management Environment

Introduction to setting up the management environment of S2600.

Caution

- The IP addresses of iSCSI host ports on one controller must be configured on different subnets. In addition, the IP addresses cannot be on the same network segment as that of the management network interface.
- The IP addresses of iSCSI host ports on the controller must be configured on a different network segment from the IP address (192.168.2.0/24) of the heartbeat network interface. Otherwise, an exception occurs on the network and services fail to run properly.

Procedure

Step 1 Connect the ASs, Ethernet switches, maintenance terminal, and other devices.

For details on the networking of the S2600, see "**2 Setting up Management Environment**."

Step 2 Connect the cables and fix them onto the cabinet.

Table 1-2 lists the check items of cable connection.

Table 1-2 Check items of cable connection

Check Item	Correct	Incorrect
Grounding cables	● The grounding cables of the controller enclosure, disk enclosures, and Ethernet switches are correctly connected to the grounding terminals of the cabinet. ● The ASs and maintenance terminals are grounded as required.	● The grounding cables of the controller enclosure, disk enclosures, and Ethernet switches are not correctly connected to the grounding terminals of the cabinet, or the connections are loosened. ● The ASs and maintenance terminals are not properly grounded.
Power cables	● The power supply of the UPS module is connected as required. [a] ● The UPS is connected to the controller enclosure as required. [a] ● The power supplies of the controller enclosure and disk enclosures are connected in redundancy mode. ● The Ethernet switches, ASs, and maintenance terminal are connected to their power supplies as required.	● The power supply of the UPS module is connected incorrectly. ● The UPS is incorrectly connected to the controller enclosure. ● The power supplies of the controller enclosure and disk enclosures are not connected in redundancy mode. The live, neutral, and ground wires are connected incorrectly. ● The power supplies of Ethernet switches, ASs, and maintenance terminal are not connected as required. The live, neutral, and ground wires are connected incorrectly.
SAS cable (mini SAS to mini SAS)	● Ensure that the controller enclosure and disk enclosures are properly connected according to the cascading principles. ● The interface of the mini SAS HBA of the AS is connected to the SAS host port of the controller. [b] ● The uplink connector of the mini SAS cable is inserted into the PRI expander port, and the downlink connector is inserted into the EXP expander port.	● Based on the cascading principles, the controller enclosure and disk enclosures are incorrectly connected. ● The interface of the mini SAS HBA of the AS is incorrectly connected to the SAS host port of the controller. ● The uplink connector of the mini SAS cable is incorrectly inserted into the PRI expander port, and the downlink connector is incorrectly inserted into the EXP expander port.

Check Item	Correct	Incorrect
SAS cable (mini SAS to SAS)	● The interface of the mini SAS HBA of the AS is connected to the SAS switch, and the SAS host port of the controller is connected to the SAS switch. [c] ● The interface of the SAS HBA of the AS is connected to the SAS host port of the controller. [b]	● The interface of the SAS HBA of the AS is incorrectly connected to the SAS switch, or the SAS host port of the controller is incorrectly connected to the SAS switch. ● The interface of the SAS HBA on the AS is incorrectly connected to the SAS host port of the controller.
SAS cable	The interface of the SAS HBA of the AS is connected to the SAS switch. **NOTE** For details on the SAS cables (mini SAS to mini SAS, mini SAS to SAS, and SAS), see the OceanStor S2600 Controller Enclosure User Guide.	The interface of the SAS HBA of the AS is incorrectly connected to the SAS switch.
Network cables	● The network interface of the AS is connected to the Ethernet switch, and the iSCSI host port of the controller is connected to the Ethernet switch. [d] ● The network interface of the AS is connected to the iSCSI host port of the controller [e]. ● The management network interface on each controller is connected to the network interface of the maintenance terminal. **NOTE** For details on how to connect the network cables when setting up the cluster environment, see the related product documents.	● The network interface of the AS is incorrectly connected to the Ethernet switch, or the iSCSI host port of the controller is incorrectly connected to the Ethernet switch. ● The network interface of the AS is incorrectly connected to the iSCSI host port of the controller. ● The management network interface on a controller is incorrectly connected to the network interface of the maintenance terminal.
Optical fiber [i]	● The interface of the FC HBA of the AS is connected to the FC switch, and the FC host port of the controller is connected to the FC switch. [g] ● The interface of the FC HBA of the AS is connected to the FC host port of the controller. [h]	● The interface of the FC HBA of the AS is incorrectly connected to the FC switch, or the FC host port of the controller is incorrectly connected to the FC switch. ● The interface of the FC HBA of the AS is incorrectly connected to the FC host port of the controller.

Check Item	Correct	Incorrect
Serial cables	• The CLI serial port on each controller is connected to the serial port on the maintenance terminal by a serial cable (with an RJ-45 connector at one end and a DB-9 connector at the other end). • The UPS serial port of the controller is connected to the UPS by a serial cable (with an RJ-45 connector at one end and a DB-9 connector at the other end).	• The CLI serial port on a controller is not connected to the serial port on the maintenance terminal. • The UPS serial port of the controller is not connected to the UPS.
a: The item is checked when a UPS is selected. b: The item is checked when the S2600S and ASs form the SAS SAN with the direct topology. c: The item is checked when the S2600S and ASs form the SAS SAN with SAS switches. d: The item is checked when the S2600i and ASs form the IP SAN with Ethernet switches. e: The item is checked when the S2600i and ASs form the IP SAN with the direct topology. g: The item is checked when the S2600F and ASs form the FC SAN with FC switches. h: The item is checked when the S2600F and ASs form the FC SAN with the direct topology. i: For details on how to install the small form-factor pluggable (SFP) module and optical fibers, see the *OceanStor S2600 Controller Enclosure User Guide*.		

CAUTION

During power-on, do not insert or remove hard disks, controllers, expander modules, optical fibers, optical modules, interface modules, network cables, or SAS cables. Otherwise, data may be lost.

Step 3 Power on the cabinet, UPS tray, disk enclosures, S2600 controller enclosure, switches, and ASs in turn.

NOTE

When setting up the cluster environment, you need to set the power-on parameters of each device. For details on the power-on sequence of the cluster, see the related product documents.

----End

1.6 Setting the IP Addresses of the Management Network Interfaces on the Controllers

Introduction to configuring the IP address of the management network interface on the S2600 controller.

Context

When logging in to the OceanStor ISM, you need to enter the IP of the management network interfaces on the controllers. The IP addresses of the management network interfaces on the controllers are initially 192.168.128.101 and 192.168.128.102. To change the IP address, follow the instructions below.

- To set the IP address of the management network interface of the controller on the OceanStor ISM, you need to "**1.7 Logging In to the OceanStor ISM**" and "**1.8 Discovering Array**." For details on how to set the IP address of the management network interface of the controller on the OceanStor ISM, see the *OceanStor S2600 Storage System Help*.
- To set the IP address of the management network interface of the controller in command line interface (CLI) mode:
  - When logging in to the CLI through the serial port, see the "**1.6.1 Logging in to the CLI**".
  - When logging in to the CLI through the management network port, see the "**1.6.2 Logging in to the CLI Through the Management Network Port**".

CAUTION

The IP address of the management network interface must be on a different network segment from that of the heartbeat network interface or the iSCSI host port are set.

1.6.1 Logging in to the CLI
Introduction to logging in to the CLI.

1.6.2 Logging in to the CLI Through the Management Network Port
This topic describes how to log in to the CLI through the management network port.

1.6.3 Setting and view the IP Addresses of the Management Network Interfaces on the Controllers
Introduction to setting and view the IP Addresses of the management network interfaces on the controllers.

1.6.1 Logging in to the CLI

Introduction to logging in to the CLI.

Context

CAUTION

- How to connect the controller to the maintenance terminal with a serial cable, see the *OceanStor S2600 Controller Enclosure User Guide*.
- When connecting the controller to the maintenance terminal with a serial cable, connect the serial port cable to the maintenance terminal first. When disconnecting the controller from the maintenance terminal, to avoid that the current user cannot discover the array after logging in to the OceanStor ISM, you are recommended to run the **logout** command to log out of the system. For details about the **logout** command, see the *OceanStor S2600 Storage System Command Reference*.
- After connecting the maintenance terminal to the controller with a serial cable, do not start the controller and the maintenance terminal at the same time.

After connecting the controller to the maintenance terminal with a serial cable that has an RJ-45 connector at one end and a DB-45 connector at the other end, log in to the command line interface (CLI) of the controllers by running the HyperTerminal or other programs of Windows.

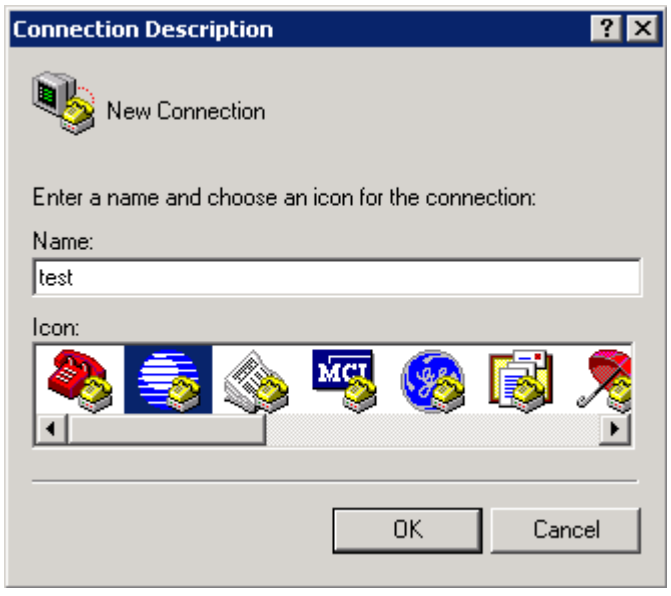
NOTE

This section describes how to log in to the CLI of the controllers through the HyperTerminal of a Windows OS, for example.

Procedure

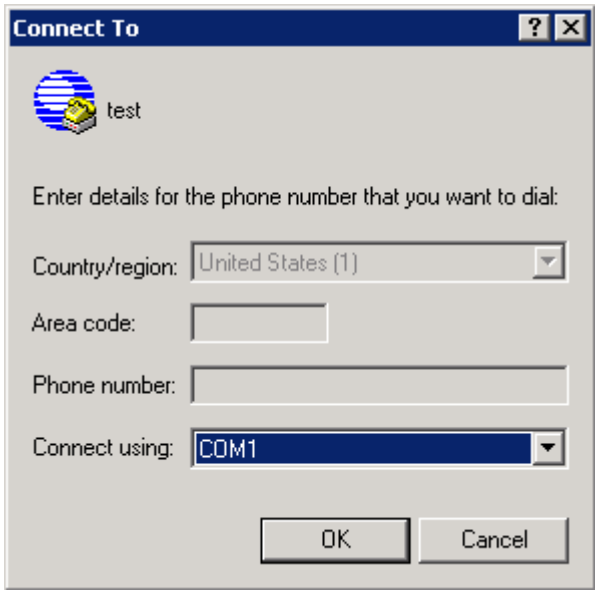
Step 1 Run the HyperTerminal of the Windows OS. A dialog box is displayed, as shown in **Figure 1-3**. Enter a name and select an icon for the new connection. Click **OK**.

Figure 1-3 Connection Description dialog box



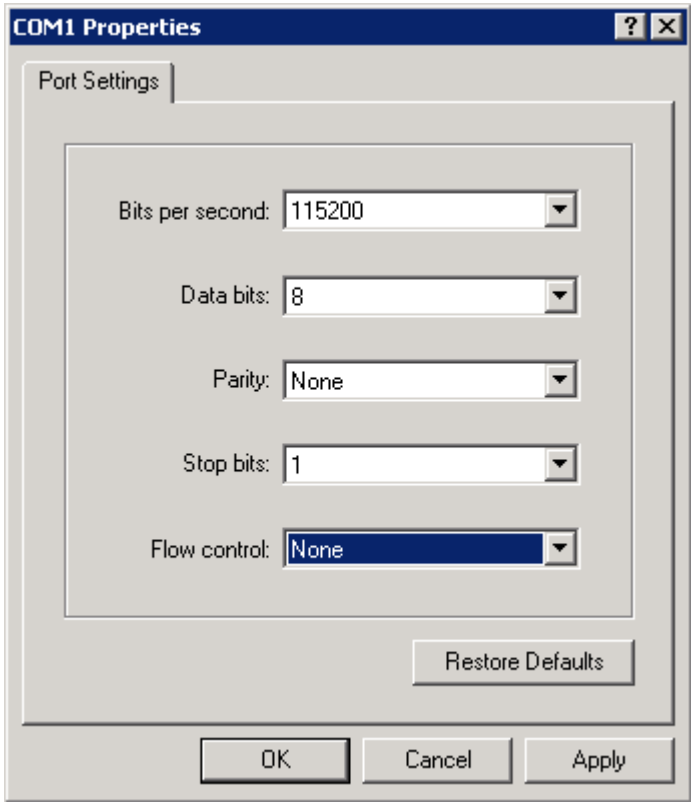
Step 2 The **Connect To** dialog box is displayed, as shown in **Figure 1-4**. In the **Connect using** drop-down list box, select the serial port to be used, for example, **COM1**. Click **OK**.

Figure 1-4 Connect To dialog box



Step 3 The system displays the **COM1 Properties** dialog box, as shown in **Figure 1-5**. Set the parameters according to**Figure 1-5** and click **OK**. The main interface of the HyperTerminal is displayed.

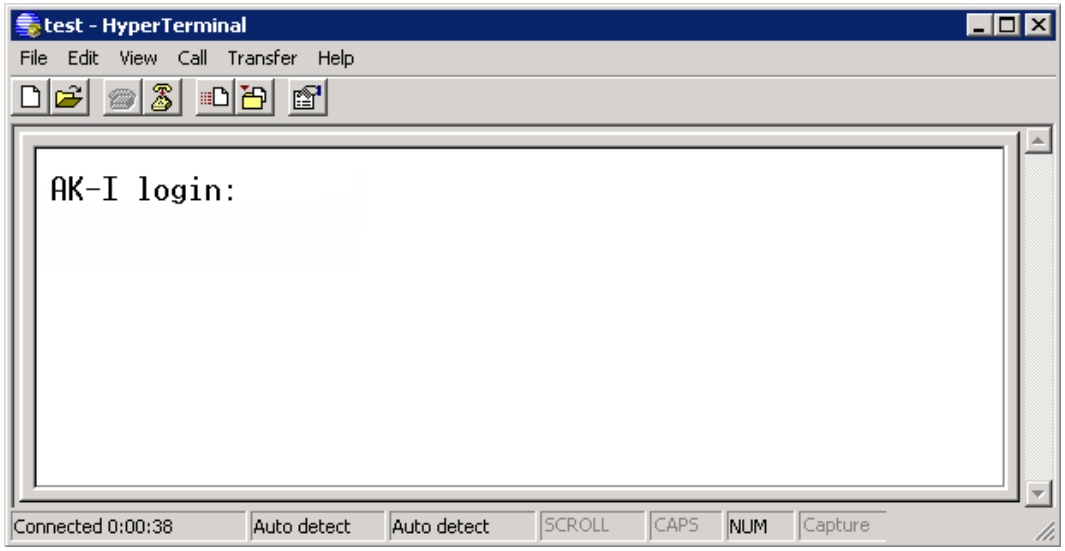
Figure 1-5 COM1 Properties dialog box



Step 4 Press **Enter**.

The interface after successful connection to the S2600 controller enclosure is displayed, as shown in **Figure 1-6**.

Figure 1-6 Interface after successful connection

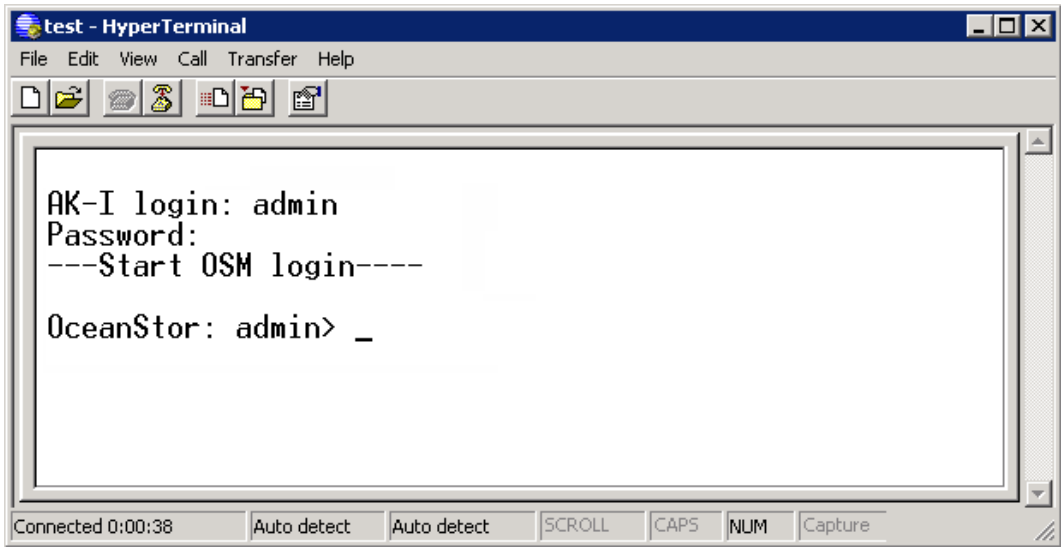


Step 5 Enter the correct user name and password. An interface indicating successful login is displayed, as shown in **Figure 1-7**.

CAUTION

The initial user name and password for the administrator of the system are **admin** and **123456** respectively. After the first login, change your password in time for security of the system.

Figure 1-7 Interface indicating successful login



----End

Result

After you are authenticated by the system successfully, you can operate in CLI mode.

1.6.2 Logging in to the CLI Through the Management Network Port

This topic describes how to log in to the CLI through the management network port.

Context

After connecting the maintenance terminal to the management network port of the controller subrack, you can log in to the CLI through the remote login software that supports the SSH protocol.

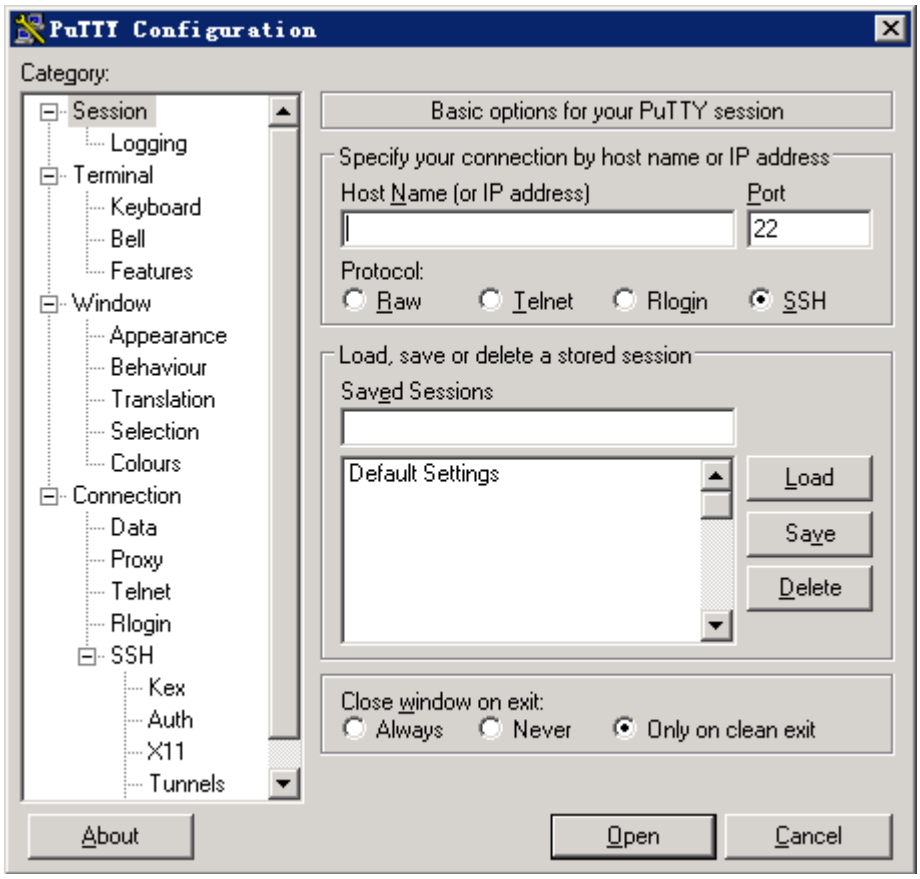
NOTE

This document takes the PuTTY software as an example. You can download the PuTTY software on related websites.

Procedure

Step 1 Run the PuTTY software and the **PuTTY Configuration** dialog box is displayed, as shown in **Figure 1-8**.

Figure 1-8 PuTTY configuration



Step 2 Enter the IP address of the management network port in **Specify your connection by host name or IP addressHost Name (or IP address)**. Select **Protocol** as **SSH**.

NOTE

The default IP addresses of the management network port is 192.168.128.101/16 .

Step 3 Click **Open** and the displayed interface is as shown in **Figure 1-9**.

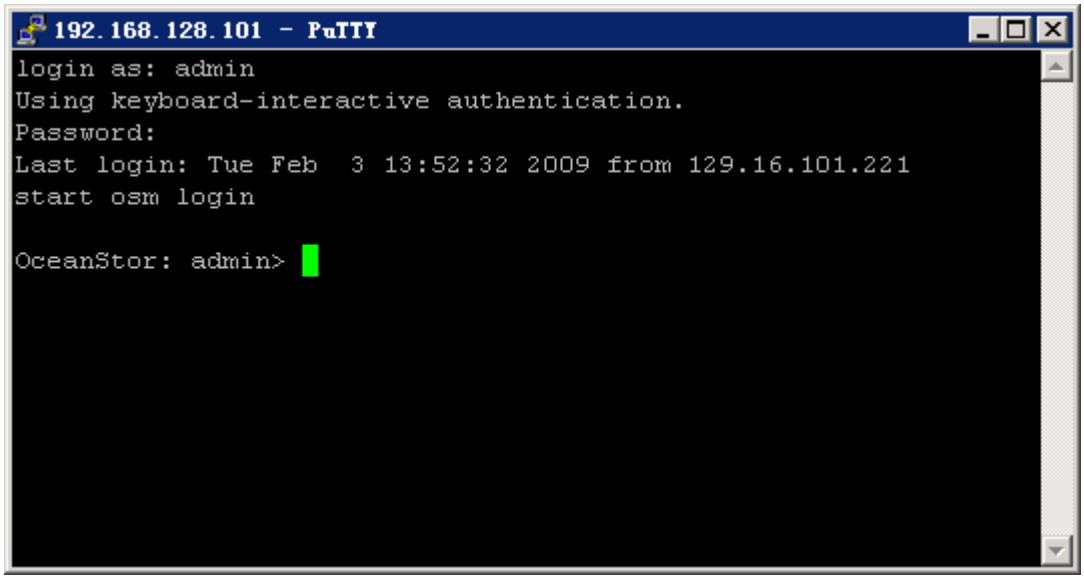
Figure 1-9 Logging to the server through the PuTTY software

Step 4 Enter the user name and the password in the prompt of the CLI interface, as shown in **Figure 1-10**.

CAUTION

The initial user name and password for the administrator of the system are **admin** and **123456** respectively. After the first login, change your password in time for security of the system.

Figure 1-10 Interface of successful login



Step 5 The user successfully logs in and enters the CLI mode.

----End

1.6.3 Setting and view the IP Addresses of the Management Network Interfaces on the Controllers

Introduction to setting and view the IP Addresses of the management network interfaces on the controllers.

Setting the IP Addresses of the Management Network Interfaces on the Controllers

In CLI mode, run the chgctrlip command to set the IP addresses of the management network interfaces on the controllers.**Table 1-3** lists the syntax and parameter description of the chgctrlip command.

Table 1-3 Syntax and parameter description of the chgctrlip command

Syntax	Parameter Description
chgctrlip -c *controller ID* { **-a** *IP address* | **-s** *subnet mask* | **-g** *gateway* } *	• **-c** *controller ID*: indicates the ID of a controller. The value is a or b. a stands for controller A, b stands for controller B. • **-a** *IP address*: indicates the IP address of the management network interface on a controller. • **-s** *subnet mask*: indicates the subnet mask. • **-g** *gateway*: indicates the gateway.

For example, set the IP address of the management network interface on controller A. Set the IP address to 10.147.124.238, subnet mask to 255.255.254.0, and gateway to 10.147.124.1.

```
OceanStor: admin> chgctrlip -c a -a 10.147.124.238 -s 255.255.254.0 -g 10.147.124.1
```

View the IP Addresses of the Management Network Interfaces on the Controllers

After running the chgctrlip command to set the IP address of the management network interface on the controller, you can run the showctrlip command to view the IP address of the management network interface.**Table 1-4** describes the syntax and parameters of the showctrlip command.

Table 1-4 Syntax and parameter description of the showctrlip command

Syntax	Parameter description
showctrlip [**-c** *controller ID*]	• **-c** *controller ID*: controller ID. The value is a or b. a stands for controller A, and b stands for controller B.

Before running the showctrlip command, note that? ?

- **showctrlip**: queries the IP addresses for all controllers.
- **showctrlip -c** *controller ID*: queries the IP address for a specified controller.

For example, query the IP addresses of the management network interfaces on all controllers.

```
OceanStor: admin> showctrlip
  Controller  IP Address       Subnet Mask      Gateway          MAC Address
           A  129.26.10.31     255.255.0.0      0.0.0.0          00:12:34:56:70:46
           B  129.26.10.32     255.255.255.0    0.0.0.0          00:12:34:56:79:92
```

After completing the previous operations, to enable that the user can discover an array after logging in to the OceanStor ISM, you are recommended to run the logout command to log out of the CLI. For detail on the logout command, see the *OceanStor S2600 Storage System Command Reference*.

For details on how to set and view the IP address of the management network interface, see the *OceanStor S2600 Storage System Command Reference*. If any exception occurs when you set the IP addresses for the management network interface, contact Huawei for technical support. For details on how to obtain help, see "**A How to Obtain Help**"

1.7 Logging In to the OceanStor ISM

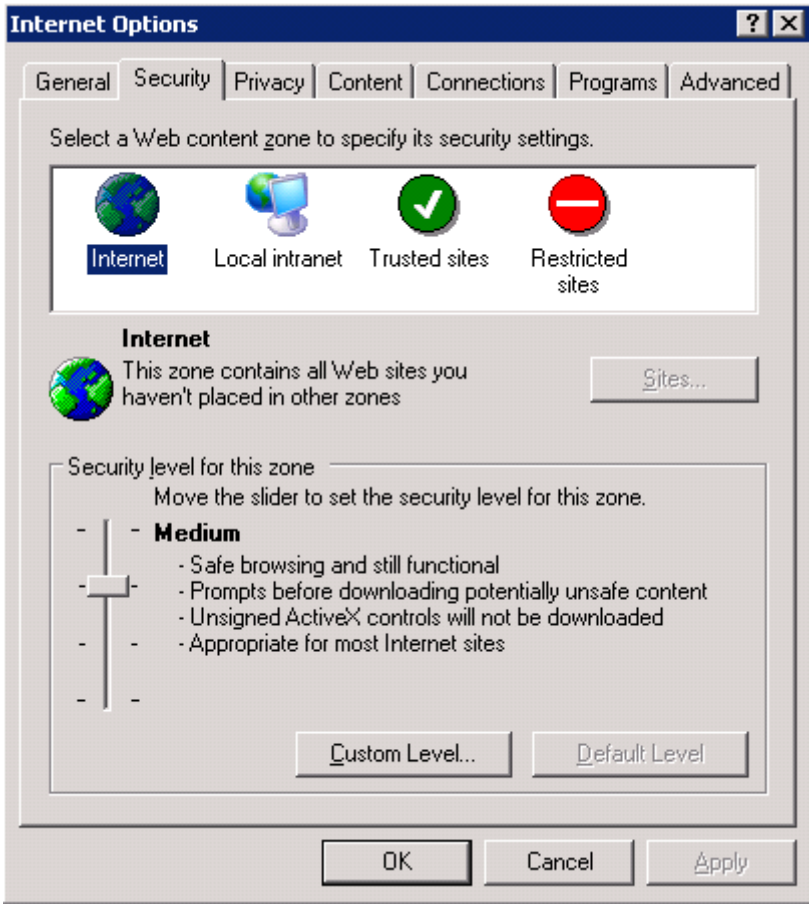
This section describes how to log in to the OceanStor ISM.

Prerequisite

If you install Windows 2003 or Windows XP on the client, you should add the IP address of the management network ports on the controller to the zone of trusted sites, make sure the interface display normally. Do as follows.

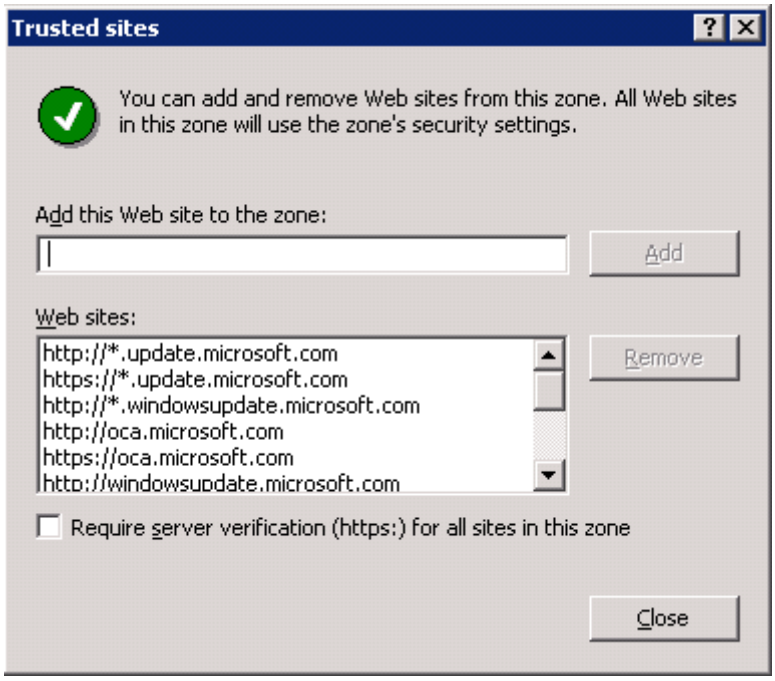
1. Run the IE. On the menu bar, choose **Tools** > **Internet Options...**.
2. In the **Internet Options** dialog box, select the **Security** tab, the dialog box is displayed as shown in **Figure 1-11**.

Figure 1-11 Internet Options dialog box



3. Click **Trusted sites**, and then click **Sites...**, the **Trusted sites** dialog box is displayed as shown in **Figure 1-12**.

Figure 1-12 Trusted sites dialog box



4. Enter **http://XXX.XXX.XXX.XXX** in the **Add this Web site to the zone**, **XXX.XXX.XXX.XXX** is the IP address of downloading the OceanStor ISM.
5. Click **Add**.
6. Click **Close**, the **Trusted sites** dialog box is closed.
7. Click **OK**, the **Internet Options** dialog box is closed.

Context

This section takes the **Admin** user that logs in to the OceanStor ISM in Windows OS as an example.

- When you log in to the OceanStor ISM, the default user name is**admin**and the default password is**123456**. After Logging in to the OceanStor ISM, modify the default password in time.
- After logging in to the OceanStor ISM, if you perform no operations within ten minutes, the system locks the OceanStor ISM automatically. To log in to the OceanStor ISM again, reenter the password.

Table 1-5 lists the OSs supported by the OceanStor ISM.

Table 1-5 OSs supported by the OceanStor ISM

OS	Browser Version
Microsoft Windows XP	● Internet Explorer 5.5 ● Internet Explorer 6.x ● Netscape 6.2x ● Netscape 7 ● Mozilla 1.4 or later ● Firefox
Microsoft Windows 2003	● Internet Explorer 5.5 ● Internet Explorer 6.x ● Netscape 6.2x ● Netscape 7 ● Mozilla 1.4 or later ● Firefox
RedHat Enterprise Linux AS5	● Netscape 6.2x ● Netscape 7 ● Mozilla 1.4 or later
SUSE Linux Enterprise Server 10	● Netscape 6.2x ● Netscape 7 ● Mozilla 1.4 or later
Solaris 10(x86)	Mozilla 1.4 or later

When the IP addresses of the maintenance terminal and the management network port are not in the same network segment, you need to set the routing for the controller. In this way, the maintenance terminal can remotely access and maintain storage arrays. Uses can set the routing about the controller in the following methods:

- Setting the routing of the controller through the OceanStor ISM interface

  For details , see the *OceanStor S2600 Storage System User Guide*.
- Setting the routing of the controller through the CLI

  For details , see the *OceanStor S2600 Storage System Command Reference*.

CAUTION

- Before install the OceanStor ISM, install the Java Runtime Environment (JRE) software. Ensure that the version of the JRE is JRE 5.0 or later (except JRE 5.0.16).
- JRE 5.0.16 has defects (see http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=6746185) , therefore , to avoid failing to download the OceanStor ISM, do not use the JRE with the version 5.0.16.

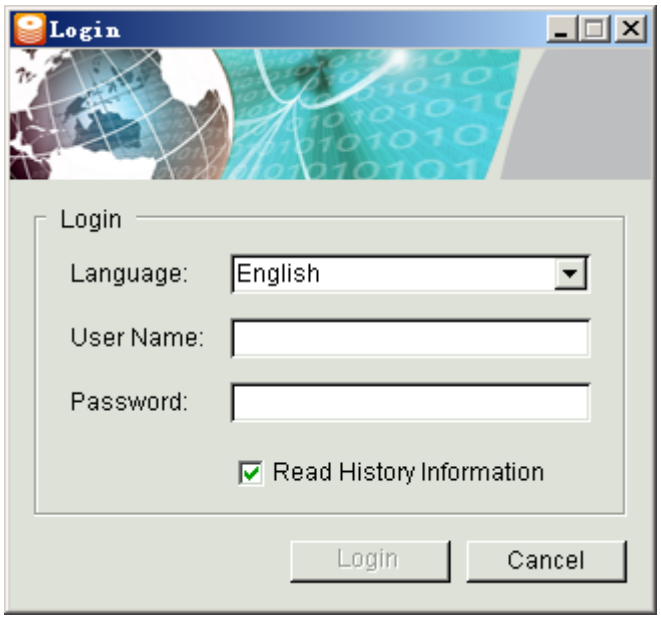
Procedure

Step 1 Install the JRE and the OceanStor ISM.

For details on installing the JRE and the OceanStor ISM, see **3.1 Installing the JRE**.

Step 2 Run the OceanStor ISM. The system displays the **Login** dialog box, as shown in **Figure 1-13**.

Figure 1-13 Login dialog box



Step 3 In **Language**, choose a proper language.

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

Step 5 In **Password**, enter the user password.

NOTE

- When you log in to the OceanStor ISM for the first time, **Read History Information** is disabled.
- When you have logged into the OceanStor ISM and successfully discovered arrays before, after you select **Read History Information**, the system can automatically connect arrays according to the IP addresses of arrays in the history configuration files. In the configuration files, the arrays that are discovered the last time you logged in and exist are displayed as nodes in the navigation tree.

Step 6 Click **Login** or press **Enter**. The system goes to the OceanStor ISM welcome interface.

Click **Discover Array**. The system displays the **Discover Array** dialog box. For details on discovering arrays, see **1.8 Discovering Array**.

----End

1.8 Discovering Array

Introduction to discovering array.

Procedure

Step 1 Log in to the OceanStor ISM, the welcome interface is displayed. See **Figure 1-14**.

Figure 1-14 Welcome interface

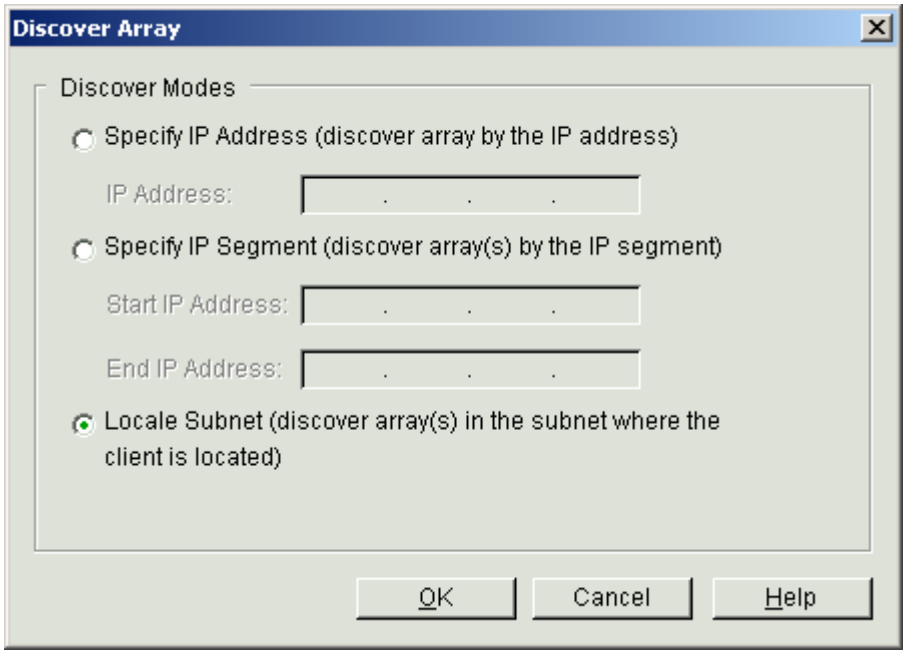
NOTE

- If you click the **Close** button, as shown in **Figure 1-14**, the OceanStor ISM interface is displayed. Only System and Help are displayed on the menu bar.
- If you plan to manage the storage system, choose **System** > **Discover Array...** on the menu bar. The **Discover Array** interface is displayed. See **Figure 1-15**.

Step 2 On the interface as shown in **Figure 1-14**, click **Discover array**.

The **Discover Array** interface is displayed, as shown in **Figure 1-15**.

Figure 1-15 Discover Array interface



Step 3 Select a discover mode as required.

Table 1-6 describes the parameters for discovering a storage array.

Table 1-6 Parameters for discovering a storage array

Parameter	Description
Specify IP Address	It indicates that the system starts the discovery based on the specified IP address of the management network interface on a storage array. When setting this parameter, note that: ● The first field on the left ranges from 1 to 223 (excluding 127). ● The last field ranges from 1 to 254. ● The other fields range from 0 to 255.
Specify IP Address Range	It indicates that the system starts the finding based on the specified IP address range of the management network interfaces on a storage array. **Start IP Address** and **End IP Address** indicate the start point and the end point for discovering a device. When setting this parameter, note that: ● The first field on the left ranges from 1 to 223 (excluding 127). ● The last field ranges from 1 to 254. ● The other fields range from 0 to 255. ● The value of **Start IP Address** must be smaller than or equal to the value of **End IP Address**. [a]

Parameter	Description
Locale Subnet	The parameter indicates that the discovering range is the subnet segment of the IP address where the OceanStor ISM client is located. By default, this parameter is enabled.
a: When you compare the two IP addresses, whose value of the first field is larger, the IP address is larger. When the values of the first fields are the same, whose value of the second field is larger, the IP address is larger. When the values of the second fields are the same, compare the values of the third fields with the same method.	

Step 4 Click **OK**.

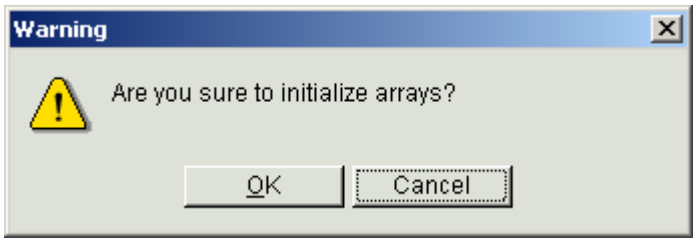
After the storage array is discovered successfully, the **Info** dialog box is displayed, saying "`Operation succeeded.`". See **Figure 1-16**.

Figure 1-16 Info dialog box

Step 5 Click **OK**.

The **Warning** dialog box is displayed, as shown in **Figure 1-17**.

Figure 1-17 Warning dialog box



Step 6 If you perform the initialization configuration on the S2600, click **OK**. The **Initial Configuration Wizard: Welcome** interface is displayed. For details on how to discover a storage array, see "**4.1 Configuration Wizard**". If you do not perform this operation, perform **Step 7**.

Step 7 Click **Cancel**.

NOTE

All the discovered storage arrays are displayed in the navigation tree.

----End

1.9 Configuring the Storage System

Introduction to configuring the S2600 storage system.

For details on the initial configuration of the S2600, see "**4 Configuring the Storage System**".

1.10 Setting Additional Information

Introduction to setting additional information for the S2600.

For details on how to set additional information about the S2600, see "**5 Setting Additional Information**".

2 Setting up Management Environment

About This Chapter

Introduction to preparations made before setting up a management environment and typical networking for the S2600.

2.1 Preparations

Introduction to the preparations made before setting up a management environment, including list of devices and networking configuration.

2.1.1 List of Devices

Introduction to the list of devices.

Before configuring the S2600, you need to configure the networking.

- S2600S

  The system uses the SAS SAN networking mode and the ASs access the data in the storage system over the SAS protocol.
- S2600F

  The system uses the FC SAN networking mode and the ASs access the data in the storage system over the FC protocol.
- S2600i

  The system uses the IP SAN networking mode and the ASs access the data in the storage system over the iSCSI protocol.
- S2600C

  The system uses the FC SAN+IP SAN networking mode and the ASs access the data on the storage system over the FC or iSCSI protocol.

Table 2-1 lists the devices required for the typical networking of the S2600.

Table 2-1 List of devices required for typical networking

Device	Description
S2600	● S2600 controller enclosure ● D120S disk enclosure ● UPS tray
AS	The ASs on which a Windows/Linux/IBM AIX/HP Unix/SUN Solaris OS is installed **NOTE** You can choose the AS that is installed with the cluster software or that is configured with the cluster function.

Device	Description
Switch	● S2600S: SAS switch ● S2600i: Ethernet switch ● S2600F: FC switch ● S2600C: FC switch and Ethernet switch
Cables	● Network cable ● SAS cable (mini SAS to mini SAS) ● SAS cable (mini SAS to SAS) ● SAS cable ● Serial cable with a DB-9 connector at one end and an RJ-45 connector at the other end ● Optical fiber
Others	Maintenance terminal

2.1.2 Networking Configuration

Introduction to networking configuration of the S2600.

In networking, you can select the ASs, SAS HBAs/FC HBAs/NICs, and Ethernet switches as required.

NOTE

For the controller enclosure of the S2600S, S2600F, or S2600i with dual-controller,

- To ensure the complete redundancy of the SAN, you are recommended to use two switches in the networking and configure two SAS HBAs, two FC HBAs, or two NICs on the ASs.
- The SAS HBAs, FC HBAs, or NICs to be installed on the same AS must be of the same model.

NOTE

For the S2600C controller enclosure with dual-controller,

- For the iSCSI networking: The NICs to be installed on the same AS must be of the same model. To improve the service performance, you are recommended to configure Gigabit NICs on the ASs and configure the Gigabit Ethernet switches.
- For the FC networking: The FC HBAs to be installed on the same AS must be of the same model.

Table 2-2 lists the recommended configurations for the devices used in the networking. They are for your reference.

Table 2-2 Recommended configurations for the devices

Device	Recommended Configuration
AS	Huawei server blade BH22: ● Two Intel Xeon 3 GHz processors ● Two 1 GB memories IBM Server 7969-IEF: ● Two AMD opteron 252-2.6 GHz processors ● Two 1 GB memories DELL PE2950: ● Two Xeon 2.6 GHz processors ● Two 1 GB memories
SAS HBA	LSI 1068E HBA (SAS3442E-R) **NOTE** For details on how to configure a SAS HBA, see "**1.4 Configuring the NICs or HBAs for the ASs**".
NIC	● Intel Pro/1000 MT Server Adapter that needs a driver of version 5.3.42.0 or later. ● Broadcom NetXtreme Gigabit Ethernet that needs a driver of version 9.52.0.0 or later.
FC HBA	The FC HBA and its driver are delivered with the AS. **NOTE** For details on how to configure an FC HBA, see "**1.4 Configuring the NICs or HBAs for the ASs**".
OS of the AS	● Windows: Windows Server 2003 SP (Service Pack) 1/Windows 2003 ● Linux: SLES (SuSE Linux Enterprise Server) 9 SP3 (with Linux kernel 2.6.5)/RedHat AS4 (with Linux kernel 2.6.9) ● Unix: IBM AIX/HP Unix/SUN Solaris **NOTE** Contact Huawei technical support engineers for obtaining the latest OS compatibility list.
Initiator version	● Windows: Microsoft iSCSI Initiator of version 2.0.1 or later ● Linux: the rpm package compatible with the actual version
Ethernet switch	● Huawei switch blade NX20 **NOTE** Huawei switch blade must work with Huawei server blade. ● Huawei Quidway S5516 and Quidway S2600, both of which are Gigabit switches.

Device	Recommended Configuration
FC switch	• Huawei switch blade NX20 **NOTE** A Huawei switch blade must work with a Huawei server blade. • Brocade SilkWorm 240E
SAS switch (blade)	Huawei switch blade NX20 **NOTE** A Huawei switch blade must work with a Huawei server blade.

2.2 Networking Model

Introduction to the typical networking of S2600.

NOTE

- In the networking diagram described in this section, the S2600 controller enclosure stands for the S2600 storage system. (D120S disk enclosures are not connected to the S2600 controller enclosure.)
- In this document, all the networking modes are described by taking the S2600 with dual-controller as an example. You can refer to these modes to configure the networking that the S2600 with single controller.

2.2.1 Networking Modes of the S2600S

Introduction to the networking modes of the S2600S.

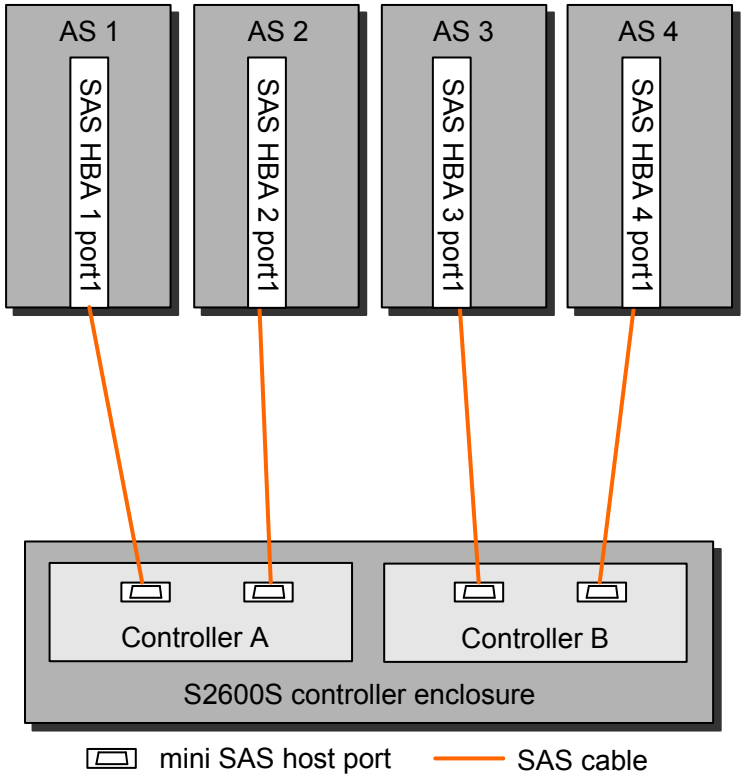
NOTE

In the S2600S networking, SAS HBAs or mini SAS HBAs are installed on ASs. In this section, the SAS HBAs are described as an example. The SAS cables used in the networking may include the mini SAS to mini SAS, mini SAS to SAS, and SAS cable. In this section, the SAS cable is described as an example.

Dual-controller + ASs with Single SAS HBA + Direct Topology

Figure 2-1shows the networking of dual-controller + ASs with single SAS HBA + direct topology.

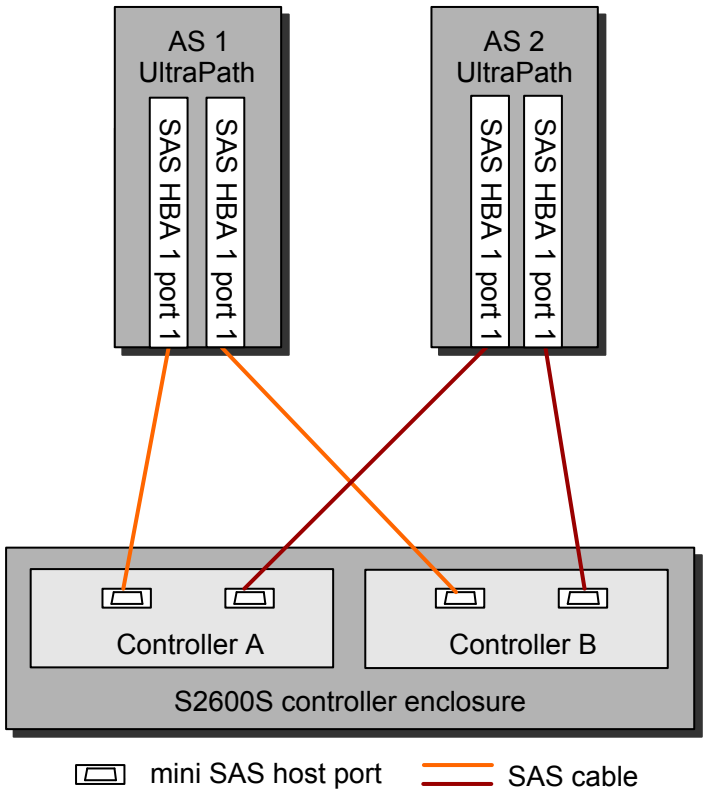
Figure 2-1 Networking of dual-controller + ASs with single SAS HBA + direct topology



Dual-controller + ASs with Double SAS HBAs + Direct Topology

Figure 2-2 shows the networking of dual-controller + ASs with double SAS HBAs + direct topology.

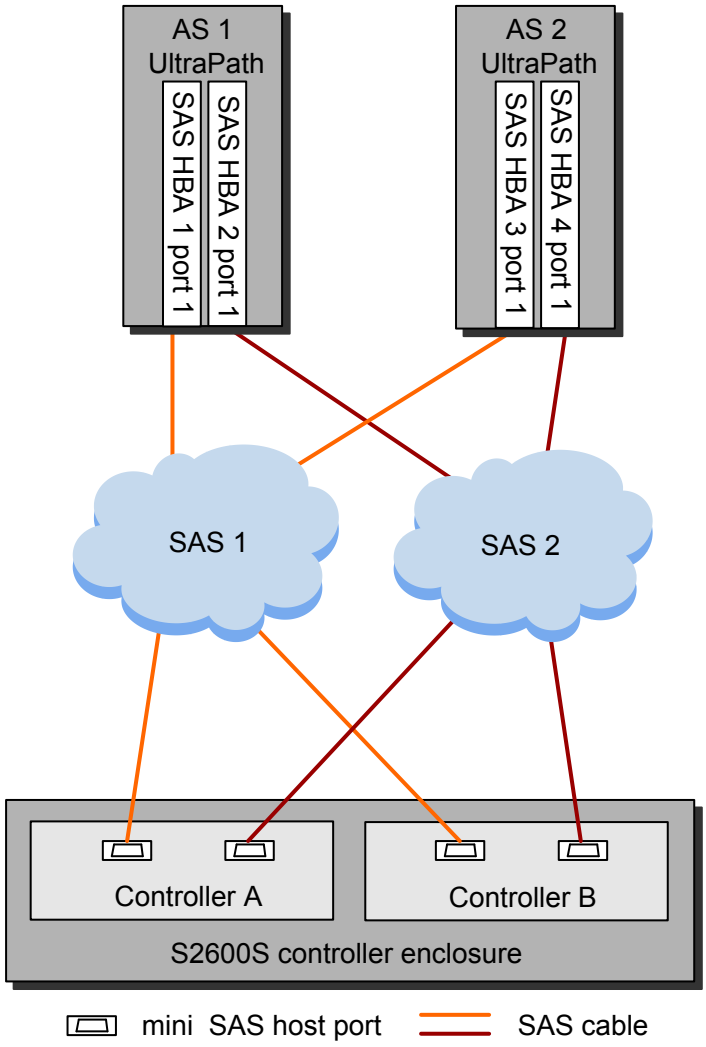
Figure 2-2 Networking of dual-controller + ASs with double SAS HBAs + direct topology



Dual-controller + ASs with Double SAS HBAs + Two SAS Switches

Figure 2-3 shows the networking of dual-controller + ASs with double SAS HBAs + two SAS switches.

Figure 2-3 Networking of dual-controller + ASs with double SAS HBAs + two SAS switches



Cluster Networking with Dual-controller

NOTE

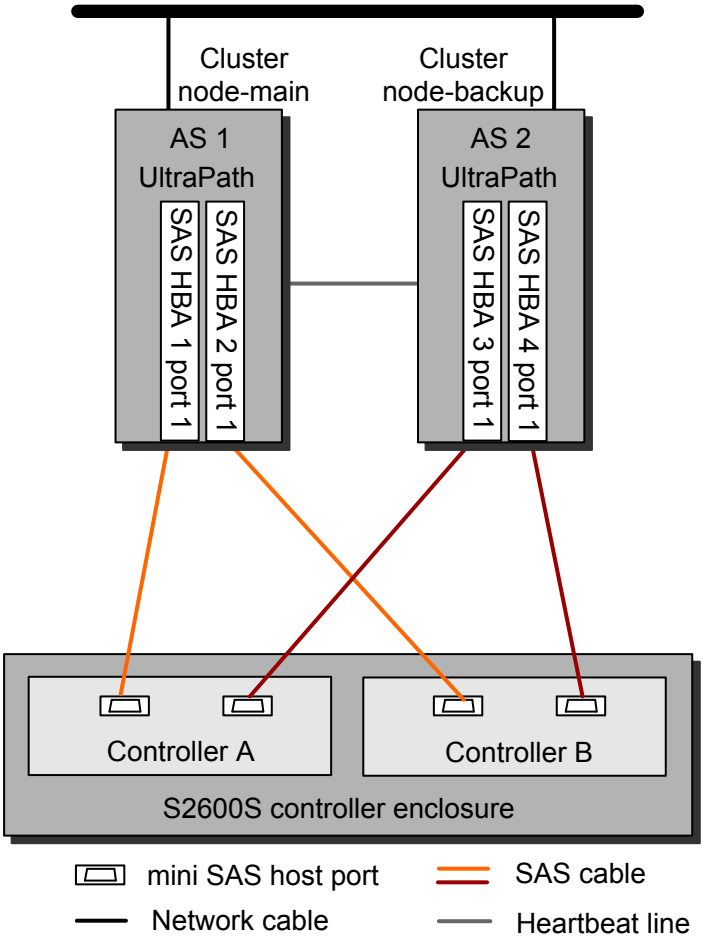
- In this document, the service segment IP addresses on the storage device side are configured to 192.168.0.0/19 for setting up the two-node system cluster environment.
- For Windows OS, the primary node and the secondary node are in the same domain.

CAUTION

When you set up the two-node system cluster environment of Windows Server 2003 based on the related typical networking, after adding a mapping to the host group to which the cluster belongs, you are recommended to restart the secondary node before initially switching over the cluster owning node. If you do not restart the secondary node, double-click **My Computer**, the new drive letters are not displayed. This, however, does not affect the normal use of LUNs.

Figure 2-4 shows the networking of dual-controller + ASs with double SAS HBAs + clusters + direct topology.

Figure 2-4 Networking of dual-controller + ASs with double SAS HBAs + clusters + direct topology



2.2.2 Networking Modes of the S2600F

Introduction to the networking modes of the S2600F.

Networking Principles

Proper networking ensures that storage devices and services run properly. Therefore, you need to choose the networking mode as required.

NOTE

- When the S2600 works with two switches, you need to install the UltraPath on the ASs. This improves the security, reliability, and maintainability of data storage and ensures the security of the path between the ASs and the S2600.
- For details on how to configure the zone for FC switches, see the user manuals of FC switches.

To configure the FC SAN for the ASs installed with the UltraPath, you need to comply with the following networking principles:

- One zone is configured with one FC HBA. This facilitates the isolation of packets, for example, the registered state change notification (RSCN) packet.
- To avoid the interference caused by a damaged FC HBA or the impact on the original networking caused by system expansion, you are recommended to use the small zone mode. In other words, the two interfaces of one path through the FC switch form one zone.
- Only one path is set from one FC HBA of an AS to one controller of the S2600.
- To avoid the single point failure of the FC switch, one controller of the S2600 must be connected to two FC switches.

NOTE

For the FC networking,

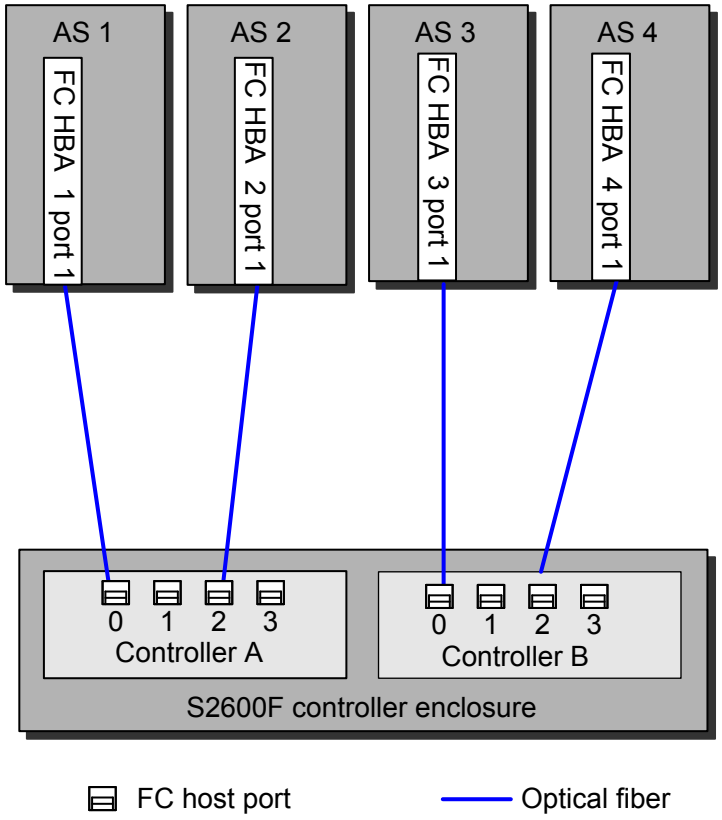
- In this document, each Fabric can be regarded as one FC switch.
- To ensure the complete redundancy of the SAN, you are recommended to use the dual-Fabric networking.
- If an FC HBA contains multiple interfaces, each interface has a unique world wide name (WWN).

Dual-controller + ASs with Single FC HBA + Direct Topology

Typically, the eight host ports of the controller enclosure connect directly without using an FC switch. Because the application scenarios prove that the controller with a 4-interface FC module (an FC interface module supports four FC host ports) can support more ASs, reduce the number of FC switches, and cut down on the costs.

Figure 2-5 shows the networking of dual-controller + ASs with single FC HBA + direct topology.

Figure 2-5 Networking of dual-controller + ASs with single FC HBA + direct topology



In this networking, the eight FC host ports can support eight ASs that use one FC HBA. Each AS has only one FC HBA and the networking does not use an FC switch. Therefore, the AS uses only one path to connect to the S2600. You do not need to install the UltraPath.

NOTE

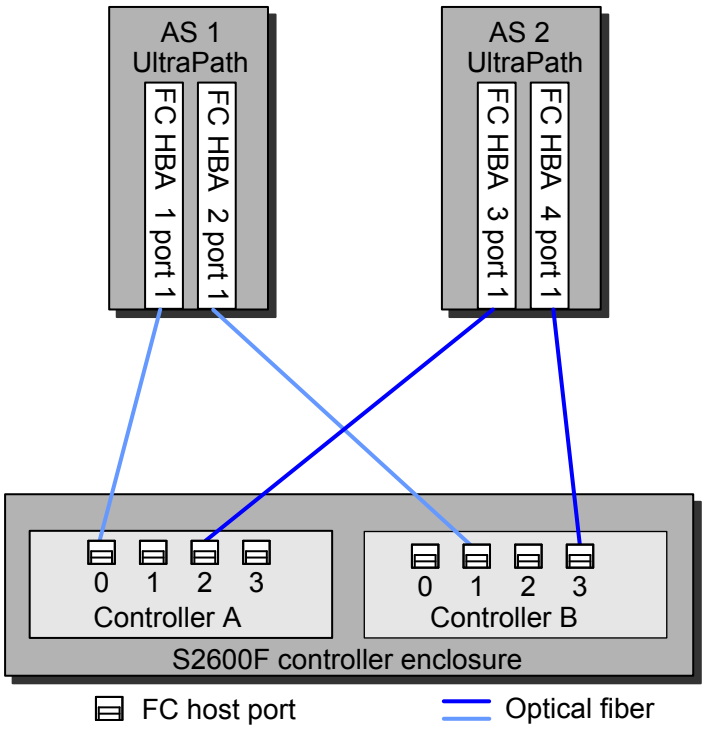
In this networking, if the UltraPath is installed on the AS, the I/O performance of the AS falls.

In this networking, when you create a LUN, you are recommended to set the ascription controller of the LUN to the controller that connects to the host path.

Dual-controller + ASs with Double FC HBAs + Direct Topology

Figure 2-6 shows the networking of dual-controller + ASs with double FC HBAs + direct topology.

Figure 2-6 Networking of dual-controller + ASs with double FC HBAs + direct topology



In this networking, the AS must be installed with the UltraPath, and you need to connect the two paths to two different controllers separately.

In **Figure 2-6**, each AS has only one path connecting to one controller. The networking does not support the load balancing but supports the failover/failback.

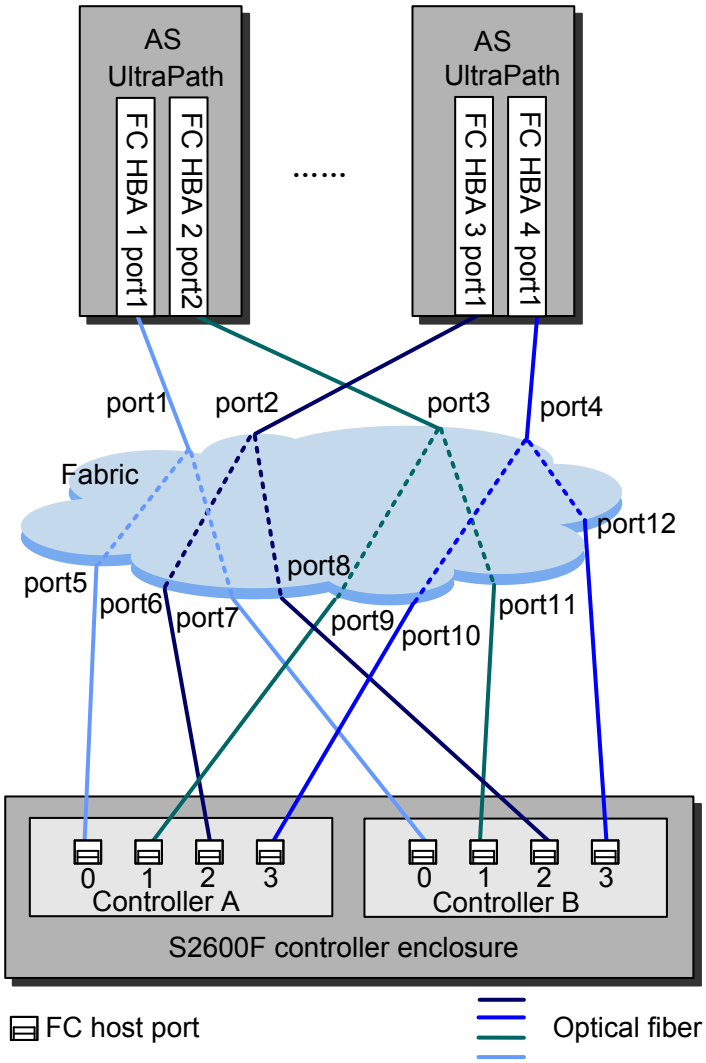
NOTE

The load balancing allows I/O flow to be borne on multiple paths to the same destination, thus implementing network traffic sharing or bandwidth extension. Failover means the automatic substitution of a functionally equivalent system component for a failed one. Failback means that the fault is rectified.

Dual-controller + One Fabric + ASs with Double FC HBAs

Figure 2-7 shows the networking of dual-controller + one Fabric + ASs with double FC HBAs.

Figure 2-7 Networking of dual-controller + one Fabric + ASs with double FC HBAs



CAUTION

In networking, one FC HBA interface of an AS can use only one path to reach a controller. According to this feature, you can allocate the zones. To be specific, port1 can connect to only port5 or port7 rather than port6 or port8.

In **Figure 2-7**, ports are allocated into zones as follows.

- zone1: port1 and port5
- zone2: port1 and port7
- zone3: port2 and port6
- zone4: port2 and port8

- zone5: port3 and port9
- zone6: port3 and port11
- zone7: port4 and port10
- zone8: port4 and port12

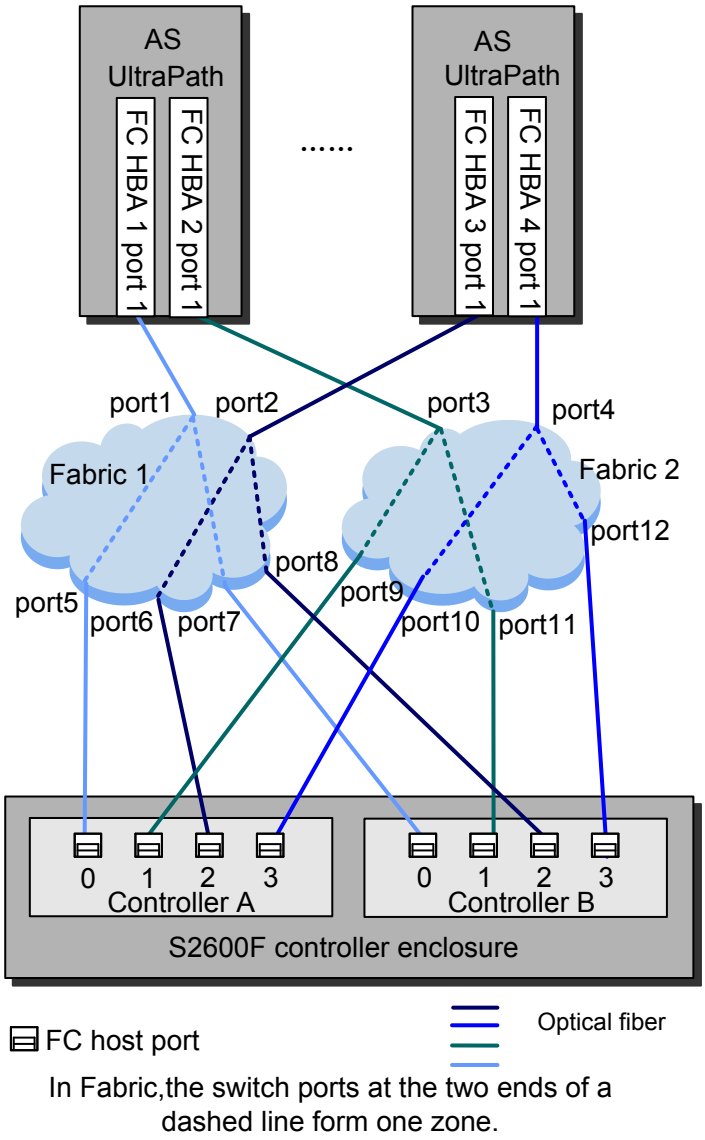
The networking mode avoids the single point failure of the FC HBA. Storage devices can connect to multiple ASs through the Fabric.

Dual-controller + Two Fabrics + ASs with Double FC HBAs

The network with two Fabrics is applicable to the networking environment that requires high service stability. Therefore, if multiple paths exist between the ASs and Fabrics as well as Fabrics and controllers, the service stability is guaranteed.

Figure 2-8 shows the networking of dual-controller + two Fabrics + ASs with double FC HBAs.

Figure 2-8 Networking of dual-controller + two Fabrics + ASs with double FC HBAs



In **Figure 2-8**, ports are allocated into zones as follows.

- zone1: port1 and port5
- zone2: port1 and port7
- zone3: port2 and port6
- zone4: port2 and port8
- zone5: port3 and port9
- zone6: port3 and port11
- zone7: port4 and port10
- zone8: port4 and port12

This networking avoids single point failures on FC HBAs, Fabric networks, and controllers.

2.2.3 Networking Modes of the S2600i

Introduction to the networking modes of the S2600i.

NOTE

- In this document, the service IP addresses on the storage device side of the iSCSI networking are configured in the format of 192.168.0.0/19.
- The four iSCSI host ports on each controller of the S2600i are independent of each other.
- The networking realizes the subnet model. An Ethernet switch can form one or more subnets.
- The performance of Ethernet switches can be improved if they are divided into virtual LANs (VLANs).

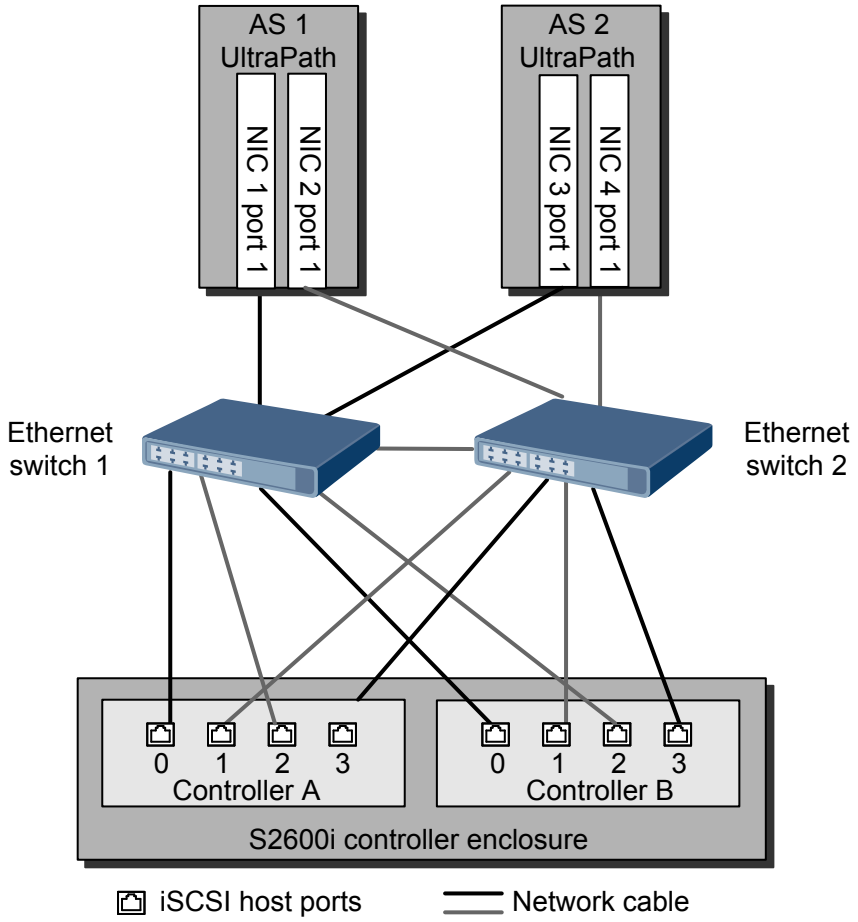
Dual-controller + ASs with Double NICs + Two Switches

Figure 2-9 shows the networking of dual-controller + AS with double NICs + two switches.

NOTE

In **Figure 2-9**, each switch is configured with two subnets.

Figure 2-9 Networking of dual-controller + ASs with double NICs + two switches



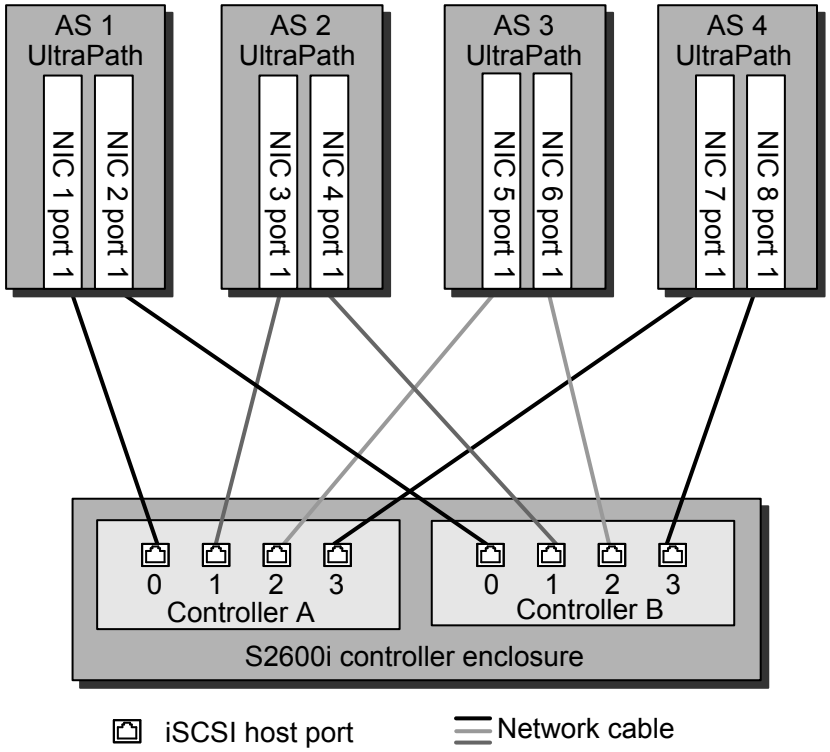
IP address of host port 0 on controller A: 192.168.11.100	Subnet mask: 255.255.255.0
IP address of host port 1 on controller A: 192.168.12.100	Subnet mask: 255.255.255.0
IP address of host port 2 on controller A: 192.168.13.100	Subnet mask: 255.255.255.0
IP address of host port 3 on controller A: 192.168.14.100	Subnet mask: 255.255.255.0
IP address of host port 0 on controller B: 192.168.11.101	Subnet mask: 255.255.255.0
IP address of host port 1 on controller B: 192.168.12.101	Subnet mask: 255.255.255.0
IP address of host port 2 on controller B: 192.168.13.101	Subnet mask: 255.255.255.0
IP address of host port 3 on controller B: 192.168.14.101	Subnet mask: 255.255.255.0
IP address of NIC 1: 192.168.11.150	Subnet mask: 255.255.255.0
IP address of NIC 2: 192.168.13.150	Subnet mask: 255.255.255.0
IP address of NIC 3: 192.168.12.150	Subnet mask: 255.255.255.0
IP address of NIC 4: 192.168.14.150	Subnet mask: 255.255.255.0

In **Figure 2-9**, one AS accesses the S2600i controller enclosure through two subnets. There are four available paths.

Dual-controller + ASs with Double NICs + Direct Topology

Figure 2-10 shows the networking of dual-controller + ASs with double NICs + direct topology.

Figure 2-10 Networking of dual-controller + ASs with double NICs + direct topology



IP address of host port 0 on controller A: 192.168.11.100	Subnet mask: 255.255.255.0
IP address of host port 1 on controller A: 192.168.12.100	Subnet mask: 255.255.255.0
IP address of host port 2 on controller A: 192.168.13.100	Subnet mask: 255.255.255.0
IP address of host port 3 on controller A: 192.168.14.100	Subnet mask: 255.255.255.0
IP address of host port 0 on controller B: 192.168.15.100	Subnet mask: 255.255.255.0
IP address of host port 1 on controller B: 192.168.16.100	Subnet mask: 255.255.255.0
IP address of host port 2 on controller B: 192.168.17.100	Subnet mask: 255.255.255.0
IP address of host port 3 on controller B: 192.168.18.100	Subnet mask: 255.255.255.0
IP address of NIC 1: 192.168.11.150	Subnet mask: 255.255.255.0
IP address of NIC 2: 192.168.15.150	Subnet mask: 255.255.255.0
IP address of NIC 3: 192.168.12.150	Subnet mask: 255.255.255.0
IP address of NIC 4: 192.168.16.150	Subnet mask: 255.255.255.0
IP address of NIC 5: 192.168.13.150	Subnet mask: 255.255.255.0
IP address of NIC 6: 192.168.17.150	Subnet mask: 255.255.255.0
IP address of NIC 7: 192.168.14.150	Subnet mask: 255.255.255.0
IP address of NIC 8: 192.168.18.150	Subnet mask: 255.255.255.0

In **Figure 2-10**:

- The IP addresses of the two NICs on the AS are configured on different subnets. Each AS can access the two controllers of the S2600i through two paths.
- The networking can be configured with a small number of ASs.

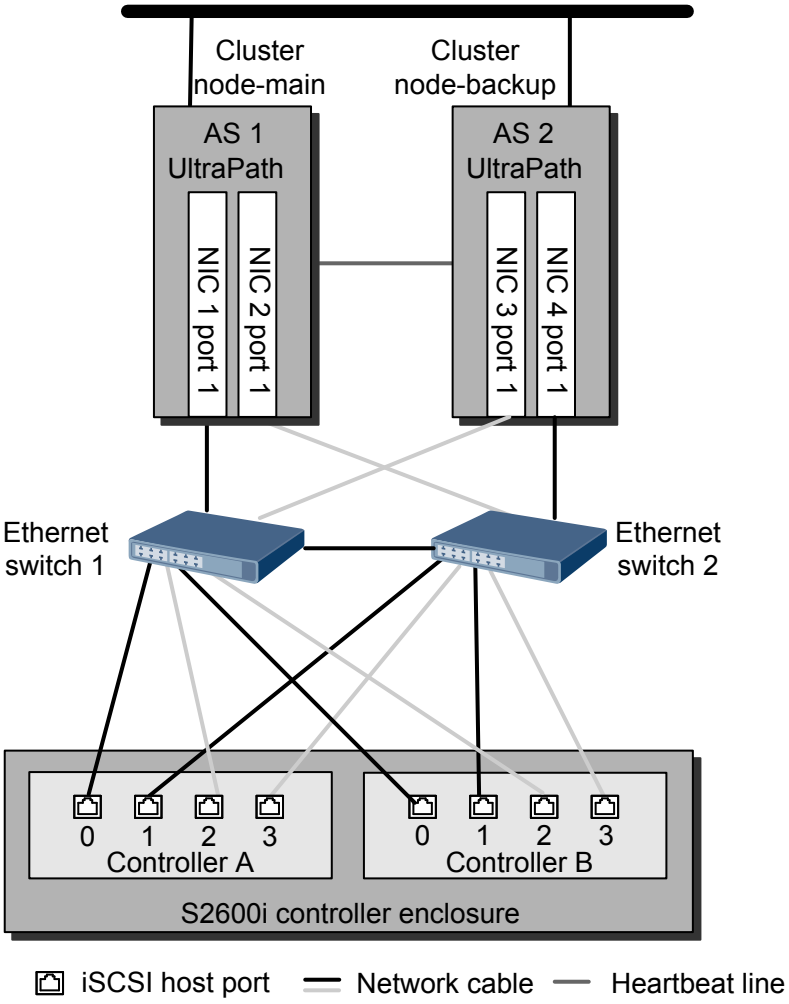
Cluster Networking with Dual-controller

Figure 2-11 shows the networking of dual-controller + ASs with double NICs and clustering + two switches.

NOTE

In **Figure 2-11**, each switch is set to two subnets.

Figure 2-11 Networking of dual-controller + ASs with double NICs and clustering + two switches



IP address of host port 0 on controller A: 192.168.11.100 Subnet mask: 255.255.255.0

IP address of host port 1 on controller A: 192.168.12.100 Subnet mask: 255.255.255.0

IP address of host port 2 on controller A: 192.168.13.100 Subnet mask: 255.255.255.0

IP address of host port 3 on controller A: 192.168.14.100	Subnet mask: 255.255.255.0
IP address of host port 0 on controller B: 192.168.11.101	Subnet mask: 255.255.255.0
IP address of host port 1 on controller B: 192.168.12.101	Subnet mask: 255.255.255.0
IP address of host port 2 on controller B: 192.168.13.101	Subnet mask: 255.255.255.0
IP address of host port 3 on controller B: 192.168.14.101	Subnet mask: 255.255.255.0
IP address of interface 1 on NIC 1: 192.168.11.150	Subnet mask: 255.255.255.0
IP address of interface 1 on NIC 2: 192.168.13.150	Subnet mask: 255.255.255.0
IP address of interface 1 on NIC 3: 192.168.12.150	Subnet mask: 255.255.255.0
IP address of interface 1 on NIC 4: 192.168.14.150	Subnet mask: 255.255.255.0

2.2.4 Networking Modes of the S2600C

Introduction to the networking modes of the S2600C.

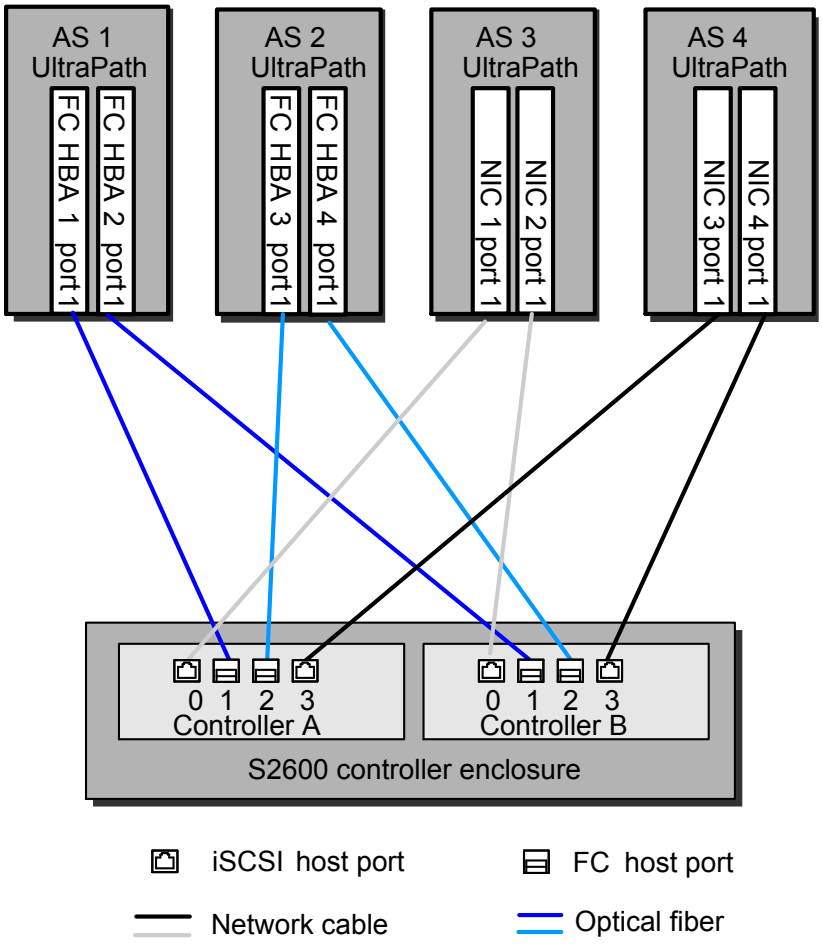
NOTE

- In this document, the IP addresses on the service network segment on the storage device side are configured to 192.168.0.0/19.
- The two iSCSI host ports on each controller of the S2600C are independent of each other.
- The networking realizes the one-subnet model. An Ethernet switch with other required devices can form one or more subnets.
- The performance of Ethernet switches can be improved if they are divided into virtual LANs (VLANs).

Dual-controller + ASs with Double FC HBAs and Double NICs + Direct Topology

Figure 2-12 shows the networking of dual-controller + ASs with double FC HBAs and double NICs + direct topology.

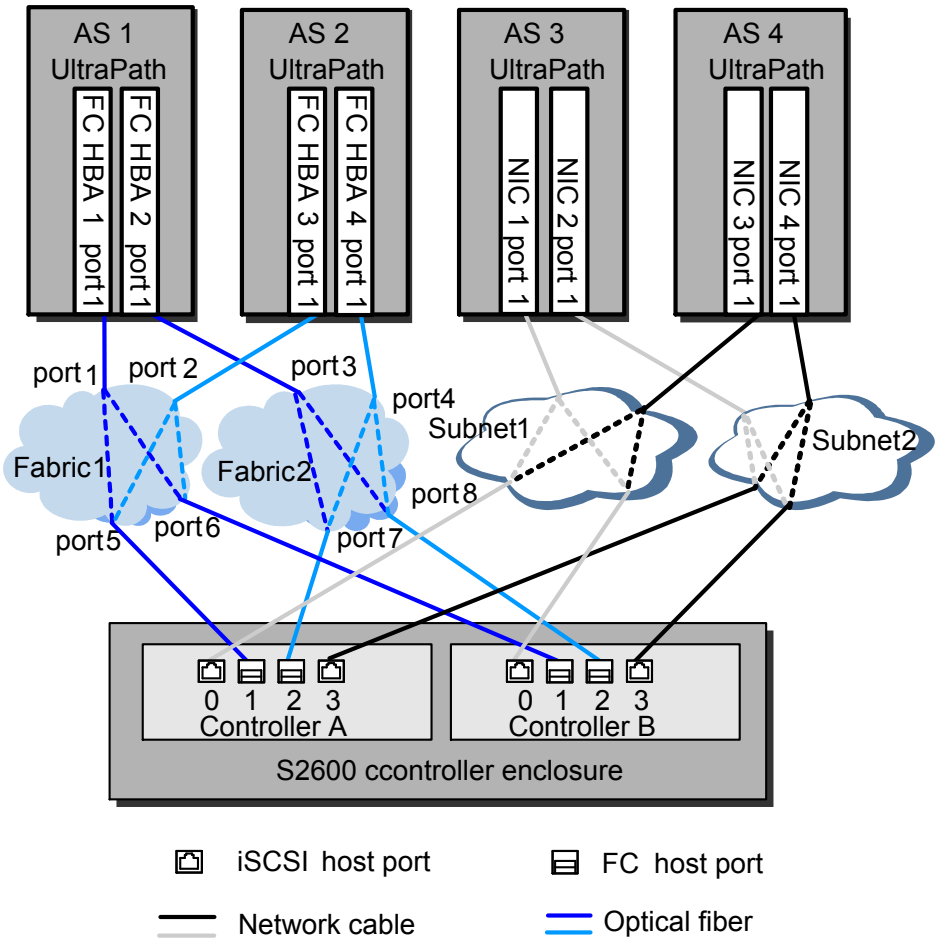
Figure 2-12 Networking of dual-controller + ASs with double FC HBAs and double NICs + direct topology



Dual-controller + ASs with Double FC HBAs and Double NICs + Two Fabrics and Two Subnets

When the S2600 is configured with FC + iSCSI host ports, the networking is dual-controller + ASs with double FC HBAs and double NICs + two Fabrics and two subnets. See **Figure 2-13**.

Figure 2-13 Networking of dual-controller + ASs with double FC HBAs and double NICs + two Fabrics and two subnets



In Fabric,the switch ports at the two ends of a dashed line form one zone.

IP address of host port 10 on controller A: 192.168.11.100	Subnet mask: 255.255.255.0
IP address of host port 11 on controller A: 192.168.12.100	Subnet mask: 255.255.255.0
IP address of host port 10 on controller B: 192.168.11.101	Subnet mask: 255.255.255.0
IP address of host port 11 on controller B: 192.168.12.101	Subnet mask: 255.255.255.0
IP address of interface 1 on NIC 1: 192.168.11.150	Subnet mask: 255.255.255.0
IP address of interface 1 on NIC 2: 192.168.12.150	Subnet mask: 255.255.255.0
IP address of interface 1 on NIC 3: 192.168.11.151	Subnet mask: 255.255.255.0
IP address of interface 1 on NIC 4: 192.168.12.151	Subnet mask: 255.255.255.0

In **Figure 2-13**

- Ports are allocated into zones as follows in FC networking.
  - zone1: port1 and port5
  - zone2: port1 and port6

- zone3: port2 and port5
- zone4: port2 and port6
- zone5: port3 and port7
- zone6: port3 and port8
- zone7: port4 and port7
- zone8: port4 and port8

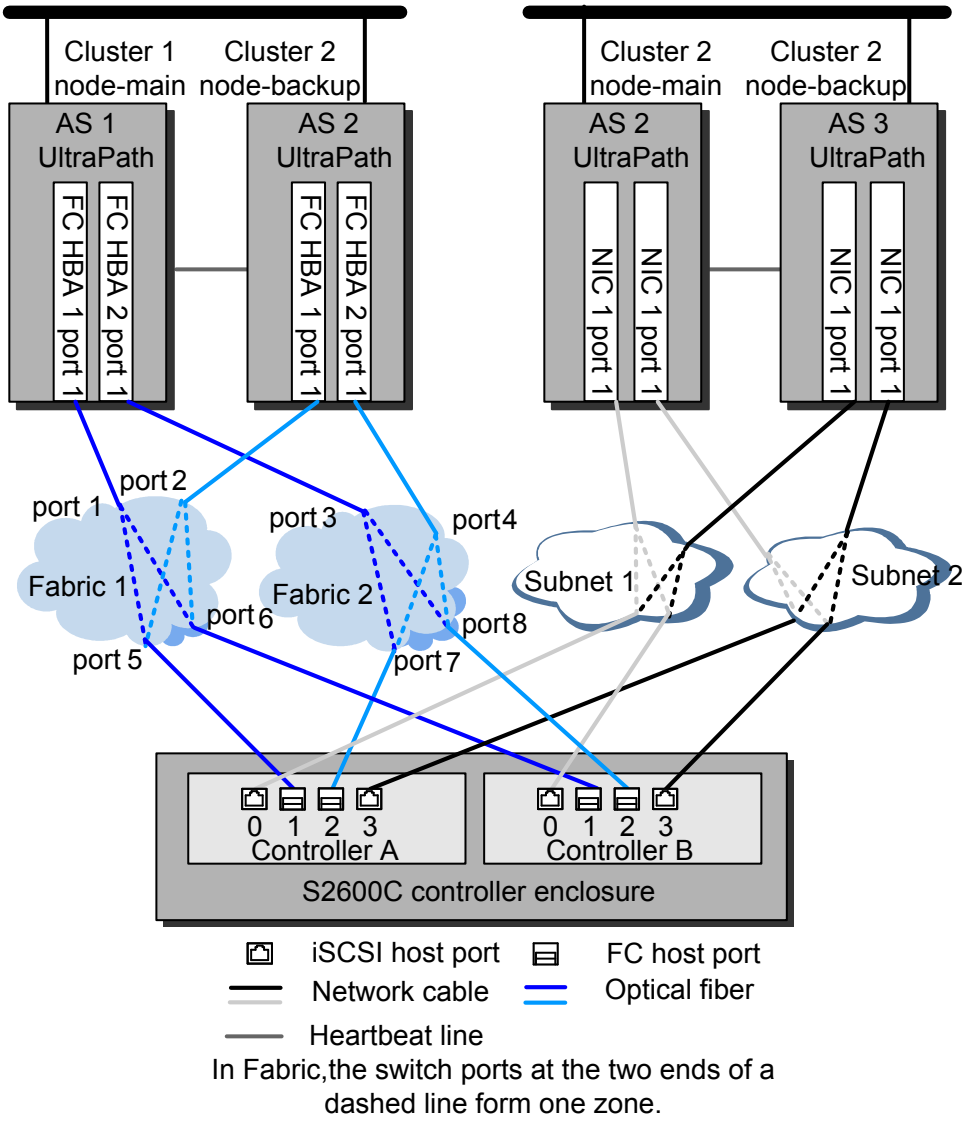
- For the iSCSI networking

  One AS accesses the S2600C controller enclosure through two subnets. There are four available paths.

Setting Up the Two-Node System Cluster Environment with Controllers

Figure 2-14 shows the networking of ASs with double FC HBAs + clusters + two Fabrics and two subnets.

Figure 2-14 Networking of ASs with double FC HBAs + clusters + two Fabrics and two subnets



IP address of host port 0 on controller A: 192.168.11.100	Subnet mask: 255.255.255.0
IP address of host port 3 on controller A: 192.168.12.100	Subnet mask: 255.255.255.0
IP address of host port 0 on controller B: 192.168.11.101	Subnet mask: 255.255.255.0
IP address of host port 3 on controller B: 192.168.12.101	Subnet mask: 255.255.255.0
IP address of interface 1 on NIC 1: 192.168.11.150	Subnet mask: 255.255.255.0
IP address of interface 1 on NIC 2: 192.168.12.150	Subnet mask: 255.255.255.0
IP address of interface 1 on NIC 3: 192.168.11.151	Subnet mask: 255.255.255.0
IP address of interface 1 on NIC 4: 192.168.12.151	Subnet mask: 255.255.255.0

In **Figure 2-14**, ports are allocated into zones as follows.

- zone1: port1 and port5

- zone2: port1 and port6
- zone3: port2 and port5
- zone4: port2 and port6
- zone5: port3 and port7
- zone6: port3 and port8
- zone7: port4 and port7
- zone8: port4 and port8

3 Installation Configuration

About This Chapter

This section describes how to install the JRE and the OceanStor ISM.

3.1 Installing the JRE

This section describes the procedure for installing the JRE.

3.1.1 Windows

This section describes the procedure for installing the JRE in Windows.

Prerequisite

When you log in to the OceanStor ISM for the first time, if the JRE is not installed on the maintenance terminal, install the JRE before installing the OceanStor ISM.

Context

This chapter takes installing **jre-1_5_0_14-windows-i586-p.exe** as an example.

Procedure

Step 1 Run the Internet Explorer (IE), for example, taking IE 6.0 as an example, on the maintenance terminal.

Step 2 Enter **http://XXX.XXX.XXX.XXX** in the address bar of the IE.

XXX.XXX.XXX.XXX indicates the IP address of the controller of the storage device that downloads the ISM.

Step 3 Click **Go** or press **Enter**. The system goes to the interface, as shown in **Figure 3-1**.

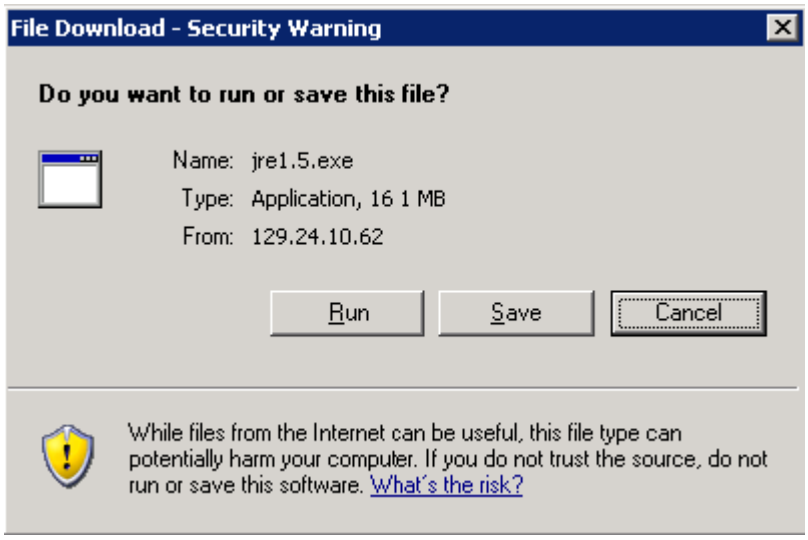
Figure 3-1 JRE download interface

Step 4 Click **Please Setup JRE1.5_0_14 for windows**. The system displays the **File Download - Security Warning** dialog box, as shown in **Figure 3-2**.

NOTE

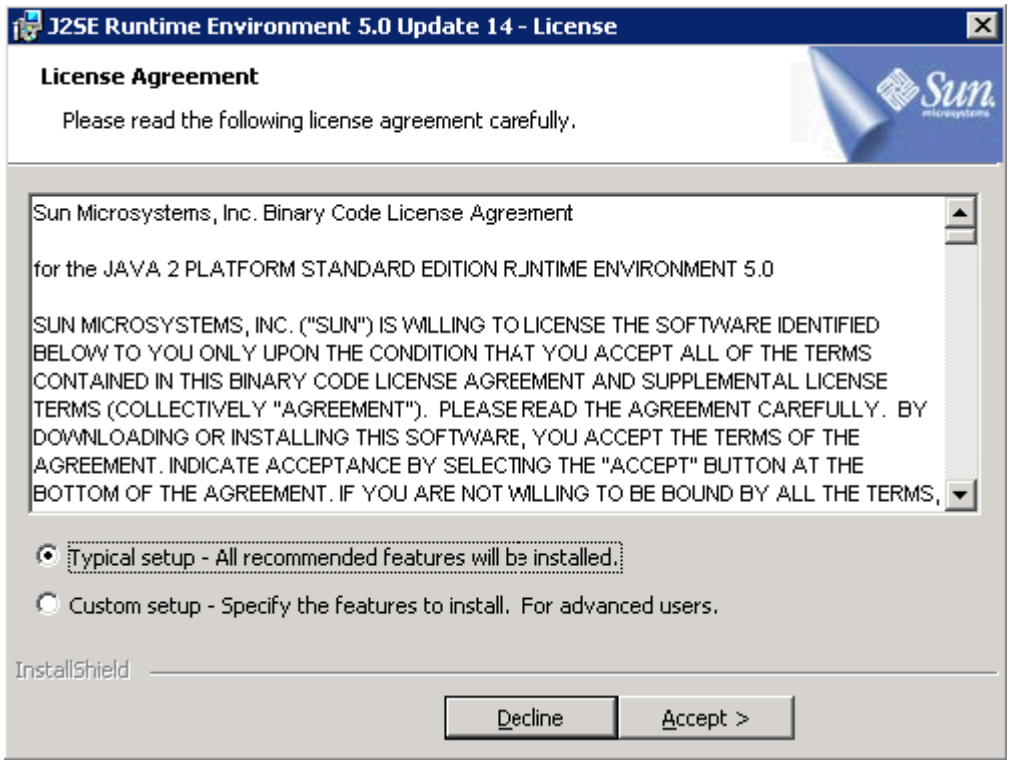
Click **Please Download Other JRE**. The system connects to the sun website. Executes the download and setup according to the guide of the website.

Figure 3-2 File Download - Security Warning dialog box



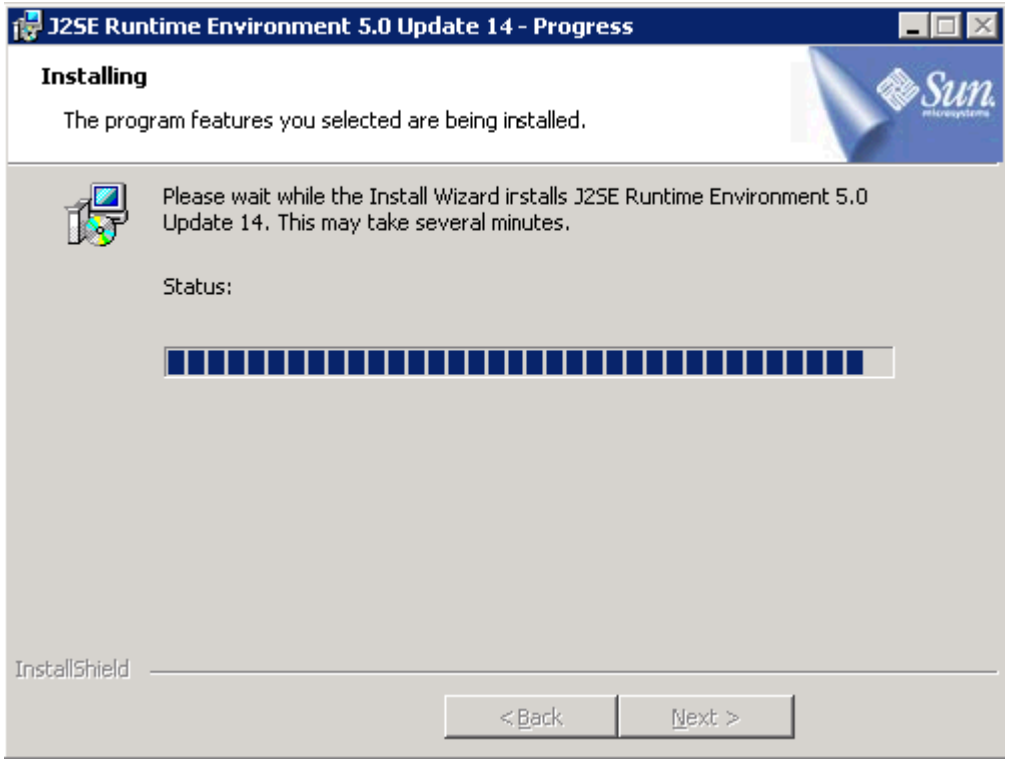
Step 5 Click **Run**. After the system unzips the installation file, the system displays the **J2SE Runtime Enviroment 5.0 Update 14-License** dialog box, as shown in **Figure 3-3**.

Figure 3-3 J2SE Runtime Enviroment 5.0 Update 14-License dialog box



Step 6 Click **Accept**. The system begins to install the JRE. **Figure 3-4** shows the installation progress.

Figure 3-4 Installing interface



Step 7 After the installation, the system goes to the **Complete** interface, as shown in **Figure 3-5**.

Figure 3-5 Complete interface

Step 8 Click **Finish**.

----End

3.1.2 Linux

This section describes the procedure for installing the JRE in Linux.

Context

This chapter takes **jre-1_5_0_14-linux-i586.bin** in Linux as an example.

Procedure

Step 1 Log in to the AS.

NOTE

If the JRE is installed in the system directory, such as **/usr/local**, you can only log in as the **Super Admin** user. If you have no rights of a super user, install the JRE in the main directory or a subdirectory where you have write rights.

Step 2 Go to the directory where the JRE installation packet is located.

To install the JRE in the directory **/jre_test** , enter **cd /jre_test**.

Step 3 Run the command **chmod a+x** *jre-1_5_0_14-linux-i586.bin* to enable the right of the installation package.

Run the command **ls -l** to check whether you have the right to execute the file.

Step 4 Run the command **./jre-1_5_0_14-linux-i586.bin** to start installation. The interface displays the binary installation permission protocol.

Step 5 After reading the protocol, enter **yes**.

NOTE

Taking installing **jre-1_5_0_14-linux-i586.rpm** as an example run the **rpm** *-iv jre-1_5_0_14-linux-i586.rpm* command to install the software package.

Step 6 After the installation, the interface displays `Done.`. The JRE is installed in the directory **/jre_test/jre-1_5_0_14**.

NOTE

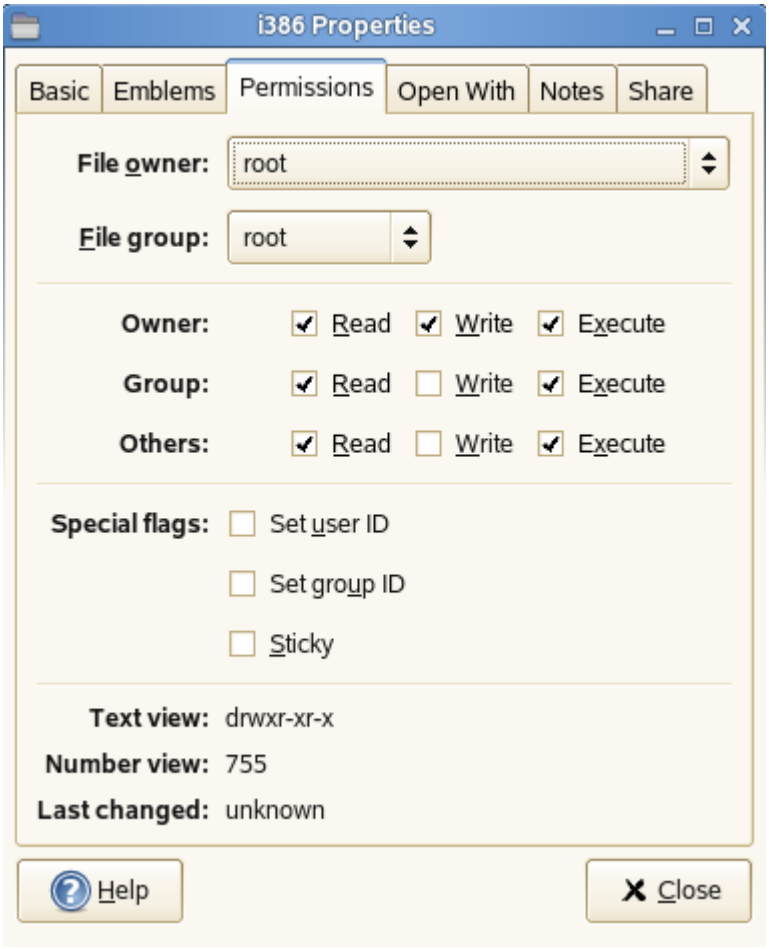
After installing the RPM, the system displays `package jre-1.5.0_14-fcs is already installed`.

----End

Postrequisite

When downloading the OceanStor ISM, set the right of the installation folder of the JRE according to the actual needs. Taking SUSE Linux Enterprise Server 10 as an example, **Figure 3-6** shows the setting interface.

Figure 3-6 i386 Properties interface



3.1.3 Solaris

This section describes the procedure for installing the JRE in Solaris.

Prerequisite

Context

This chapter takes the file **jre-1_5_0_14-solaris-i586.sh** as an example.

Procedure

Step 1 Log in to the AS.

Step 2 Go to the directory where the JRE installation packet is located.

To install the JRE in the directory **/jre_test**, enter the command **cd /jre_test**.

Step 3 Run the command **chmod a+x** *jre-1_5_0_14-solaris-i586.sh* to enable the right of the installation package.

Run the command to **ls -l** to check whether you have the right to execute the file.

Step 4 Go to the installation directory **/jre_test**. Run the command **./jre-1_5_0_14-solaris-i586.sh** to start installation. The interface displays the binary installation permission protocol.

Step 5 After reading the protocol, enter **yes**.

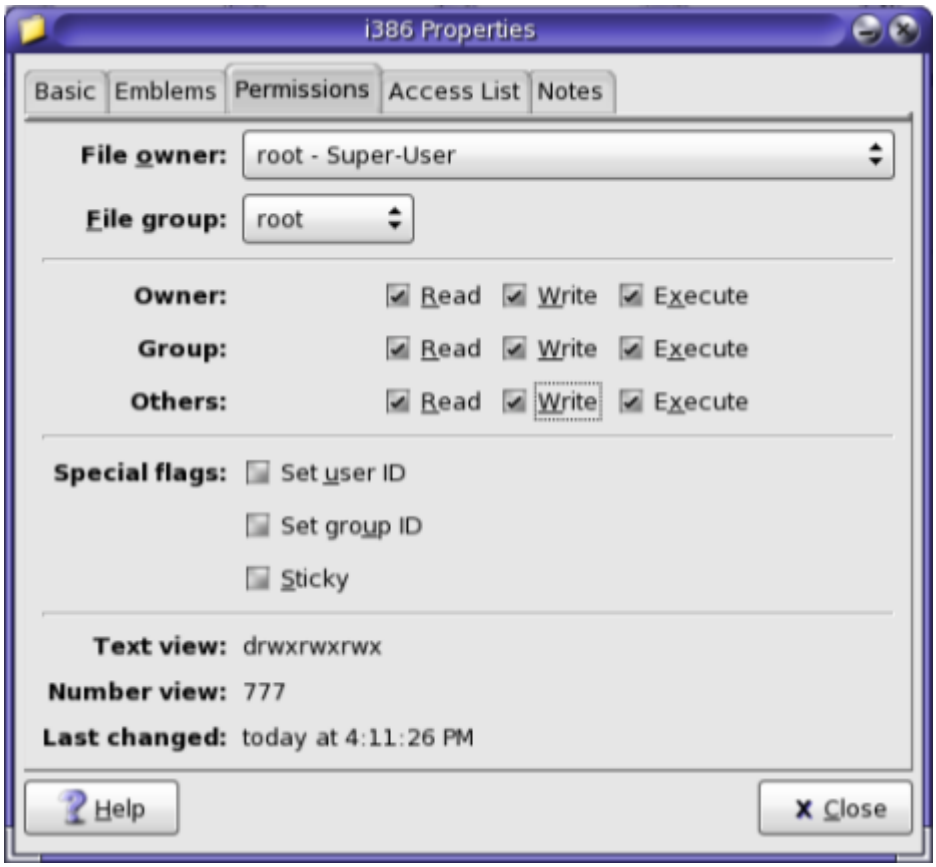
Step 6 After the installation, the interface displays `Done.`. The JRE is installed in the directory **/jre_test / jre1.5.0_14**.

----End

Postrequisite

When downloading the OceanStor ISM, set the right of the installation folder of the JRE according to the actual needs. **Figure 3-7** shows the setting interface.

Figure 3-7 i386 Properties interface



3.2 Installing the OceanStor ISM

This section describes how to configure the OceanStor ISM and operate the OceanStor ISM.

3.2.1 Windows

This section describes how to configure the OceanStor ISM and operate the OceanStor ISM in Windows.

3.2.2 Linux/Solaris
This section describes how to configure the OceanStor ISM and operate the OceanStor ISM in Linux/Solaris.

3.2.1 Windows

This section describes how to configure the OceanStor ISM and operate the OceanStor ISM in Windows.

Prerequisite

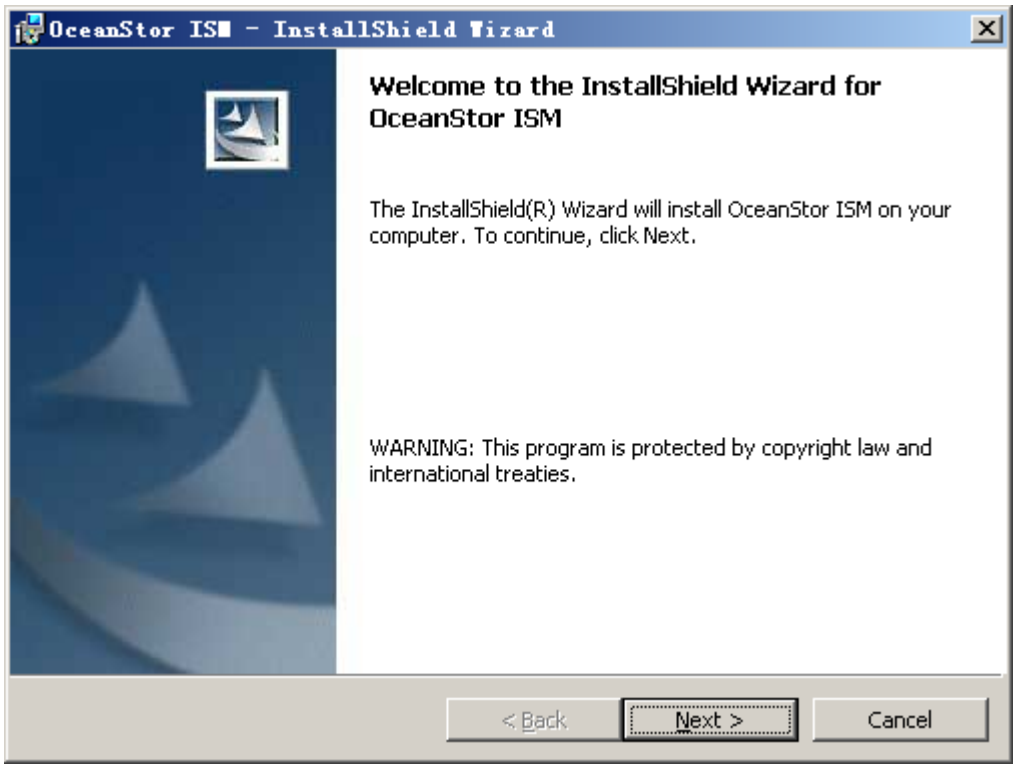
The JRE is properly installed in the system.

Procedure

Step 1 The CD delivered with products contains the OceanStor ISM setup.

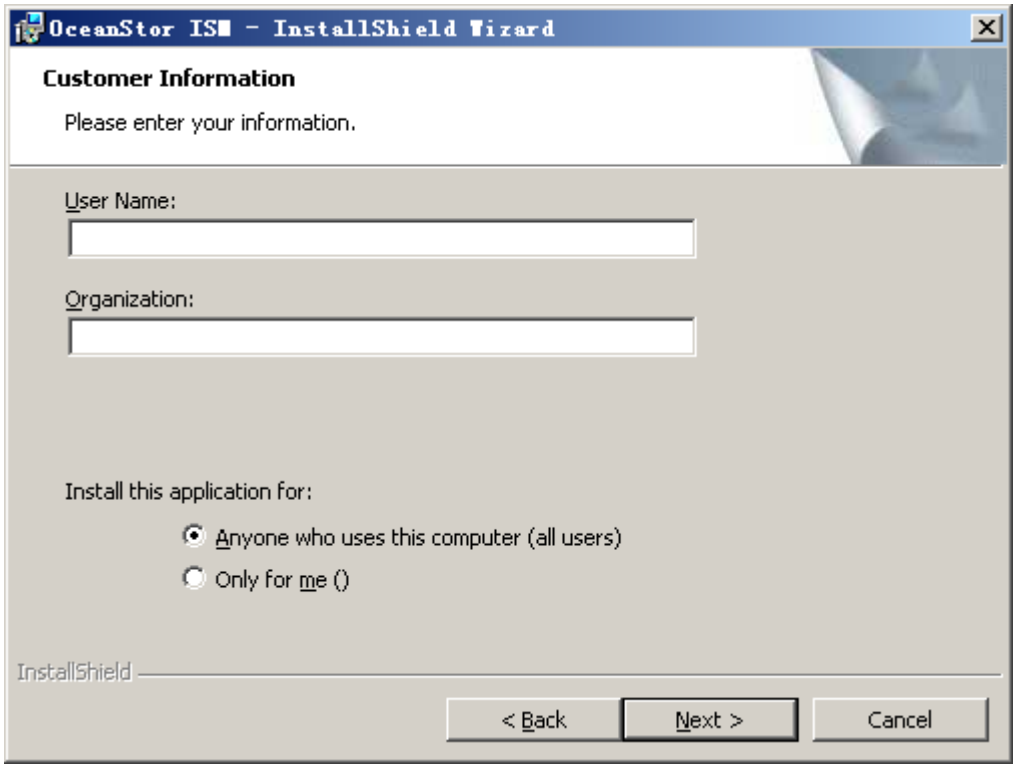
Step 2 When you run the ***.exe** setup, the system displays the **OceanStor ISM - InstallShield Wizard** interface, as shown in **Figure 3-8**.

Figure 3-8 OceanStor ISM - InstallShield Wizard interface



Step 3 Click **Next**. The system displays the **Customer Information** interface, as shown in **Figure 3-9**.

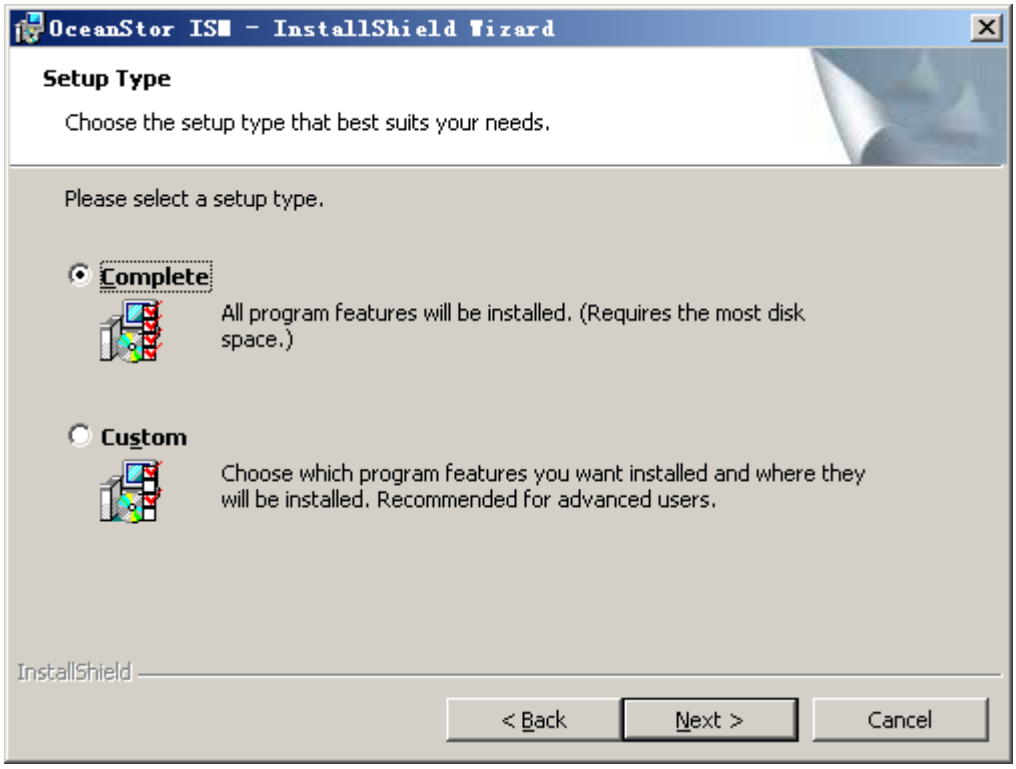
Figure 3-9 Customer Information interface



Step 4 Enter the user name in **User Name:** and the organization name in **Organization**.

Step 5 Click **Next**. The system goes to the **Setup Type** interface, as shown in **Figure 3-10**.

Figure 3-10 Setup Type interface

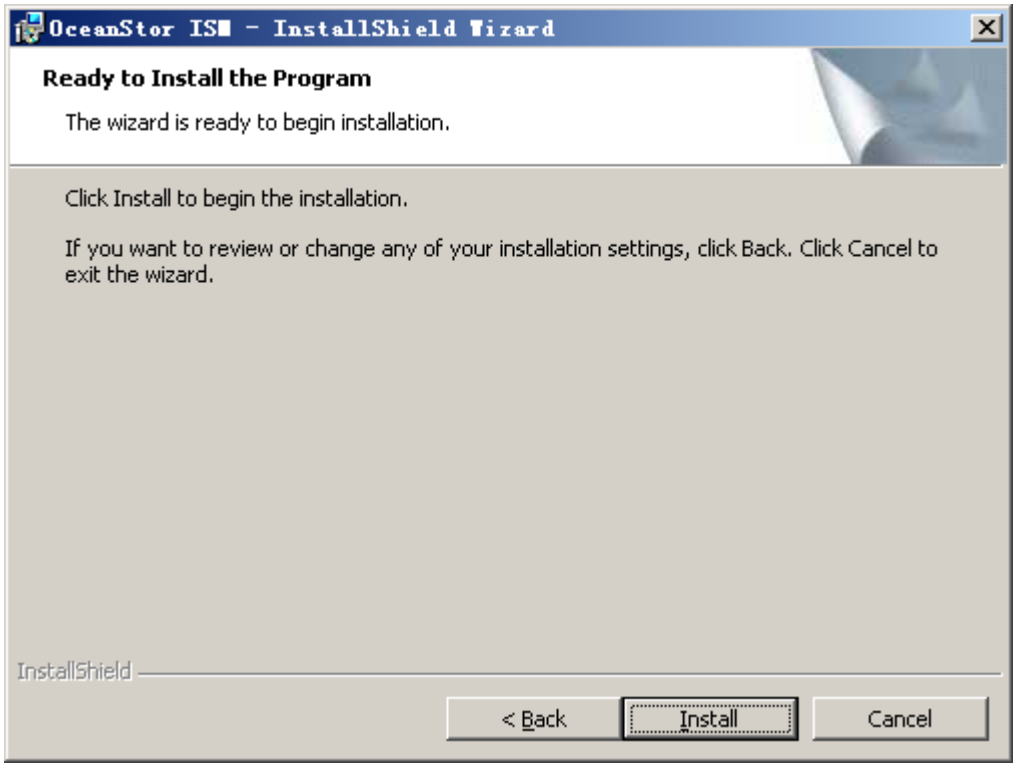


Step 6 Choose **Complete** or **Custom** according to the actual needs.

When you choose **Custom**, click **Next**. Then yo can choose the installation path on the **Custom Setup** interface.

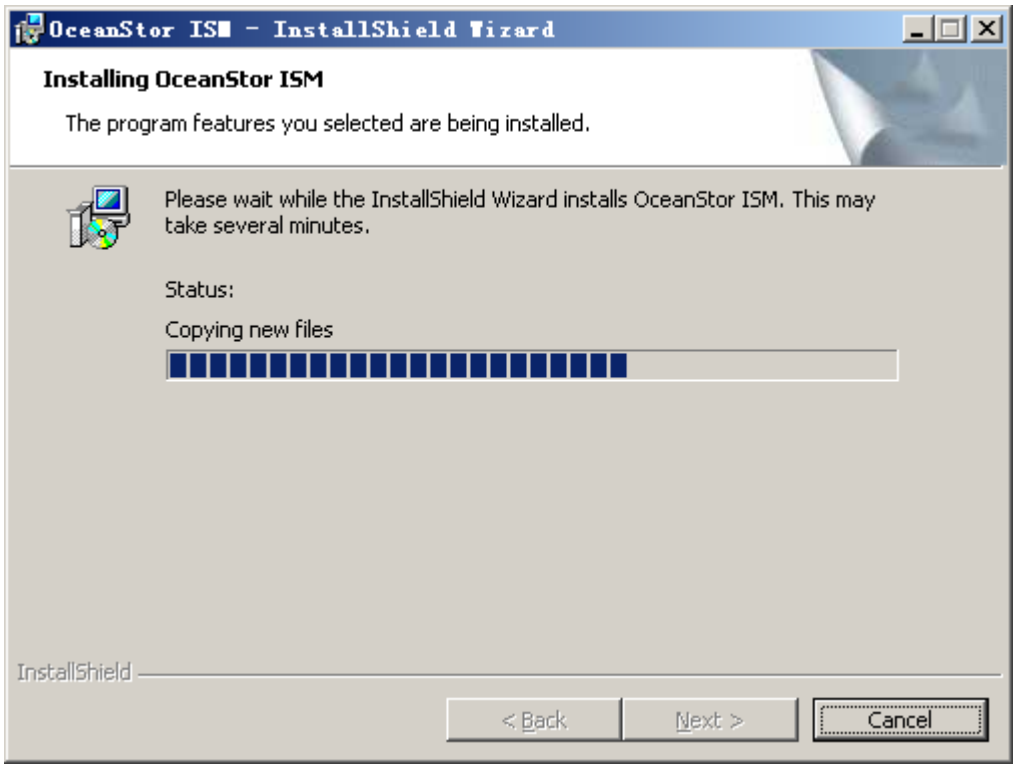
Step 7 Click **Next**. The system displays the **Ready to Install the Program** interface, as shown in **Figure 3-11**.

Figure 3-11 Ready to Install the Program interface



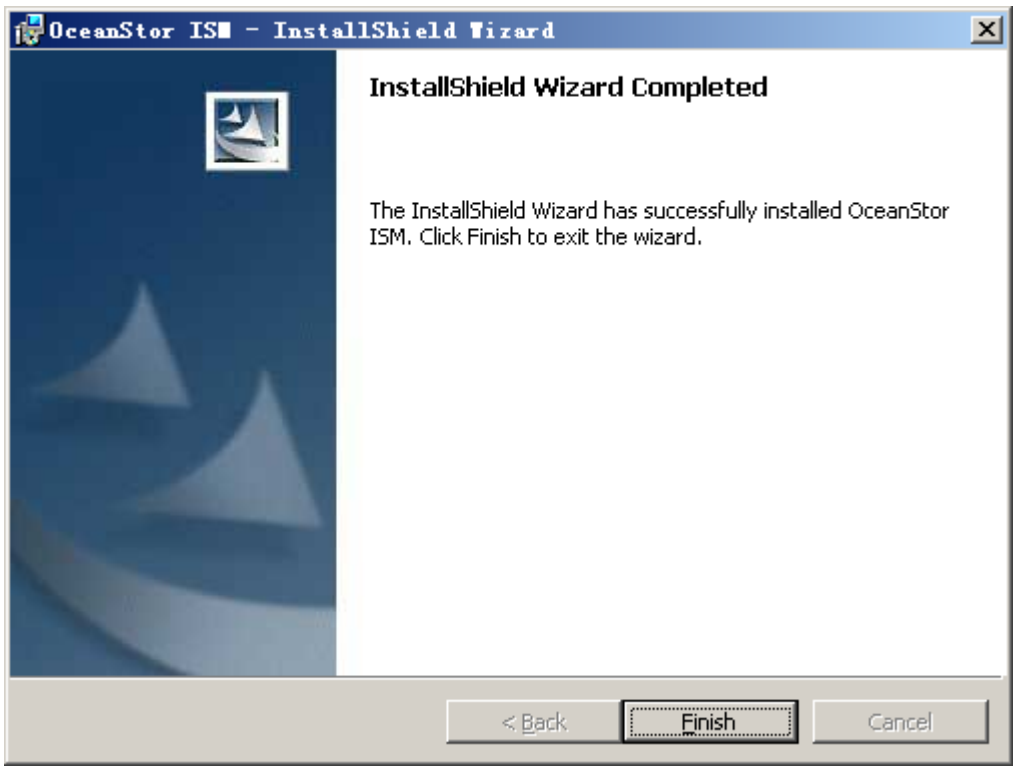
Step 8 Click **Install**. The system displays the installation progress, as shown in **Figure 3-12**.

Figure 3-12 Installing OceanStor ISM interface



Step 9 After the installation, the system displays the **InstallShield Wizard Completed** interface, as shown in **Figure 3-13**.

Figure 3-13 InstallShield Wizard Completed interface



Step 10 Click **Finish**, The OceanStor ISM is installed.

----End

Result

After the installation , a desktop shortcut for the OceanStor ISM is created.

3.2.2 Linux/Solaris

This section describes how to configure the OceanStor ISM and operate the OceanStor ISM in Linux/Solaris.

Prerequisite

The JRE is properly installed in the system.

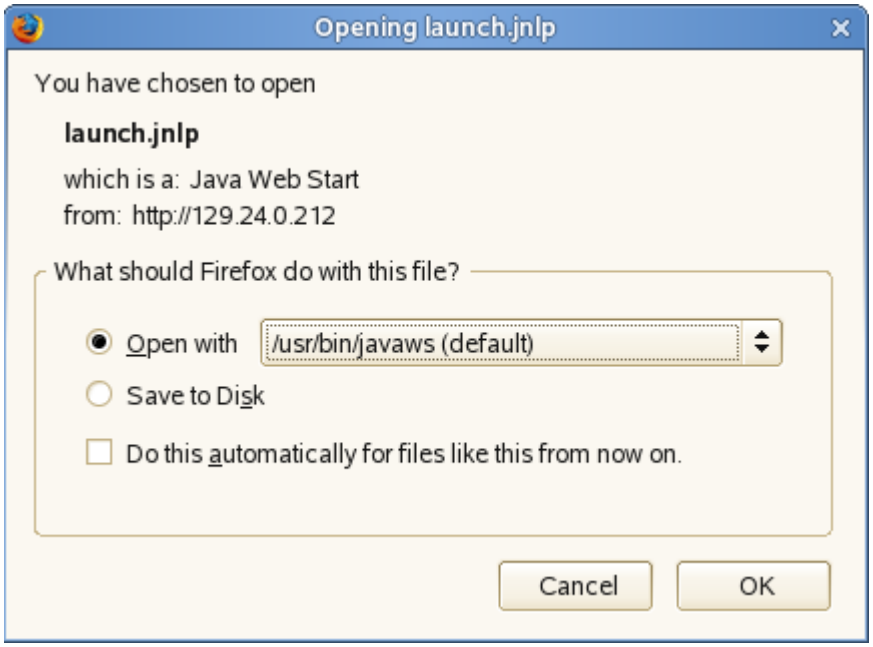
Context

This chapter takes the OS configured with Firefox/2.0.0.2 or Firefox/2.0.0.11 browser as an example to describe the procedure for configuring the OceanStor ISM.

Procedure

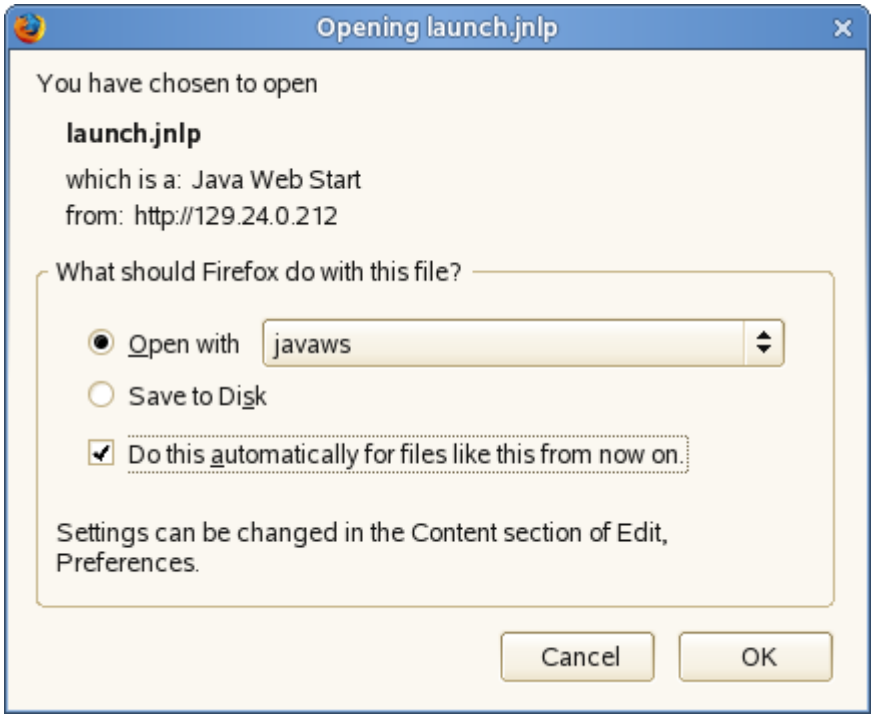
Step 1 On the maintenance terminal, open the login interface through the Firefox browser. When clicking the interface to download the ISM, if the JRE is not associated with the **jnlp** file, taking SUSE Linux Enterprise Server 10 as an example, the system displays the dialog box, as shown in **Figure 3-14**.

Figure 3-14 Openging launch.jnlp dialog box



Step 2 Choose **Open with**. In the drop-down list box, choose **Other...** and select **Do this automatically for files like this from now on**, as shown in **Figure 3-15**.

Figure 3-15 Select the related program



Step 3 Click **OK**.

Step 4 Go to the directory where the OceanStor ISM installation package is located. Run the command **tar zxvf** *OceanStor_ISM.tgz* to unzip the installation package.

After the unzipping, a directory named **OceanStor_ISM** is added.

Step 5 Go to the directory **OceanStor_ISM**. Run the command **sh** *OceanStor_ISM.sh* to start the application to run the OceanStor ISM.

----End

4 Configuring the Storage System

About This Chapter

This chapter describes the wizard, flow chart, and procedure for configuring the storage system.

4.11 Adding an Initiator

An initiator is added to manage iSCSI host port. After the initiator is added, the AS can connect to the storage array through the iSCSI host port for data access.

4.12 Adding a Mapping

Introduction to adding a mapping.

4.13 Adding an Interface

Introduction to adding a interface.

4.14 Using a LUN on an AS

After mapping a device LUN to an AS, you must configure the LUN on the AS.

4.1 Configuration Wizard

The initial configuration wizard and typical application configuration.

4.1.1 Initial Configuration Wizard

Introduction to the initial configuration wizard.

Context

The S2600 provides the initial configuration wizard, which helps users to complete the initial configuration of arrays conveniently and quickly.

Through the initial configuration wizard, you can complete the following operations:

- Changing the name of an array and its location
- Setting an array clock
- Changing a user password
- Setting the information about an interface

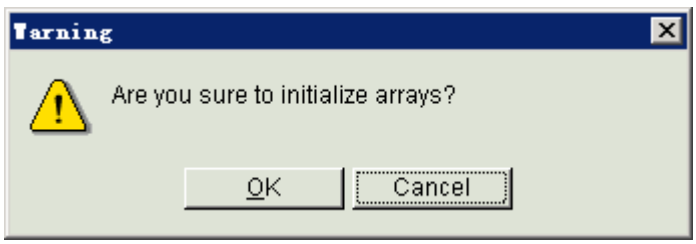
CAUTION

- This section takes the S2600i as an example to describe the initial configuration wizard.
- When the storage array is the S2600S, the initial configuration wizard does not contain the procedure for setting interfaces.
- When the storage array is S2600F or S2600C, for details on how to change the rate, see "**4.7 Setting the FC Host Port on the Controller**".

Procedure

Step 1 Log in to the OceanStor ISM and discover an array successfully, the **Warning** dialog box is displayed, prompting you whether to perform the initial configuration operation. See **Figure 4-1**.

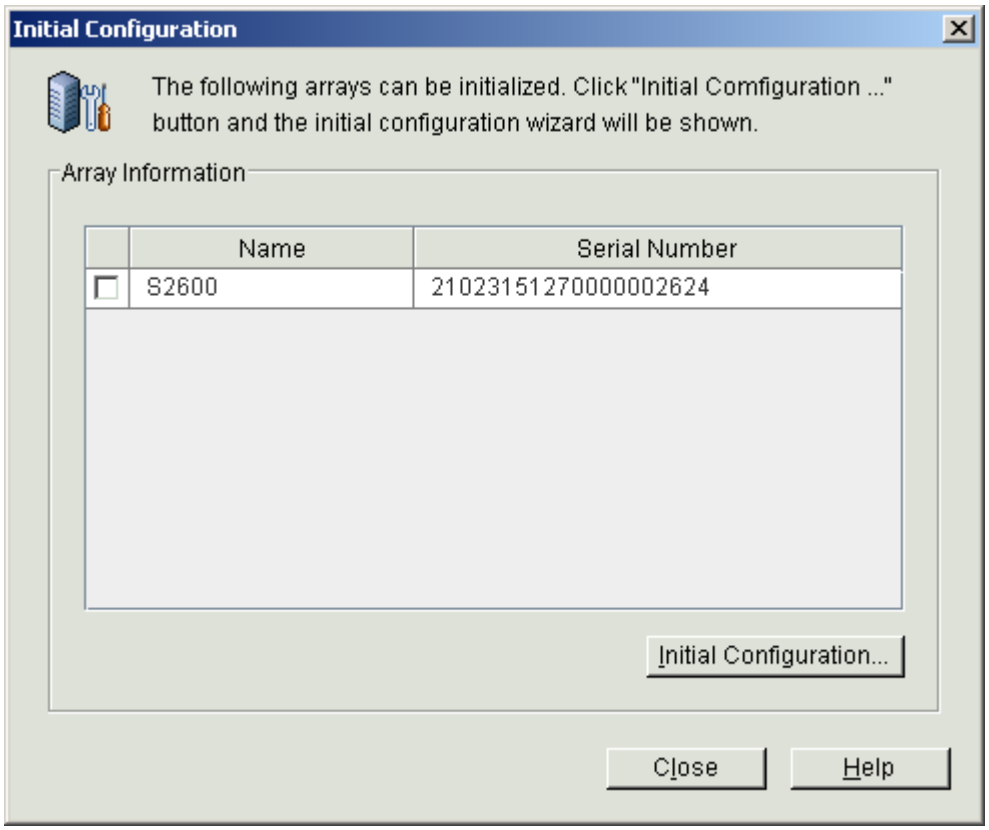
Figure 4-1 Warning dialog box



Step 2 Click **OK**.

The **Initial Configuration** interface is displayed, as shown in **Figure 4-2**.

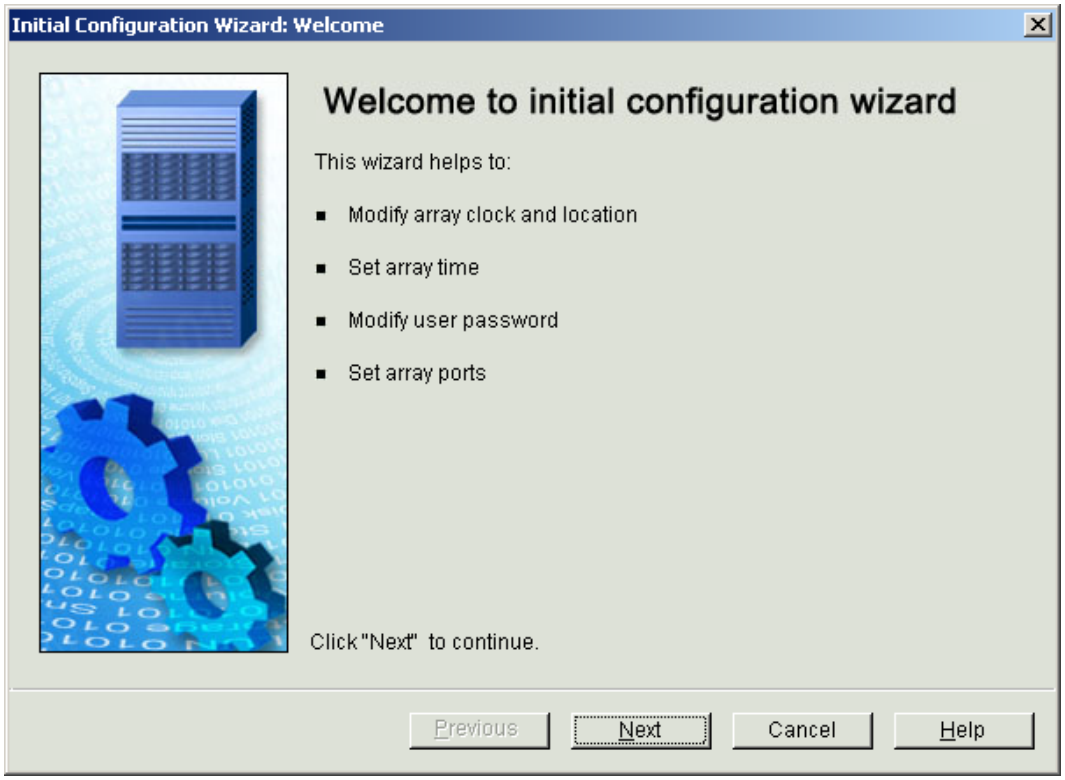
Figure 4-2 Initial Configuration interface



Step 3 Select the required array and click **Initial Configuration...**.

The **Initial Configuration Wizard: Welcome** interface is displayed. See **Figure 4-3**.

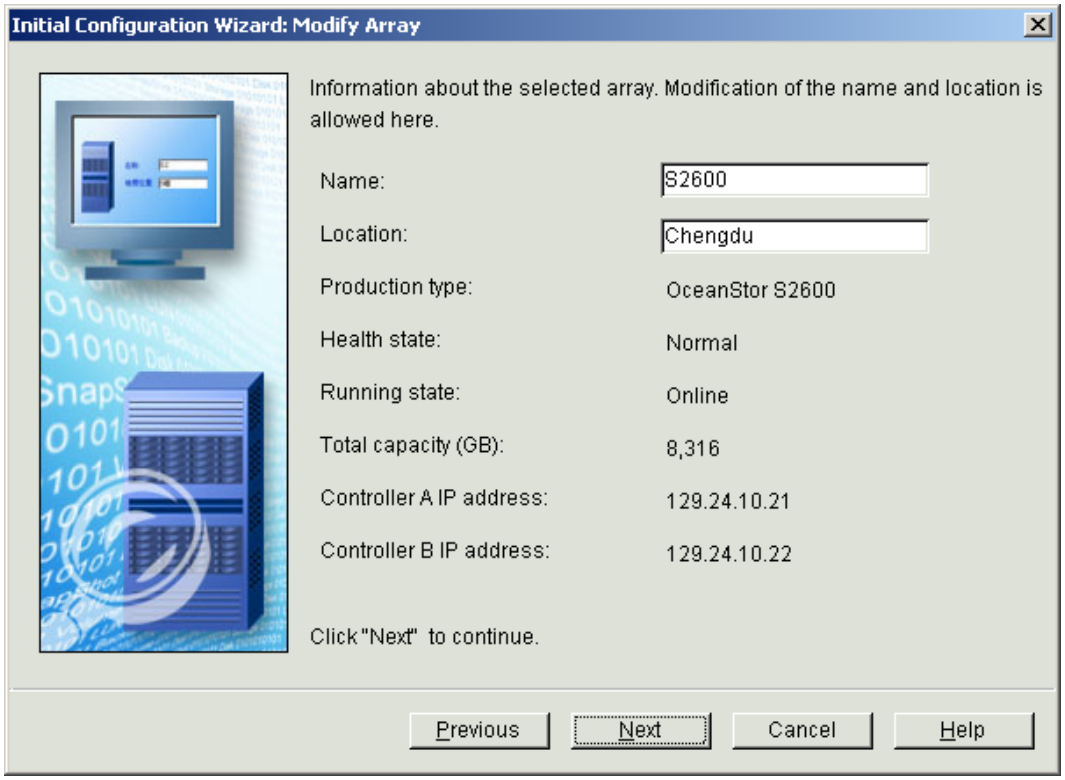
Figure 4-3 Initial Configuration Wizard: Welcome interface



Step 4 Click **Next**.

The **Initial Configuration Wizard: Modify Array** interface is displayed. See **Figure 4-4**.

Figure 4-4 Initial Configuration Wizard: Modify Array interface



Step 5 Enter the array name and the location.

Table 4-1 lists the parameter description.

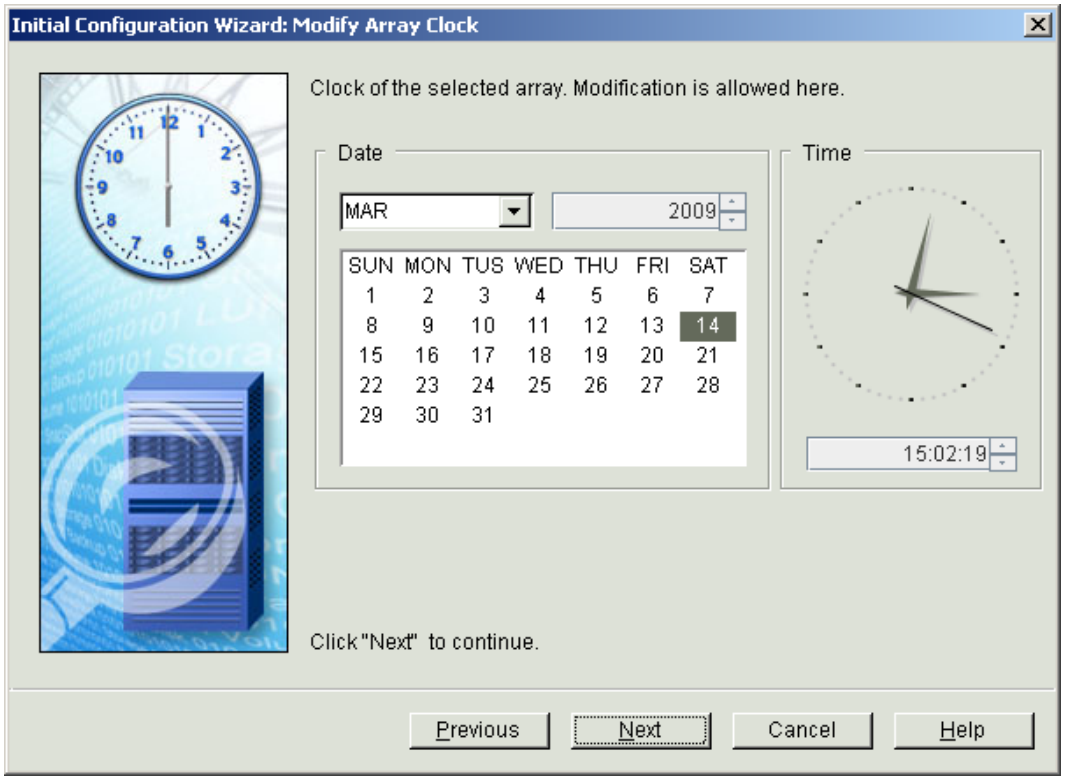
Table 4-1 Parameters for changing the information about an array

Parameter	Description
Name	The parameter indicates the name of the S2600 to be set. Note that: ● The value contains letters, digits, underscores, or hyphens only. ● The value contains a maximum of 32 characters.
Location	The parameter indicates the location of the S2600. Note that: ● The value contains letters, digits, underscores, or hyphens only. ● The value contains a maximum of 32 characters.

Step 6 Click **Next**.

The **Initial Configuration Wizard: Modify Array Clock** interface is displayed. See **Figure 4-5**.

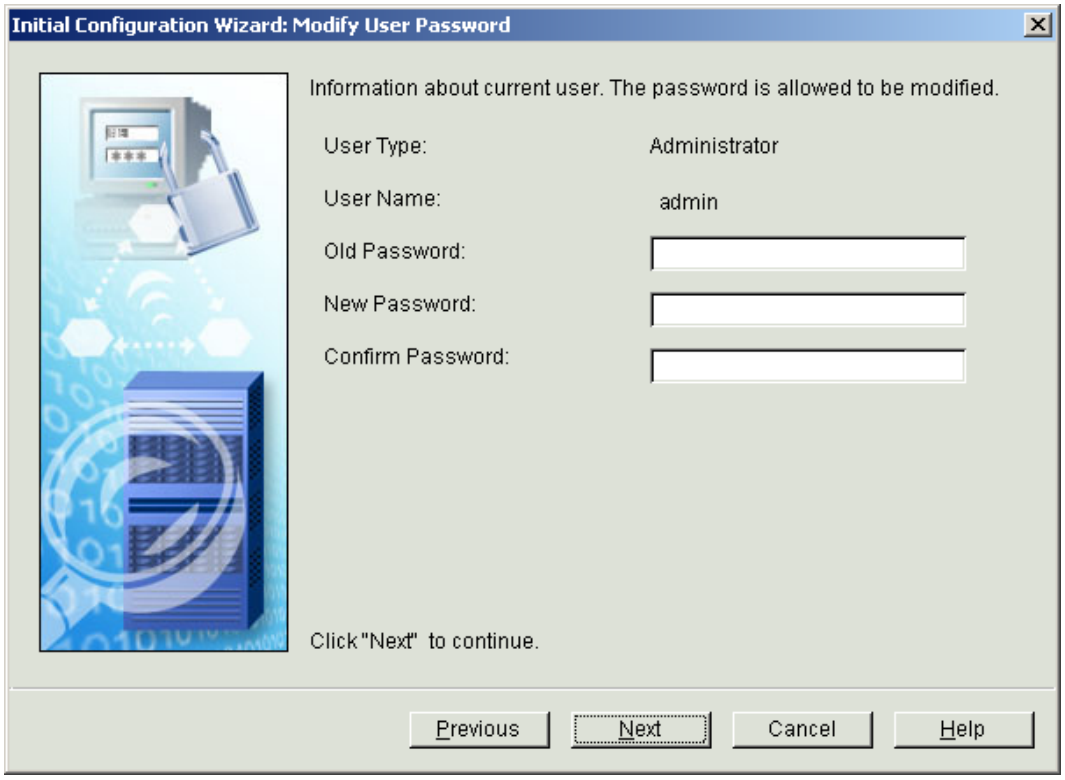
Figure 4-5 Initial Configuration Wizard: Modify Array Clock interface



Step 7 Set the date and time, and click **Next**.

The **Initial Configuration Wizard: Modify User Password** interface is displayed. See **Figure 4-6**

Figure 4-6 Initial Configuration Wizard: Modify User Password interface



Step 8 Change the password of a login user.

For parameter description, see **Table 4-2**.

Table 4-2 Parameters for changing a password

Parameter	Description
Old Password	The parameter indicates the old password of the user.
New Password	The parameter indicates the new password of the user. [Value range] The length of the password ranges from 6 to 16 characters.
Confirm Password	The parameter indicates the confirm password. The value must be the same as that of **New Password**.

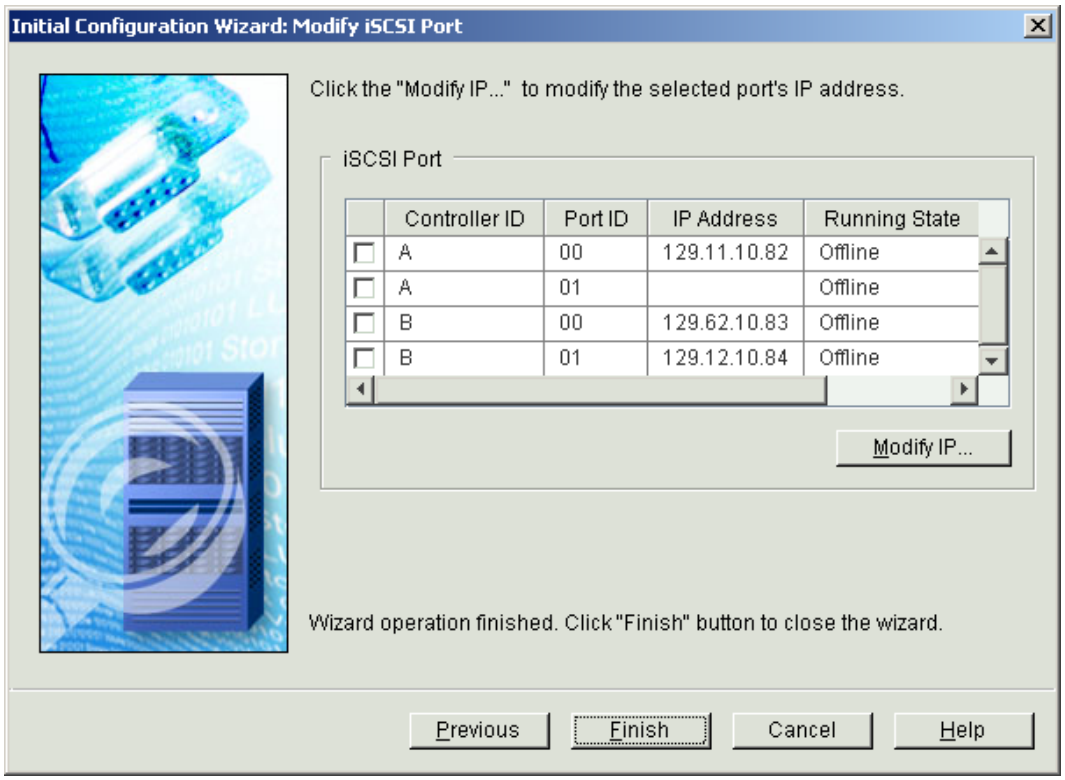
NOTE

If the S2600S is discovered, the initial configuration is complete. On the displayed **Initial Configuration Wizard: Modify user password** interface, click **Finish**.

Step 9 Click **Next**.

The **Initial Configuration Wizard: Modify iSCSI Port** interface is displayed, as shown in **Figure 4-7**

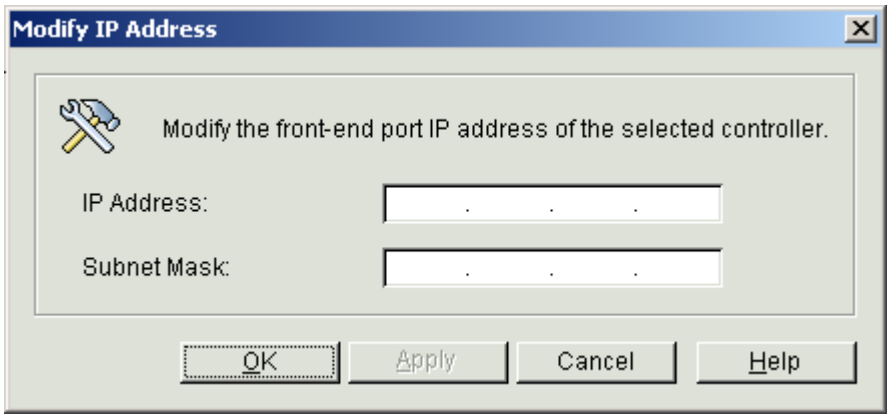
Figure 4-7 Initial Configuration Wizard: Modify iSCSI Port interface



Step 10 If you want to change the IP address of an interface, select the required interface and click **Modify IP...**. The **Modify IP Address** interface is displayed, as shown in **Figure 4-8**.

If you want to complete the operation, click **Finish**.

Figure 4-8 Modify IP Address interface



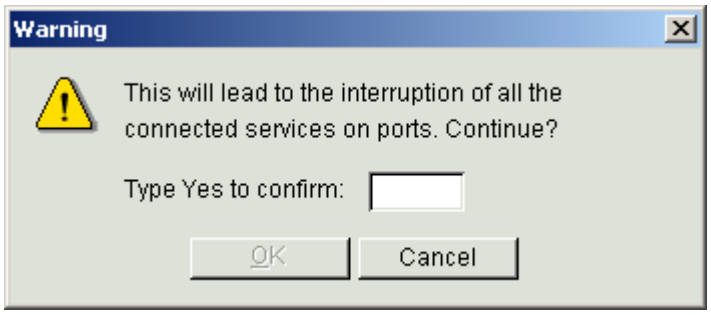
Step 11 Enter the required IP address and its subnet mask.

For the details on how to set an IP address, see **Table 4-3**.

Step 12 Click **OK**.

The **Warning** dialog box is displayed, as shown in **Figure 4-9**.

Figure 4-9 Warning dialog box



Step 13 In the text box, enter **Yes**, and then click **OK**.

The **Info** dialog box is displayed, stating "**Operation succeeded.**".

Step 14 Click **OK**.

----End

4.1.2 Typical Application Configuration

Typical application configuration provides the capacity allocation function. According to different application requirements, you can allocate capacity to a host group or a host to meet the requirements of different storage applications.

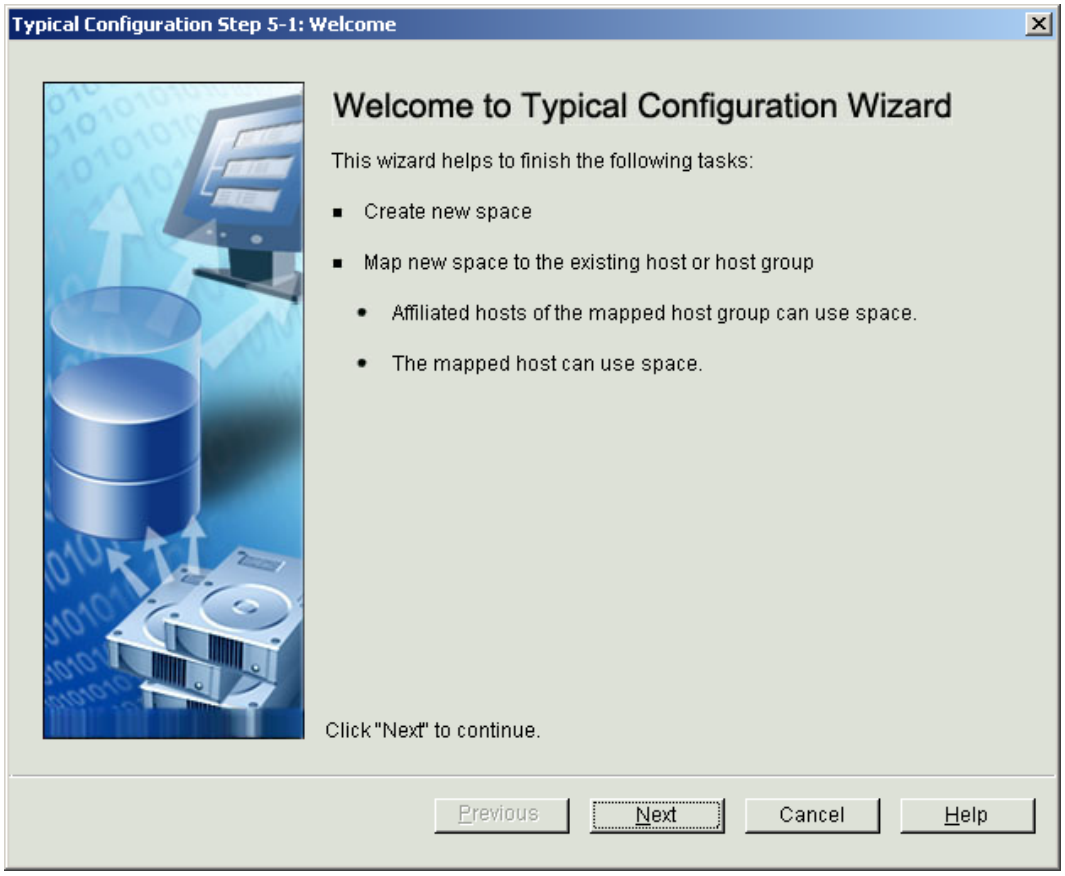
Procedure

Step 1 In the navigation tree, click the **Logical View** tab. Select the required S2600.

Step 2 On the menu bar, choose **Configuration** > **Typical Configuration...**.

The **Typical Configuration Step 5-1: Welcome** dialog box is displayed, as shown in **Figure 4-10**.

Figure 4-10 Typical Configuration Step 5-1: Welcome dialog box



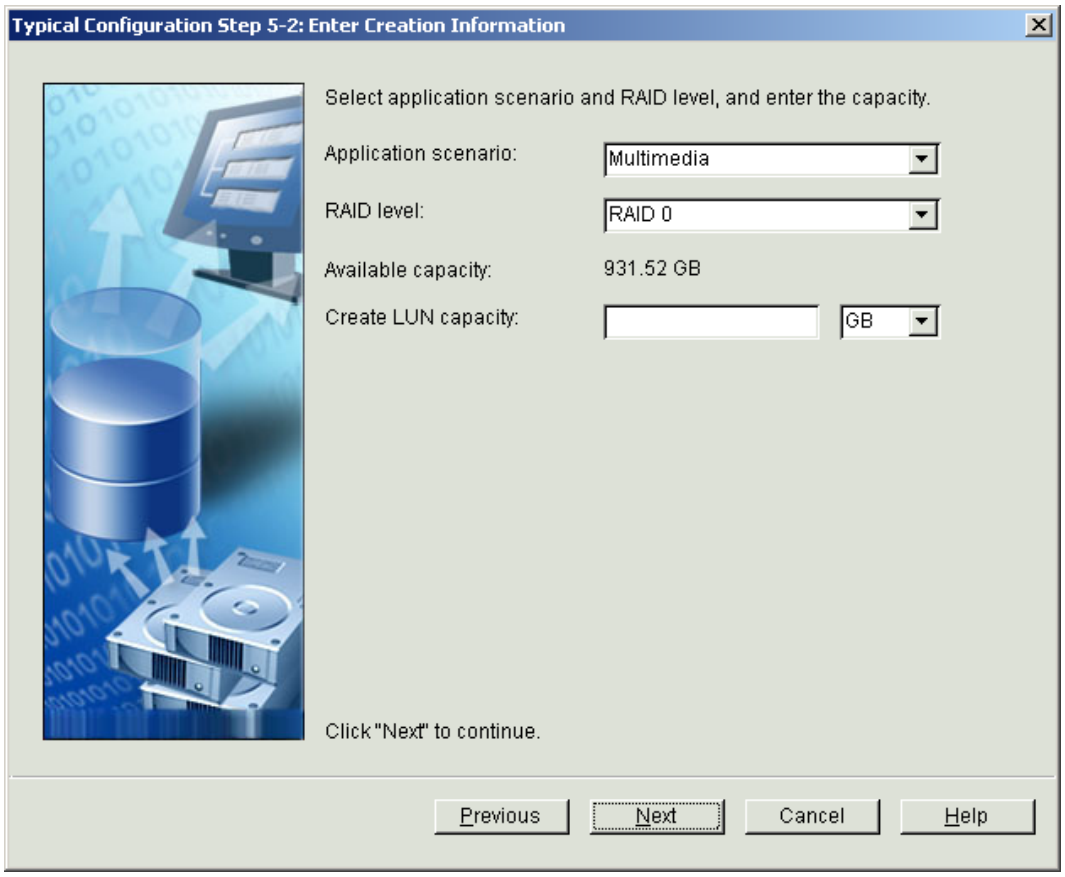
NOTE

During the typical application configuration, you can click **Cancel** as required. Then the configuration does not take effect.

Step 3 Click **Next**.

The **Typical Configuration Step 5-2: Enter Creation Information** dialog box is displayed, as shown in **Figure 4-11**

Figure 4-11 Typical Configuration Step 5-2: Enter Creation Information dialog box



Step 4 Select the scenario and the RAID level, and enter the capacity.

Table 4-3 lists the parameters for allocating capacity.

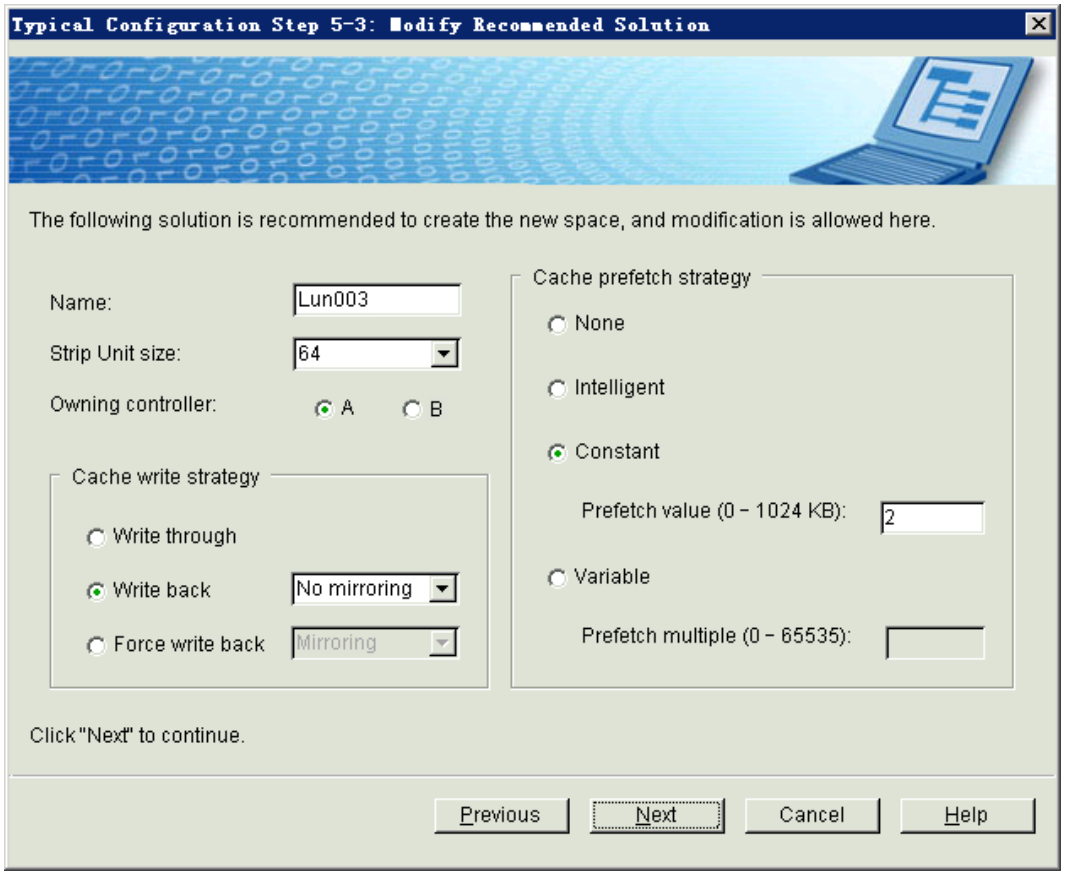
Table 4-3 Parameters for allocating capacity

Parameter	Description
Application scenario	The parameter indicates the scenario of allocating capacity. The value is **Multimedia**, **Database**, **File System**, or **Backup&Recovery**.
RAID level	The parameter indicates the RAID level for allocating capacity. The value is **RAID 0**, **RAID 1**, **RAID 10**, **RAID 6**, or **RAID 5**.
Create LUN capacity	The parameter indicates the allocated capacity. The value cannot exceed that of the **Available capacity**. The unit is TB, GB, or MB.

Step 5 Click **Next**.

The **Typical Configuration Step 5-3: Modify Recommended Solution** dialog box is displayed, as shown in **Figure 4-12**.

Figure 4-12 Typical Configuration Step 5-3: Modify Recommended Solution dialog box



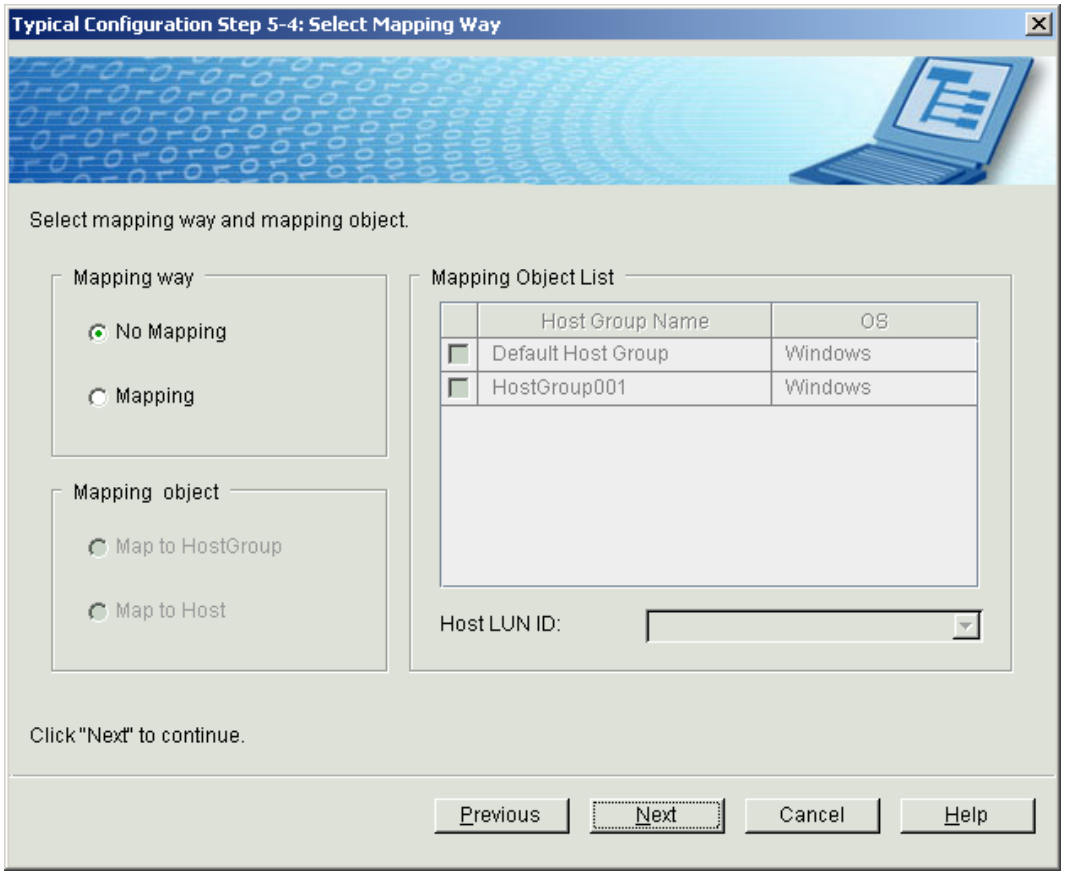
Step 6 Set the information about the recommended scheme.

For parameter description, see **Table 4-5** and **Table 4-6**.

Step 7 Click **Next**.

The **Typical Configuration Step 5-4: Select Mapping Way** dialog box is displayed, as shown in **Figure 4-13**.

Figure 4-13 Typical Configuration Step 5-4: Select Mapping Way dialog box



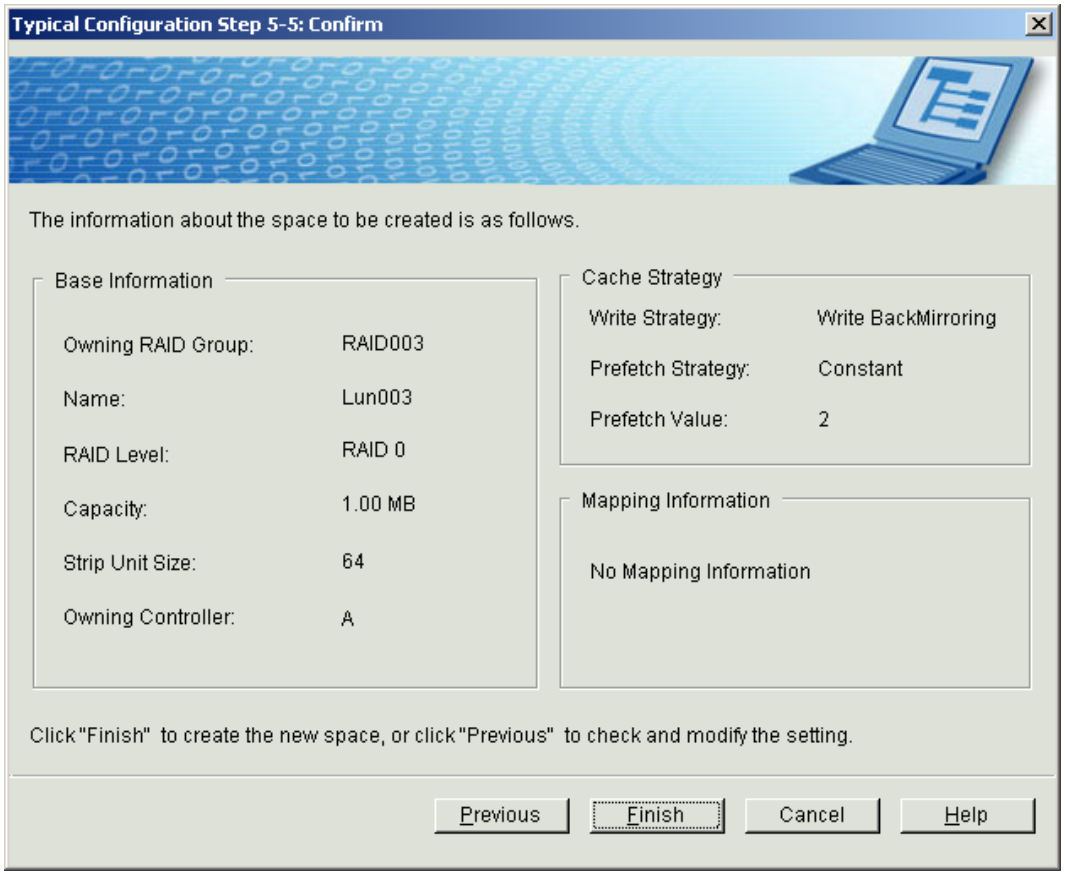
Step 8 Select a mapping way.

For parameter description, see **Table 4-7**.

Step 9 Click **Next**.

The **Typical Configuration Step 5-5: Confirm** dialog box is displayed, as shown in **Figure 4-14**.

Figure 4-14 Typical Configuration Step 5-5: Confirm dialog box



Step 10 Click **Finish**.

----End

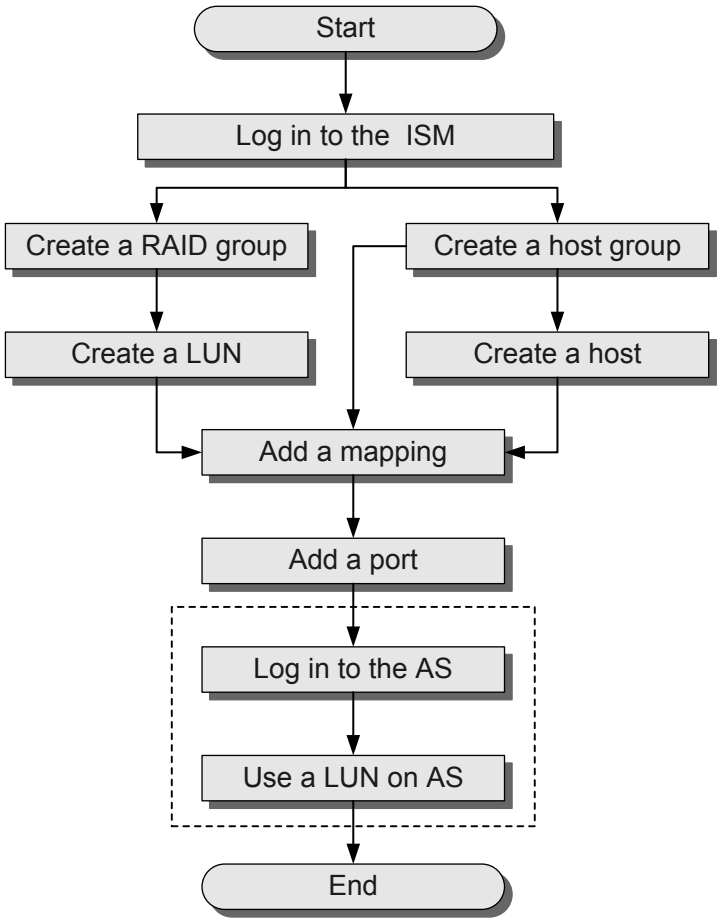
4.2 Configuration Flow Chart

After establishing a management environment for the S2600, you must configure the system through the OceanStor ISM for data access.

Flow Chart of the S2600S Initial Configuration

Figure 4-15 shows the flow chart of the S2600S initial configuration.

Figure 4-15 Flow chart of the S2600S initial configuration



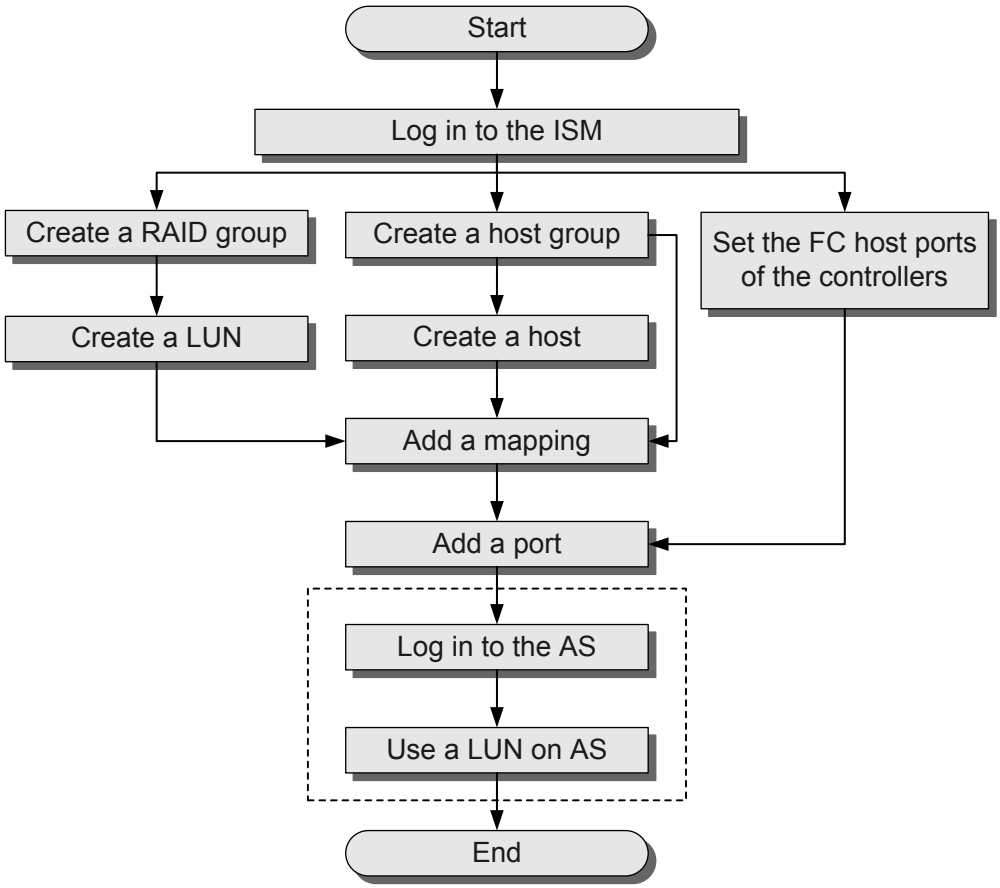
NOTE

The steps enclosed by dashed lines must be performed after you log in to the ASs.

Flow Chart of the S2600F Initial Configuration

Figure 4-16 shows the flow chart of the S2600F initial configuration.

Figure 4-16 Flow chart of the S2600F initial configuration



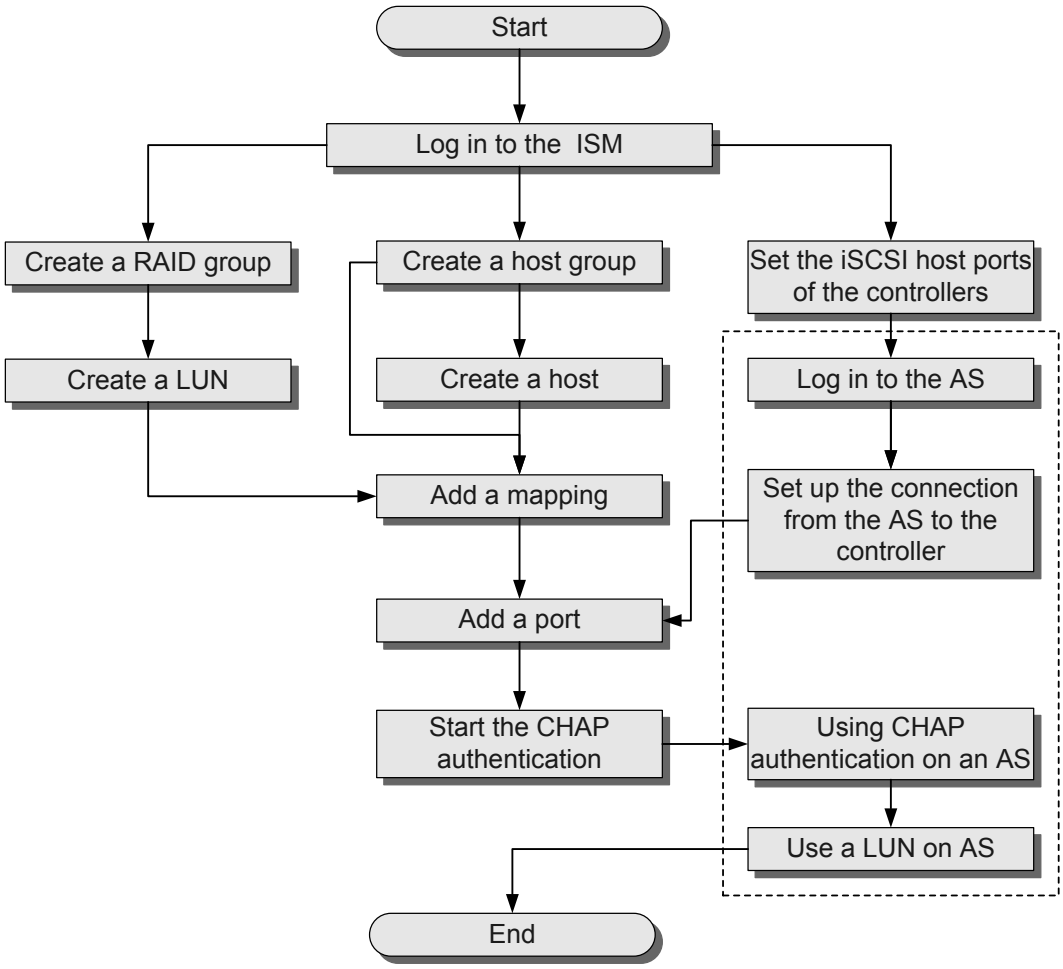
NOTE

The steps enclosed by dashed lines must be performed after you log in to the ASs.

Flow Chart of the S2600i Initial Configuration

Figure 4-17 shows the flow chart of the S2600i initial configuration.

Figure 4-17 Flow chart of the S2600i initial configuration



NOTE

The steps enclosed by dashed lines must be performed after you log in to the ASs.

Flow Chart of the S2600C Initial Configuration

For the FC networking of the S2600C initial configuration, see **Figure 4-16**, and for the iSCSI networking, see **Figure 4-17**.

4.3 Creating a RAID Group

Introduction to the creating a RAID group.

Context

The S2600 supports RAID 0, RAID 1, RAID 5, RAID 6, and RAID 10. Select a RAID level as required.

The four levels are compared as follows:

- Reliability

- RAID 0 does not provide the redundancy function. If one hard disk is damaged, all data cannot be accessed. RAID 0 is not suitable for key services because of its lowest reliability among all the four RAID levels.
- RAID 1 backups the data in real time by using the mirroring technology. In a RAID 1 group, every working disk has a mirroring disk. When the system writes data, the data must be written to the working disk and mirroring disks at the same time; when the system reads data, the data can be read from the working disk only. When the working disk is faulty, the mirroring disk will take over its services. After the faulty disk is replaced with a new hard disk, the data stored on the working disk can be reconstructed and restored. Compared with other RAID levels, RAID 1 has the highest reliability.
- RAID 5 adopts cyclic redundancy check (CRC) to guarantee the reliability of the stored data. The check data is distributed on each member disk in the RAID. When a member disk in the RAID fails, the data on the other member disks in the RAID can be used to reconstruct the data on the faulty member disk.
- RAID 6 produces the check data by performing two independent logical operations and distributes the check data separately on each member disk in the RAID group. RAID 6 allows the situation that two member disks are faulty at the same time. The data on the faulty disk can be reconstructed by the data on other member disks.
- RAID 10 has the characteristics of both RAID 1 and RAID 0. It stores data on the member disks in the RAID 1 group in a distributed way and provides a mirroring disk for each member disk so that data is stored in full redundancy mode. RAID 10 is more reliable than RAID 5.

- Read-write performance
  - RAID 0 supports concurrent read and write operations to provide the highest read-write speed. For an application of broad bandwidth, RAID 0 is preferred.
  - For RAID 1, when the system writes data, the data must be written to the working disk and mirroring disks at the same time; when the system reading data, the data can be read from the working disk only. Therefore, RAID 1 has lower performance than other RAID levels.
  - For an application of many write operations, RAID 5 is recommended. Generally, RAID 5 has higher write performance but lower read performance than RAID 10.
  - RAID 6 provides double data check; therefore, RAID 6 is complex and burdened by heavy load. The read/write performance is lower than that of RAID 5.
  - RAID 10 provides high read and write performance. More mirroring disks lead to higher read performance but lower write performance.
- Cost
  - The disk usage of RAID 0 is 100%, which means the lowest cost. − RAID 1 provides mirroring disks for a working disk, and the disk usage is 1/m, in which m stands for the number of mirroring disks. A RAID 1 group has lower disk usage and higher cost than a RAID 5 group.
  - The disk usage of a RAID 5 group is (n-1)/n, in which n stands for the number of member disks. For example, a RAID group consisting of three hard disks has the lowest disk usage, only 66.7%. The verification data in a RAID 5 group is equivalent to one hard disk capacity. Therefore, a RAID 5 group has a low storage cost.
  - The disk usage in RAID 6 is (n-2)/n (n is the number of member disks in the RAID group). When the RAID group is composed of four disks, the usage is the lowest only 50%. The amount of the check data in RAID 6 is equal to the capacity of two disks;

therefore, the storage cost of RAID 6 is higher than RAID 0 and RAID 5, and lower than RAID 1 and RAID 10.

- RAID 10 provides mirroring disks for a working disk, and the disk usage is 1/m, in which m stands for the number of mirroring disks. A RAID 10 group has lower disk usage and higher cost than a RAID 5 group.

CAUTION

- If the new RAID group has the same name as an existing RAID group, creating the RAID group fails.
- To ensure system reliability, create a hot-spare disk. A coffer disk cannot be used as a hot-spare disk. For details on how to create a hot-spare disk, see the *OceanStor S2600 Storage System Help*.

Procedure

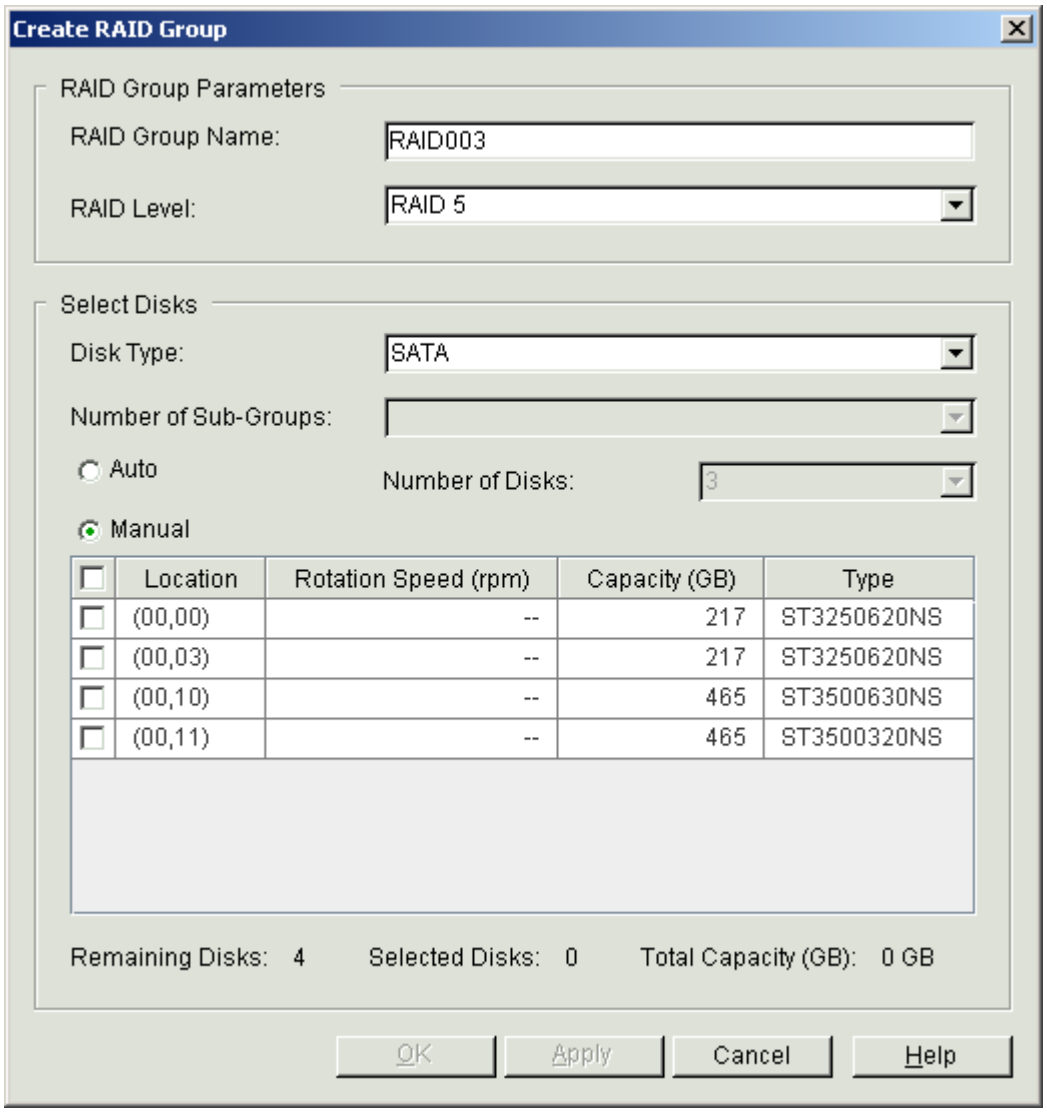
Step 1 On the OceanStor ISM main interface, click the **Logical View** tab.

In the navigation tree, click the storage array on which the RAID group is to be created.

Step 2 On the menu bar, choose **Configuration** > **Create RAID Group...**.

The **Create RAID Group** interface is displayed, as shown in **Figure 4-18**.

Figure 4-18 Create RAID Group interface



Step 3 Set the parameters for creating a RAID group.

Table 4-4 describes the parameters for creating a RAID group.

Table 4-4 Parameters for creating RAID group

Parameter	Description
RAID Group Name	The parameter indicates the name of the new RAID group. When setting this parameter, note that: ● The name of the new RAID group must be different from any existing RAID group names in the storage array. ● The value contains letters, digits, underscores, or hyphens only. ● The value contains a maximum of 32 characters.

Parameter	Description
RAID Level	The parameter indicates the level of the new RAID group. The value is **RAID 0**, **RAID 1**, **RAID 5**, **RAID 6**, or **RAID 10**.
Disk Type	The parameter indicates the disk type of the new RAID group. The value is **SAS** or **SATA**.
Number of Sub-Groups	The parameter is valid only when the RAID level is set to RAID 10. It indicates the number of RAID 10 mirroring groups. **NOTE** The value must be a divisor of the number of member disks in the RAID group, except 1. For example, for a RAID 10 group consisting of eight hard disks, you can set the number of sub-groups to 2 or 4. If it is set to 2, four hard disks form a mirroring group. These two hard disks are in 1+3 redundant mode. If it is set to 4, two hard disks form a mirroring group. These two hard disks are in 1+1 redundant mode.
Auto	After you select Auto, the system specifies member disks automatically.
Manual [a]	If you select Manual, you need to specify the member disks of the RAID group in the free disk list.
Number of Disks	The parameter indicates the number of member disks in a RAID group.
a: The parameter Location indicates the location where the disk is. In the controller enclosure or disk enclosure, the hard disk modules are numbered according to slot numbers from left to right and from top to bottom. The 12 slots are numbered from 00 to 11.The number of the slot on the left top of the controller enclosure is 00. For example, (00, 02) indicates that the disk is in enclosure 00 and slot 02.	

NOTE

- If the RAID Level is set to RAID 0, you need to choose at least two disks.
- If the RAID Level is set to RAID 1, you need to choose at least two disks.
- If the RAID Level is set to RAID 5, you need to choose at least three disks.
- If the RAID Level is set to RAID 6, you need to choose at least four disks.
- When the RAID level is set to RAID 10, at least four disks must be selected. The total number of member disks must be a multiple of the number of mirroring disks.
- If the number of free disks is less than the minimum number of disks required by a RAID group, corresponding RAID group levels are not listed in the drop-down list box.

Step 4 Click **OK**. The **Info** dialog box is displayed, stating "`Operation succeeded.`".

Step 5 Click **OK**.

----End

4.4 Creating a LUN

A logical unit number (LUN) refers to a logical group of disks that a controller provides for an AS.

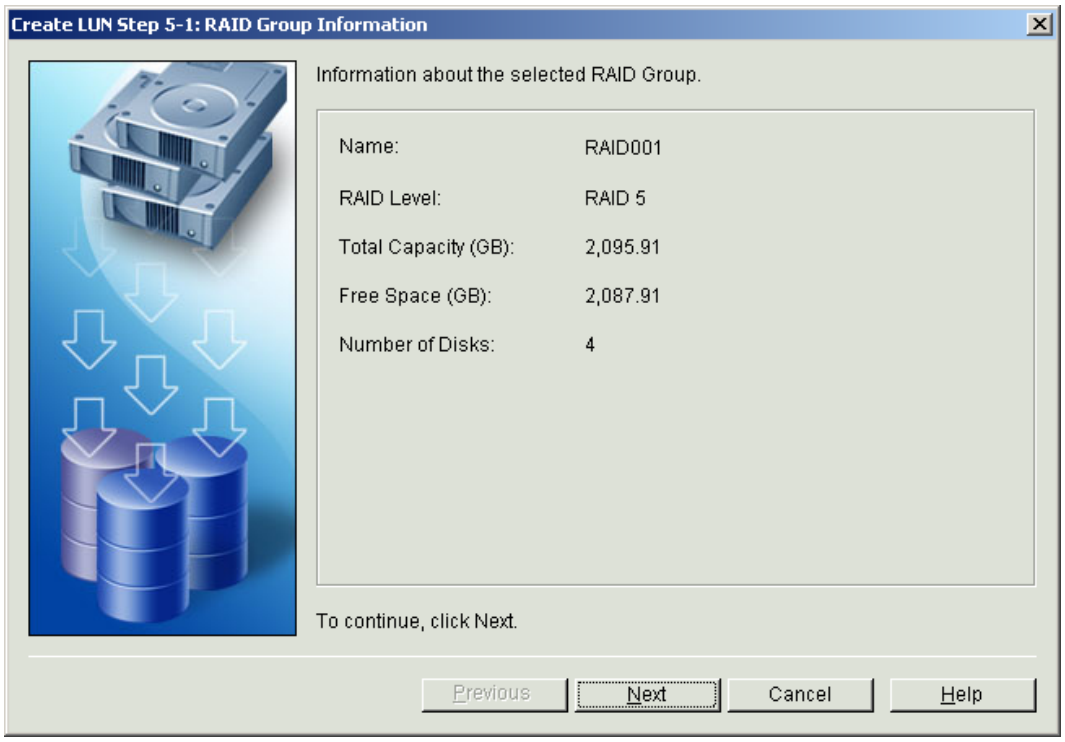
Procedure

Step 1 On the OceanStor ISM main interface, click the **Logical View** tab. In the navigation tree, click the RAID group on which the LUN is to be created.

Step 2 On the menu bar, choose **Configuration** > **Create LUN...**.

The **Create LUN Step 5-1: RAID Group Information** interface is displayed, as shown in **Figure 4-19**.

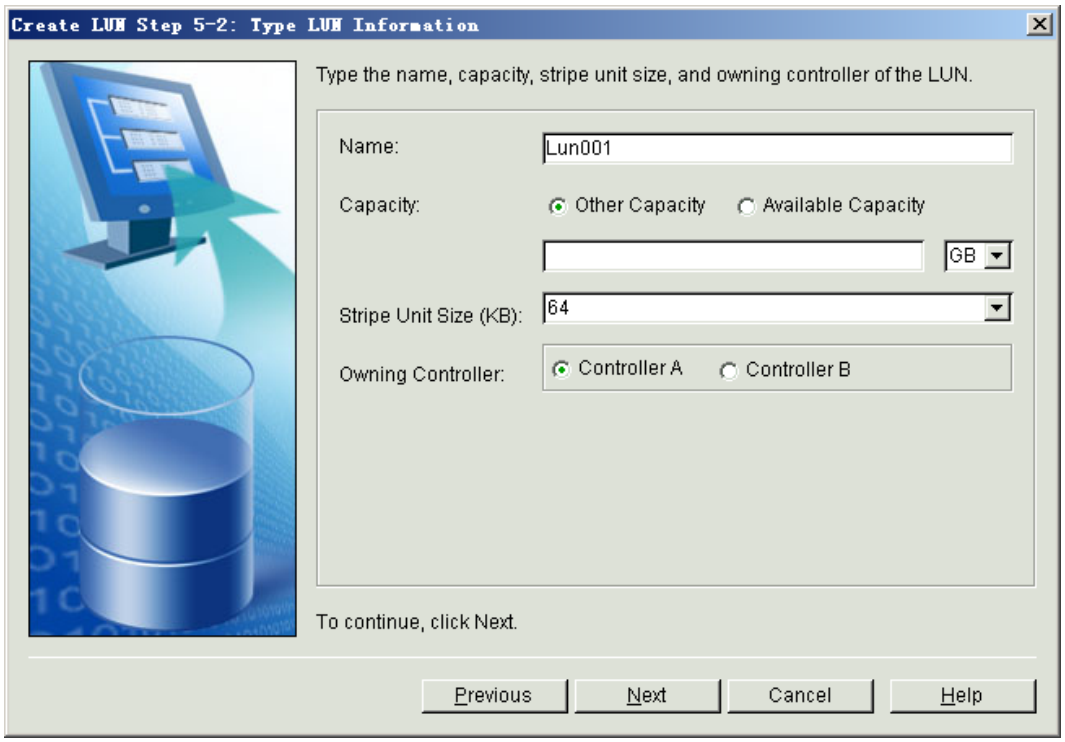
Figure 4-19 Create LUN Step 5-1: RAID Group Information interface



Step 3 Click **Next**.

The **Create LUN Step 5-2: Type LUN Information** interface is displayed, as shown in **Figure 4-20**.

Figure 4-20 Create LUN Step 5-2: Type LUN Information interface



Step 4 Set the parameters for creating a LUN.

Table 4-5 describes the parameters for creating a LUN.

Table 4-5 Parameters for creating a LUN

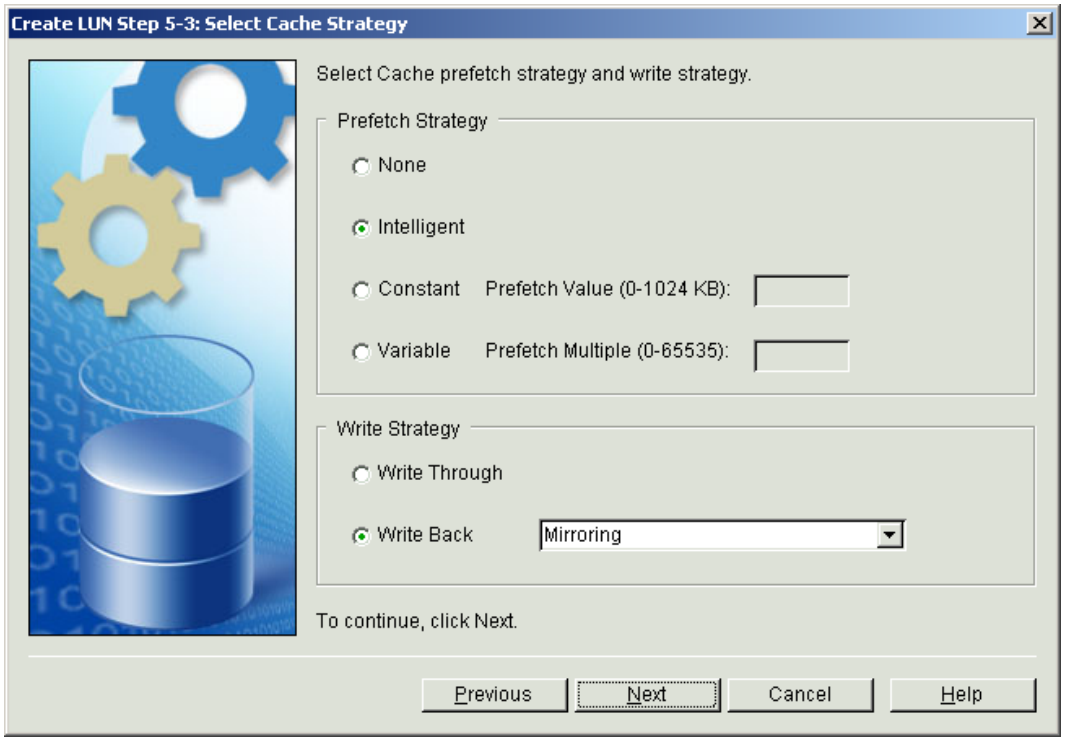
Parameter	Description
Name	The parameter indicates the name of the new LUN. When setting this parameter, note that: ● The name of the new LUN must be different from any existing LUN names in the storage array. ● The value contains letters, digits, underscores, or hyphens only. ● The value contains a maximum of 32 characters.
Capacity	The parameter indicates the capacity of the new LUN. ● **Other Capacity** It indicates that you can set the capacity manually. When setting this parameter, note that: - The maximum capacity is the remaining capacity of the RAID group that the LUN belongs to. - Unit: MB, GB, and TB. ● **Available** It indicates that the capacity is automatically set to the remaining capacity of the RAID group that the LUN belongs to.

Parameter	Description
Stripe Unit Size [a]	The parameter indicates the stripe unit size of the LUN. In relation to a disk storage array in which data is mapped stripe by stripe, the stripe unit size refers to the quantity of blocks in a stripe. Also, in relation to a single member disk area in a RAID group, the stripe unit size refers to the quantity of consecutively addressed blocks that the consecutively addressed virtual disks are mapped to. The unit is KB. The value is 4, 8, 16, 32, 64, 128, 256, or 512.
Owning Controller	This parameter specifies the owning controller on which the LUN is to be created. All the host I/O requests of the LUN are handled by the owning controller by default. The value is **controller A** or **controller B**.
a: Affecting the I/O performance, the stripe unit size must be selected properly for different applications. For example, if the system mainly stores sequential data, for example, media data, set a large stripe unit size. If the system stores much random data, for example, transaction data, set a small stripe unit size.	

Step 5 Click **Next**.

The **Create LUN Step 5-3: Select Cache Strategy** interface is displayed, as shown in **Figure 4-21**.

Figure 4-21 Create LUN Step 5-3: Select Cache Strategy interface



Step 6 Choose the cache prefetch policy and the cache write policy.

Table 4-5 describes the parameters for the cache prefetch policy and the write policy.

Table 4-6 Parameters for the cache prefetch policy and the cache write policy

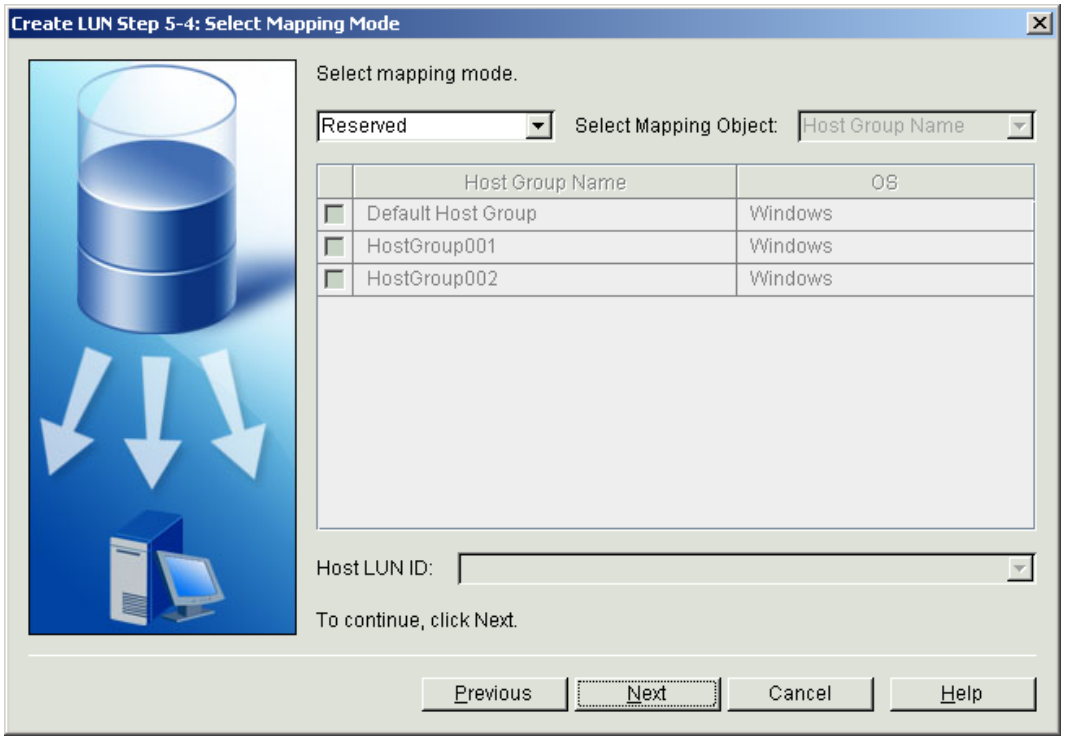
Parameter	Description
Prefetch Strategy	The parameter indicates the cache prefetch policy. This improves read performance. ● Constant: indicates that the prefetched data is the same as that of settings. The policy is used in sequential read application where the data amount is fixed. For example, in the multi-user streaming media on demand, the streaming media files on the server use the streams with the same code rate, such as 1.5 Mbit/s. ● Variable: indicates that the prefetched data is a multiple of the data in the current operation. The policy is used in sequential read application whose size is not fixed or is used when multiple users read data at the same time but they cannot determine the prefetched size of the data and cannot set the data according to the fixed prefetch data. For example, in the multi-user streaming media on demand, the streaming media files on the server use different rates of code streams, such as 1.2 Mbit/s, 1.5 Mbit/s, or 1.8 Mbit/s. ● Intelligent: indicates that the system software operates a proper prefetched data. The policy is used in read application of a single stream or when you do not know whether the application has a sequence, for example, the read and write of a file. ● None: indicates that the prefetch function is disabled. In this case, the system has the lowest read performance. The policy is used in random read application or prefetched read application, such as database application. The policy affects the read performance. It is recommended to use intelligent prefetch. If you are familiar with the applications of the product, such as a continuous data with a large traffic, you can use the constant prefetch policy or the variable prefetch policy accordingly.
Prefetch Value	The parameter indicates the prefetch value when the cache prefetch policy is the constant prefetch. The value ranges from 0 to 1024 KB. When the value of **Prefetch Policy** is **Constant**, the parameter is available.
Prefetch Multiple	The parameter indicates that the prefetched data is a multiple of the data in the current operation when the prefetch strategy is the variable prefetch. The value ranges from 0 to 65535. When the value of **Prefetch Policy** is **Variable**, the parameter is available.

Parameter	Description
Write Strategy	The parameter indicates the cache write policy. ● Write Through: It indicates that the data can be written to the disk directly. The host accesses the disk during each write operation. This policy has low performance and high reliability. ● Write Back, Mirroring: It indicates that the data can be written to the local cache and the peer cache at the same time. This policy has a higher performance and reliability. ● Write Back, No Mirroring [a]: It indicates that the data can be written to the local cache only. This policy has high performance and general reliability.
a: When the **Write Strategy** is set to **Write Back, No Mirroring**, data is written in only the local cache.	

Step 7 Click **Next**.

The **Create LUN Step 5-4: Select Mapping Mode** interface is displayed. See **Figure 4-22**. If you select **Reserved**, go to **Step 9**. If you select **Map**, go to **Step 8**.

Figure 4-22 Create LUN Step 5-4: Select Mapping Mode interface



Step 8 Choose the LUN mapping object by clicking the option button in front of a host or host group.

For parameter description, see **Table 4-7**.

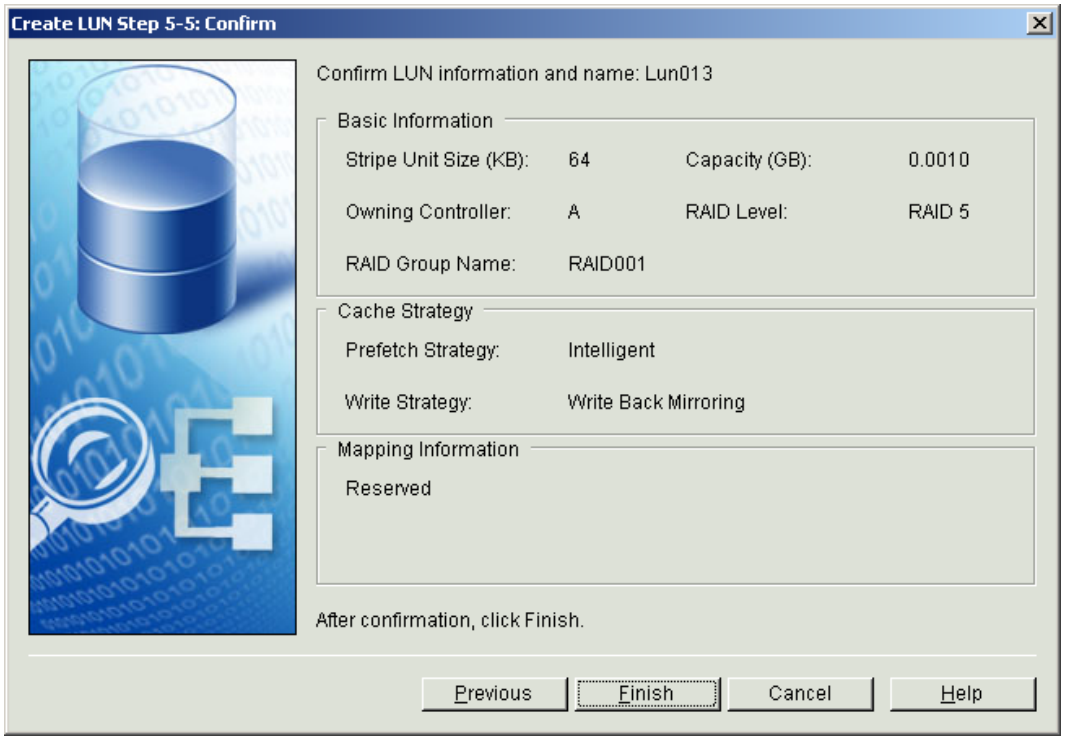
Table 4-7 Parameters for choosing the LUN mapping object

Parameter	Description
Select Mapping Object	The parameter indicates that you need to choose the LUN mapping object. ● Host Group Name: The system lists the host groups. The displayed information consists of host group names and OSs. ● Host Name: The system lists the hosts. The displayed information consists of host names, their host group names, and OSs.
Host LUN ID	The parameter indicates the LUN ID allocated by the system when a LUN is mapped to a host or a host group. If the mapping is removed, the ID of the corresponding LUN is released for the LUN that will be mapped to that host or host group in the future.

Step 9 Click **Next**.

The **Create LUN Step 5-5: Confirm** interface is displayed, as shown in **Figure 4-23**.

Figure 4-23 Create LUN Step 5-5: Confirm interface



Step 10 Click **Finish**. The **Info** dialog box is displayed, stating "`Operation succeeded.`".

Step 11 Click **OK**.

----End

4.5 Creating a Host Group

Through creating host groups, the OceanStor ISM can manage hosts of the same type easily.

Context

You can create a maximum of 32 host groups in the system.

NOTE

You can choose to use the **Default Host Group**, here you can leap over this section.

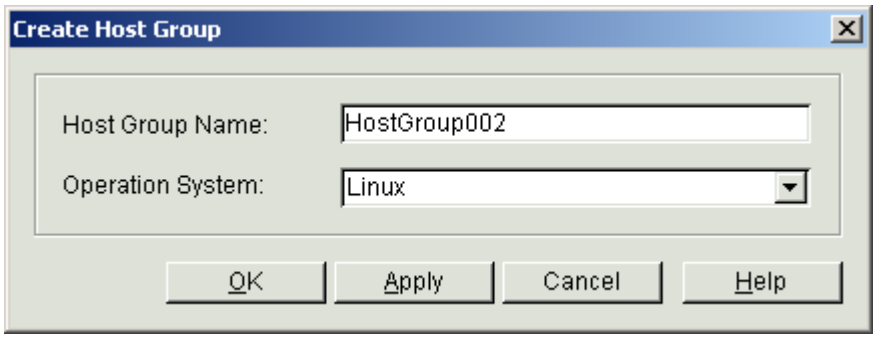
Procedure

Step 1 On the OceanStor ISM main interface, click the **Logical View** tab. In the navigation tree, click the required storage array.

Step 2 On the menu bar, choose **Configuration** > **Create Host Group...**.

The **Create Host Group** interface is displayed, as shown in **Figure 4-24**.

Figure 4-24 Create Host Group interface



Step 3 Set the parameters for creating a host group.

Table 4-8 describes the parameters for creating a host group.

Table 4-8 Parameters for creating a host group

Parameter	Description
Host Group Name	The parameter indicates the host group name. When setting this parameter, note that: ● In a storage array, the new host group name must be different from any existing host group names. ● The value contains letters, digits, underscores, or hyphens only. ● The value contains a maximum of 32 characters.

Parameter	Description
Operation System	This parameter indicates the OS type of the hosts in the host group. Value range: "Suse Linux", "Windows Server 2003", "Solaris", "HP-UX", and "AIX".

Step 4 Click **OK**. The **Info** dialog box is displayed, stating "`Operation succeeded.`".

Step 5 Click **OK**.

----End

4.6 Creating a Host

The host displayed on the OceanStor ISM interface is virtually created for easier management. It cannot be mapped to a physical AS unless a port has been added to this virtual host.

Context

You can create a maximum of 256 hosts in the system.

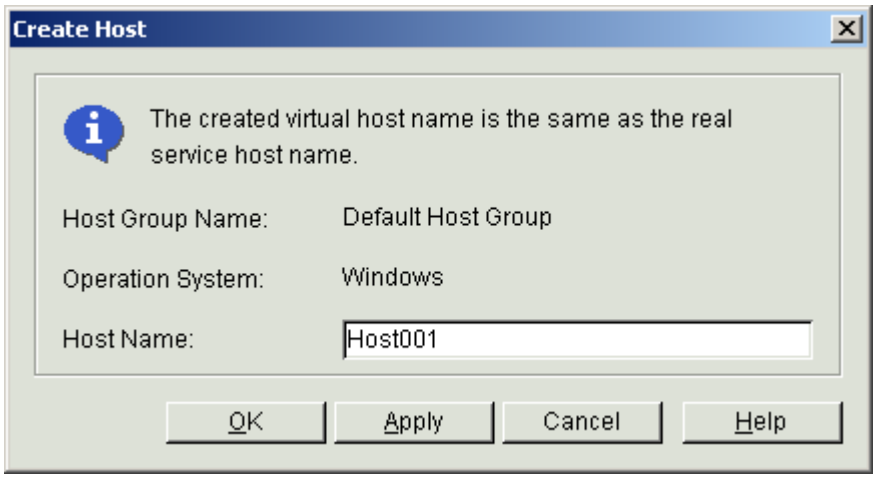
Procedure

Step 1 On the OceanStor ISM main interface, click the **Logical View** tab. In the navigation tree, click the required host group.

Step 2 On the menu bar, choose **Configuration** > **Create Host...**.

The **Create Host** interface is displayed, as shown in **Figure 4-25**.

Figure 4-25 Create Host interface



Step 3 Enter the name of the new host.

Table 4-9 describes the parameter for creating a host.

Table 4-9 Parameter for creating a host

Parameter	Description
Host Name	The parameter indicates the host name. When setting this parameter, note that: ● In a host group, the new host name must be different from any existing host names. ● The value contains letters, digits, underscores, or hyphens only. ● The value contains a maximum of 32 characters.

Step 4 Click **OK**. The **Info** dialog box is displayed, stating "`Operation succeeded.`".

Step 5 Click **OK**.

----End

4.7 Setting the FC Host Port on the Controller

To ensure the optimal port performance and to connect the controller to the server, the rate of the FC host port must be set correctly.

Context

- You need to set the rate only for front-end FC host ports.
- Modifying the rate of the FC host port online interrupts I/O.
- The FC host port supports the optical module of 1 Gbit/s, 2 Gbit/s, 4 Gbit/s, or auto-adaptation. Ensure that the rate of the FC host port must be the same as that of the FC HBA interface on the AS. Otherwise, a communication failure occurs.

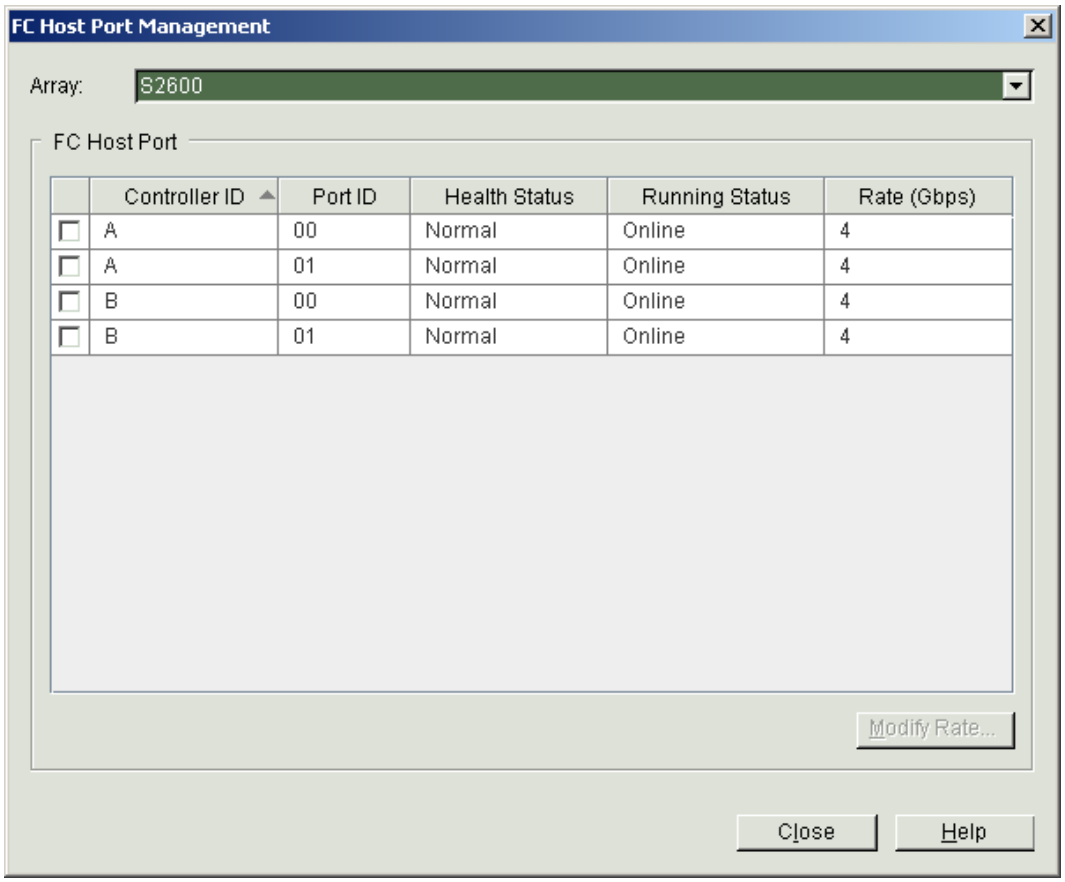
Procedure

Step 1 On the OceanStor ISM main interface, click the **Physical View** tab. In the navigation tree, click the required controller enclosure.

Step 2 On the menu bar of the OceanStor ISM main interface, choose **Configuration** > **FC Host Port Management...**.

The **FC Host Port Management** interface is displayed. See **Figure 4-26**.

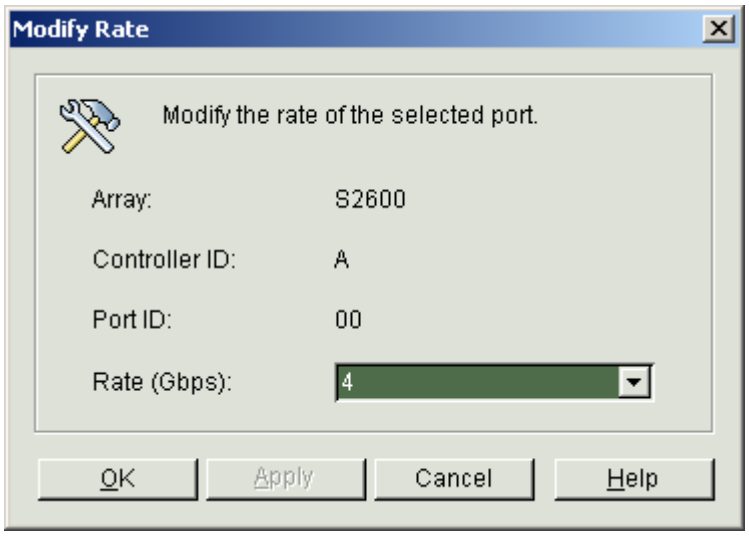
Figure 4-26 FC Host Port Management interface



Step 3 Select the required FC host port, and then click **Modify Rate...**.

The **Modify Rate** interface is displayed, as shown in **Figure 4-27**.

Figure 4-27 Modify Rate interface



Step 4 Select the rate of the FC host port.

NOTE

- The rate of an FC interface is 1 Gbps, 2 Gbps, 4 Gbps, or Auto-Adapt. Auto-Adapt indicates that the rate of the interface is automatically consistent with that of the HBA.
- You can execute the rate modification for the same FC host port at least every two minutes.

Step 5 Click **OK**. The **Info** dialog box is displayed, stating "`Operation succeeded.`".

Step 6 Click **OK**.

----End

4.8 Setting the iSCSI Host Port on the Controller

Only when correct parameters are set, can the iSCSI host port of the controller be connected to the server.

Context

- You need to set the IP addresses for only front-end iSCSI host ports.
- If you modify the IP address of the iSCSI host port, the services connected to this host port are interrupted. Therefore, perform this operation with caution.

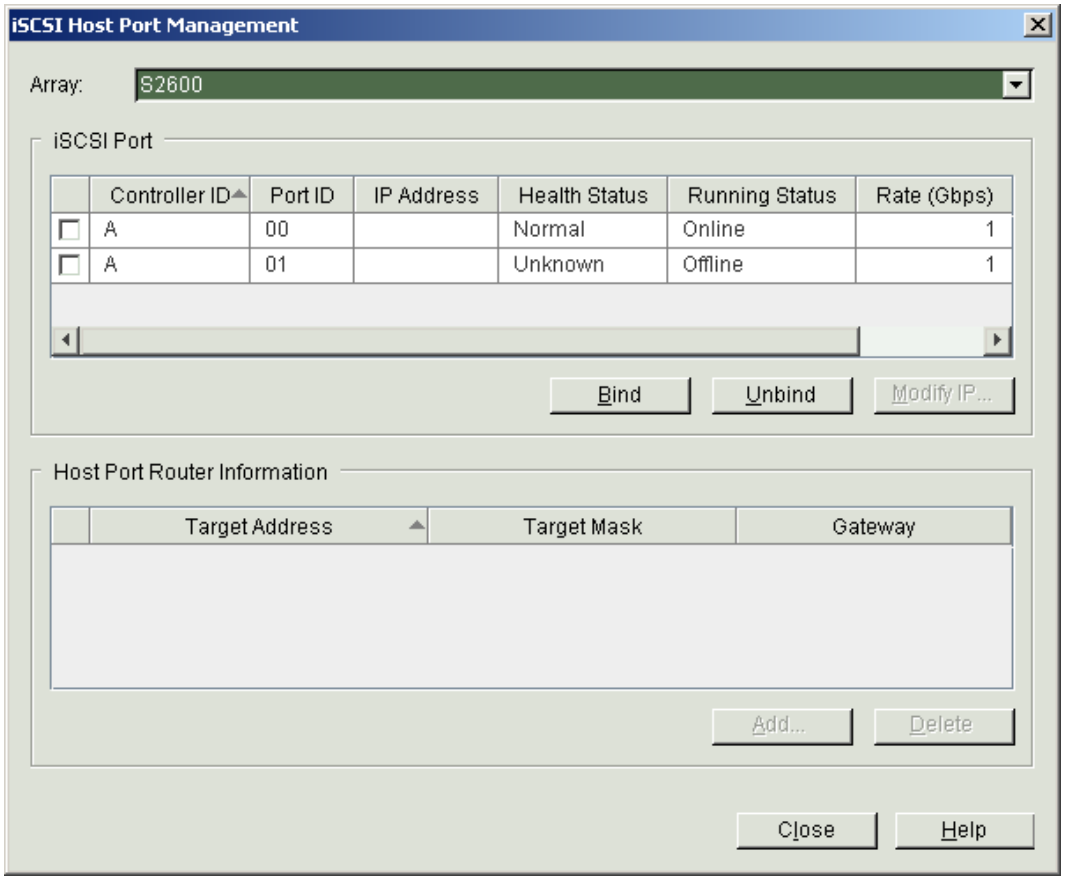
Procedure

Step 1 On the OceanStor ISM main interface, click the **Physical View** tab. In the navigation tree, click the controller enclosure on which the IP address of an iSCSI host port is to be set.

Step 2 On the menu bar, choose **Configuration** > **iSCSI Host Port Management...**.

The **iSCSI Host Port Management** interface is displayed, as shown in **Figure 4-28**.

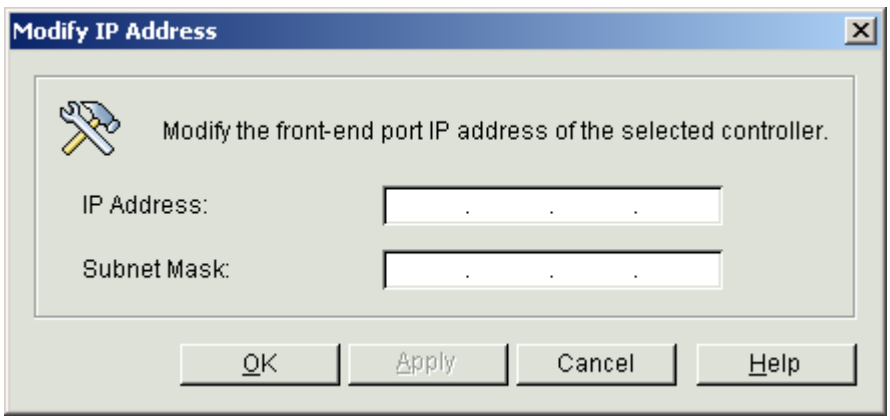
Figure 4-28 iSCSI Host Port Management interface



Step 3 Choose the host port and then click **Modify IP...**.

The **Modify IP Address** interface is displayed, as shown in **Figure 4-29**.

Figure 4-29 Modify IP Address interface



Step 4 Enter the IP address and subnet mask of the iSCSI host port.

Table 4-10 describes the parameters for setting the IP address.

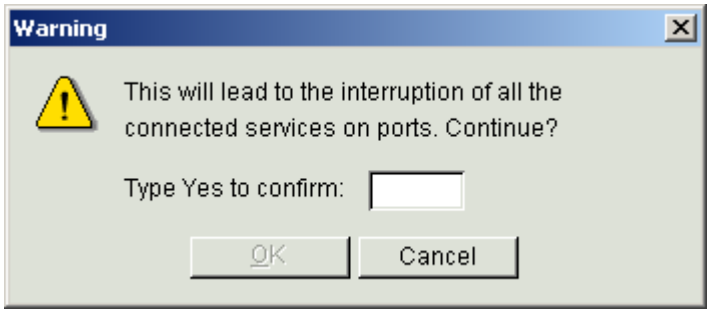
Table 4-10 Parameters for setting the IP address

Parameter	Description
IP Address	The parameter indicates the IP address. When setting this parameter, note that: ● The first field on the left ranges from 1 to 223 (excluding 127). ● The last field ranges from 1 to 254. ● The other fields range from 0 to 255. ● When configuring the network segment, do not use the public network segment. For details, see related books.
Subnet Mask	This parameter indicates the subnet mask of the iSCSI host port. When setting this parameter, note that: Each field is an integer that ranges from 0 to 255. In addition, the last field cannot be 255.

Step 5 Click **OK**.

The **Warning** dialog box is displayed, as shown in **Figure 4-30**.

Figure 4-30 Warning dialog box



Step 6 In the text box, enter **Yes**, and then click **OK**.

The **Info** dialog box is displayed, stating "`Operation succeeded.`".

Step 7 Click **OK**. If you want to set the router information of the iSCSI host port, perform **Step 8** through **Step 12**.

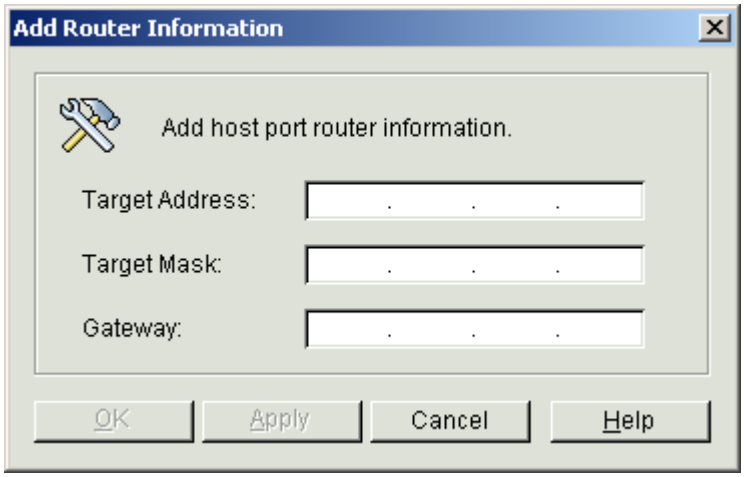
When the IP address of the iSCSI host port is on the different subnet with that of the AS, you need to configure the routing information of the iSCSI host port.

Step 8 On the interface as shown in **Figure 4-28**, select the required interface.

Step 9 Click **Add...**.

The **Add Router Information** dialog box is displayed. See **Figure 4-31**.

Figure 4-31 Add Router Information dialog box



Step 10 Enter the router information.

Table 4-11 lists the related parameter description.

Table 4-11 Parameters for adding router information

Parameter	Description
Target Address	This parameter indicates the IP address of the network interface on the AS. The first field on the left ranges from 1 to 223 (excluding 127). The last field ranges from 1 to 254, and the other fields range from 0 to 225.
Target Mask	This parameter indicates the subnet mask of the IP address of the network interface on the AS. The value of each field is an integer that ranges from 0 to 255.
Gateway	This parameter indicates the IP address of the gateway to which the iSCSI host port belongs. When setting this parameter, note that: ● The value of each field is an integer that ranges from 0 to 255. ● The value of the last field cannot be 255.

NOTE

- When configuring the network segment, do not use the public network segment. For details, see *OceanStor S2600 Storage System User Guide*.
- S2600 provides bind and unbind function for iSCSI, for details, see *OceanStor S2600 Storage System User Guide*.

Step 11 Click **OK**. The **Info** dialog box is displayed, stating "`Operation succeeded.`".

Step 12 Click **OK**.

----End

Postrequisite

After configuring the IP addresses for the iSCSI host ports, you must log in to the ASs as the administrator to configure IP addresses for the network interfaces on the ASs. Ensure that the IP address of at least one of these network interfaces is on the same network segment as that of the iSCSI host port and the connection is set up successfully.

4.9 Starting CHAP Authentication

The system provides the CHAP management function when you configure the iSCSI host ports for the controller. After CHAP user authentication is started, ASs can access the storage system securely.

Context

- The system provides the CHAP management function when you configure the iSCSI host ports for the controller.
- By default, the iSCSI host port does not enable CHAP authentication. If enabled, CHAP authentication is performed at the S2600 when the AS connects to the S2600.

4.9.1 Creating a CHAP User

CHAP users created on the OceanStor ISM are legal users of the storage system. When the CHAP User authentication is enabled, only these users can access the storage system.

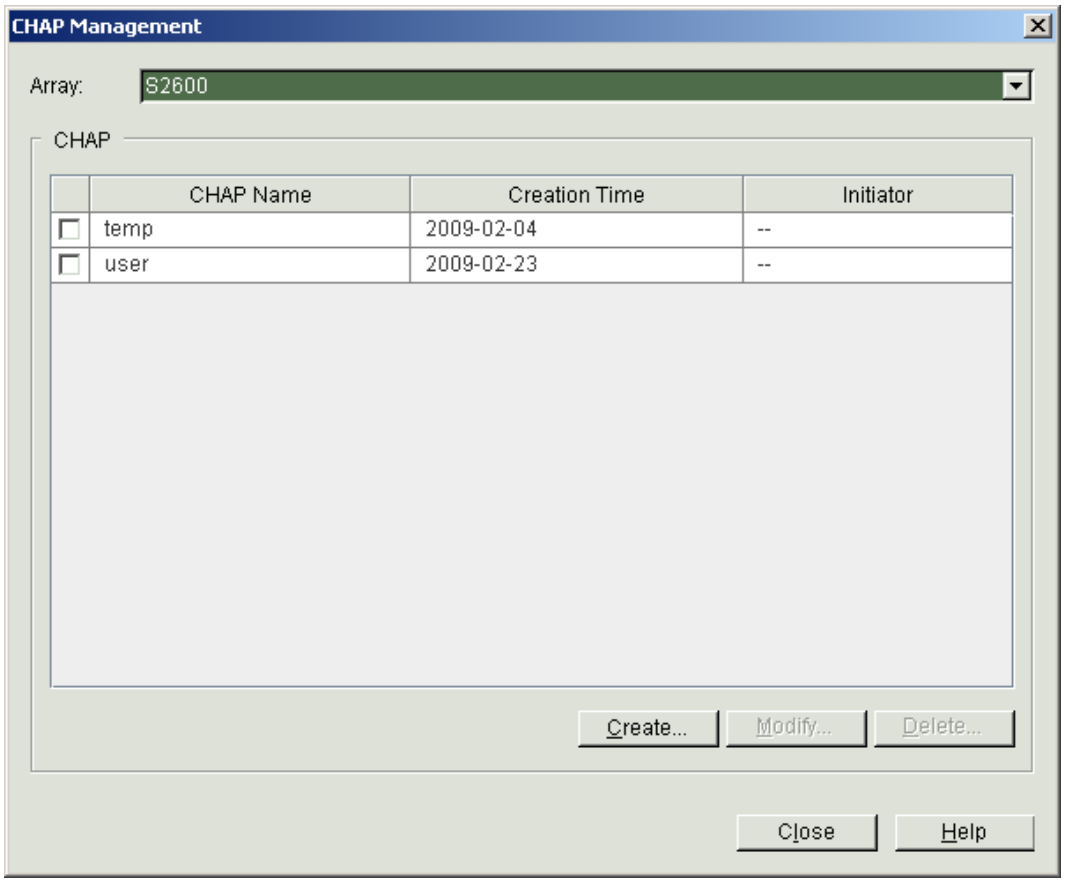
Procedure

Step 1 In the navigation tree of the OceanStor ISM main interface, click the required storage array.

Step 2 On the menu bar, choose **Security** > **CHAP Management...**.

The **CHAP Management** interface is displayed, as shown in **Figure 4-32**.

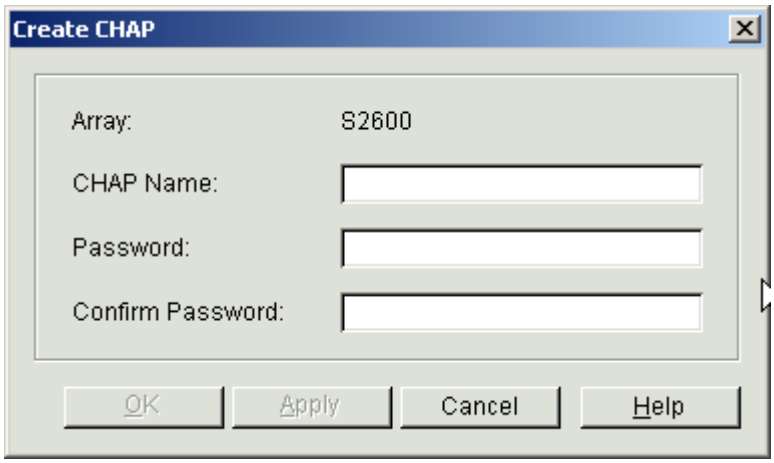
Figure 4-32 CHAP Management interface



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

The **Create CHAP** interface is displayed, as shown in **Figure 4-33**.

Figure 4-33 Create CHAP interface



Step 4 Enter the information about a CHAP user.

Table 4-12 describes the parameters for creating a CHAP user.

Table 4-12 Parameters for creating a CHAP user

Parameter	Description
CHAP Name	The parameter indicates the name of the new CHAP user. When setting this parameter, note that: ● The name must be different from any existing CHAP user names. ● The name contains letters, numbers, underscores, or hyphens. ● The length of the value ranges from 4 to 25 characters.
Password	The parameter indicates the password of the CHAP user. The length of the password ranges from 12 to 16 characters.
Confirm Password	The parameter indicates that you need to enter password of the CHAP user again. ● The length of the password ranges from 12 to 16 characters. ● The confirm password must be the same as the value of **Password**.

Step 5 Click **OK**.

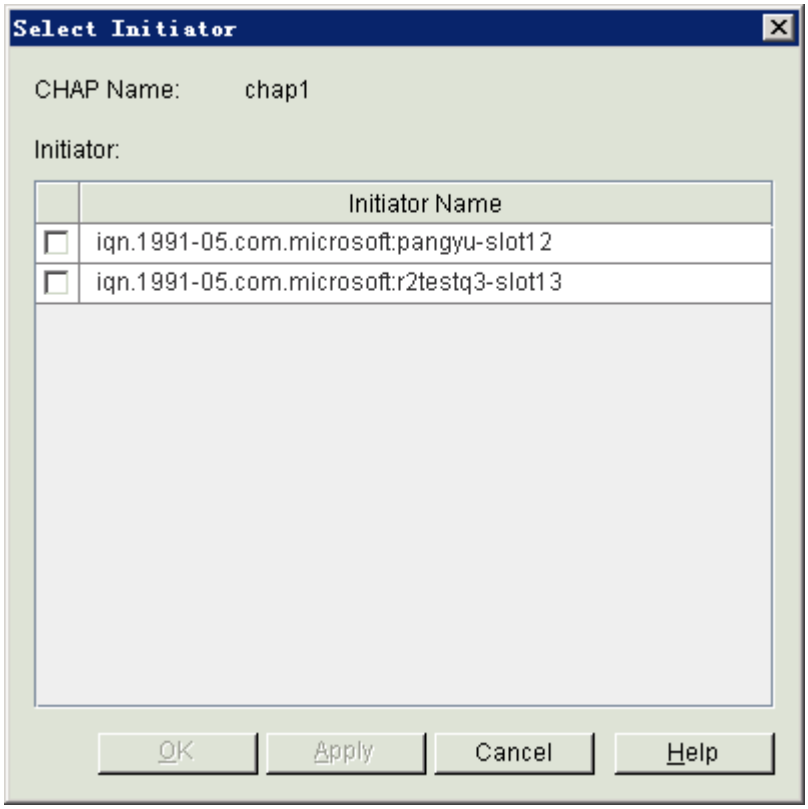
The **Warning** dialog box is displayed, saying "`Creating CHAP succeeded. Do you want to add it to the initiator?`".

If you plan to add an initiator to a CHAP user, go to **Step 6**; otherwise, go to **Step 9**.

Step 6 Click **OK**.

The **Select Initiator** dialog box is displayed, as shown in **Figure 4-34**.

Figure 4-34 Select Initiator interface



Step 7 Choose the initiator of the AS corresponding to the CHAP user.

Step 8 Click **OK**.

The Info dialog box is displayed, stating "`Operation succeeded.`".

Then go to **Step 10**.

Step 9 Click **Cancel**.

Step 10 Click **OK**.

----End

4.9.2 Enabling CHAP authentication

Introduction to enabling CHAP authentication.

Prerequisite

- A CHAP user is created and allocated to the initiator.
- The CHAP authentication is disabled.

When you set up a connection between a controller and the AS through the OceanStor ISM, CHAP authentication is not used by default. To connect them in the CHAP authentication, you can start CHAP user authentication for the iSCSI host ports.

Procedure

Step 1 On the OceanStor ISM main interface, click the **Logical View** tab. In the navigation tree, click a host on which CHAP authentication is to be started.

Step 2 On the menu bar, choose **Configuration** > **Initiator Management...**. The **Initiator Management** interface is displayed.

Step 3 Click the initiator on which CHAP authentication is **Disabled**.

Step 4 Click **Enable**.

The **Info** dialog box is displayed, stating "`Operation succeeded.`".

Step 5 Click **OK**.

----End

4.10 Setting Up the Connection from the AS to the Controller

After configuring iSCSI host ports, you need to log in to the AS to set related parameters.

Context

- The name of the iSCSI host port must be unique.
- You need to set up the connection from the AS to the controller if iSCSI host ports are configured in a storage array.

Take the Windows Server 2003 AS as an example.

NOTE

For an AS in Windows with other versions, adjust the steps as required.

Procedure

Step 1 Log in to the Windows AS with the **Administrator** account.

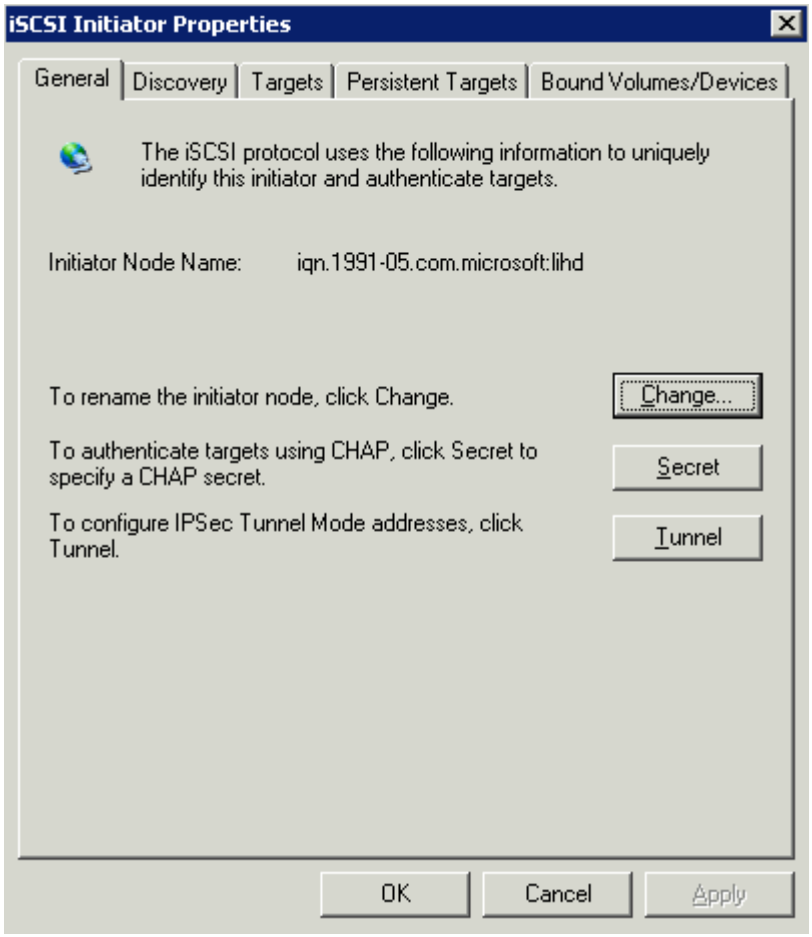
Step 2 Install the **Microsoft iSCSI Initiator** program.

NOTE

- After installation, please restart the AS.
- The Microsoft iSCSI Initiator installation program can be downloaded from the Microsoft Web site. Install the Microsoft iSCSI Initiator in version 2.01 or a later version.
- If you need to install the multipath software developed by Huawei , do not select the check box next to **Microsoft MPIO Multipathing Support for iSCSI**.

Step 3 Run the Microsoft iSCSI Initiator software. The **iSCSI Initiator Properties** interface is displayed. See **Figure 4-35**.

Figure 4-35 iSCSI Initiator Properties interface

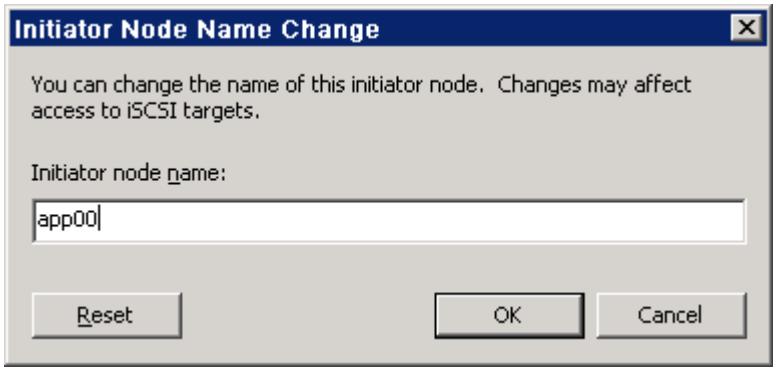


Step 4 Click **Change...**.

The **Initiator Node Name Change** dialog box is displayed. See **Figure 4-36**.

Change the name of the initiator of the AS.

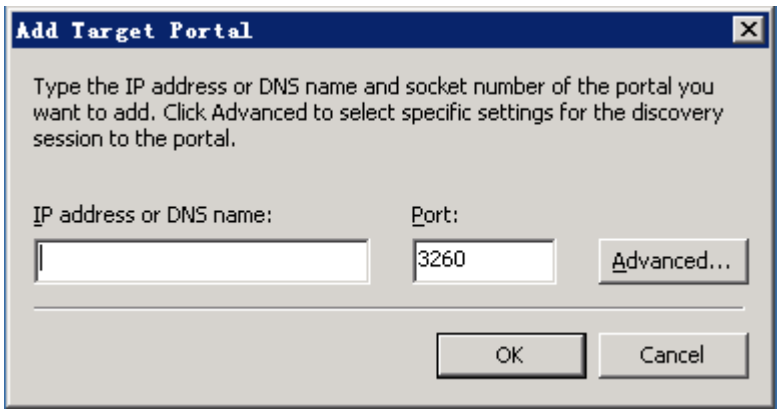
Figure 4-36 Initiator Node Name Change dialog box



Step 5 Click the **Discovery** tab and then click **Add**.

The **Add Target Portal**dialog box is displayed. See **Figure 4-37**.

Figure 4-37 Add Target Portal dialog box



CAUTION

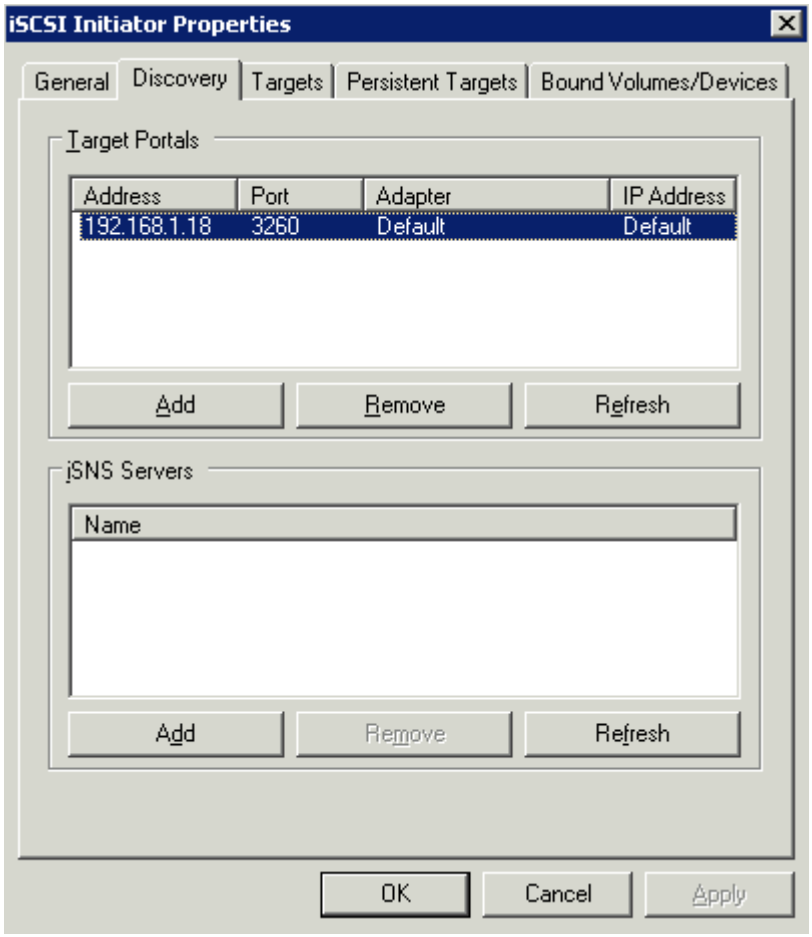
You need to set the IP address of each iSCSI host port on the controller. Ensure that the IP addresses are on the different network segments from those of management network interfaces.

Step 6 In the IP address or DNS name text box, enter the IP address of the iSCSI host port connecting to the AS. For details, see "**4.8 Setting the iSCSI Host Port on the Controller**".

Step 7 Click **OK**.

The IP address is displayed in the **Target Portals** group box. See **Figure 4-38**.

Figure 4-38 Check target ports



Step 8 If CHAP user authentication is disabled, click the **Targets** tab and click **Log On...** to go to **Step 14**.

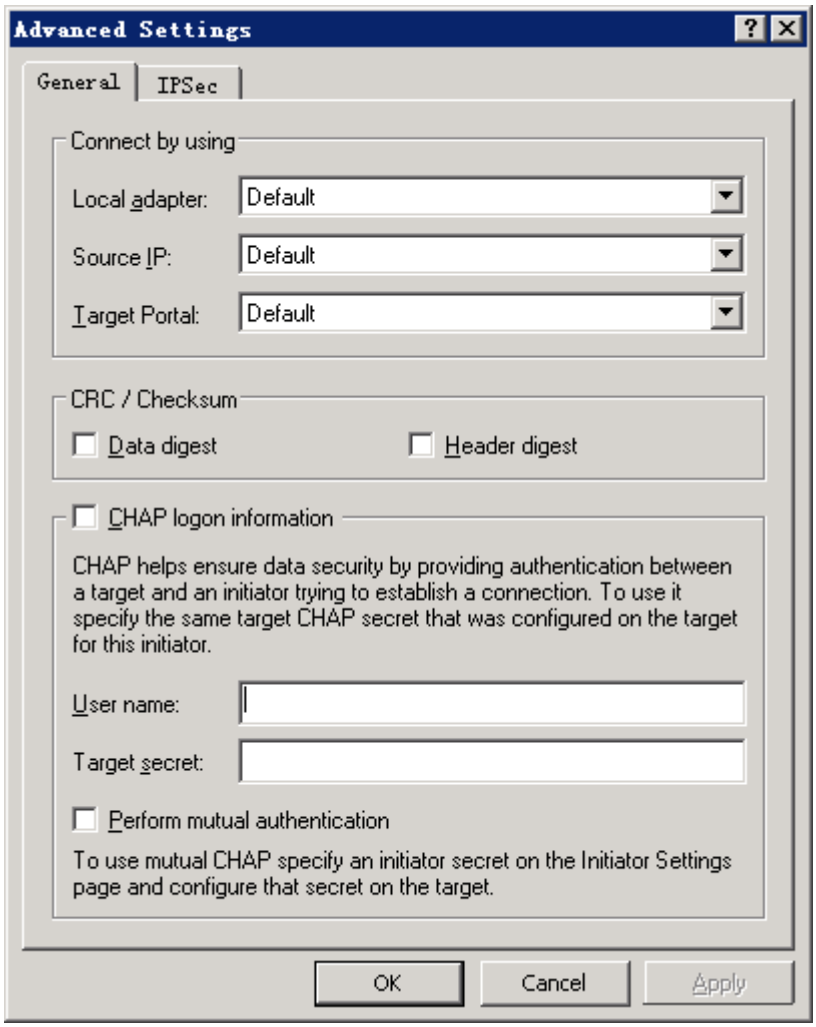
To enable CHAP user authentication, go to **Step 9**.

Step 9 Log in to the OceanStor ISM and enable CHAP user authentication. For details, see "**4.9.2 Enabling CHAP authentication**".

Step 10 Return to the **iSCSI Initiator Properties** dialog box of the AS.

Step 11 Click the **Targets** tab and click **Log On...**. The **Log On to Target** dialog box is displayed. Click **Advanced....** The **Advanced Settings** dialog box is displayed, as shown in **Figure 4-39**.

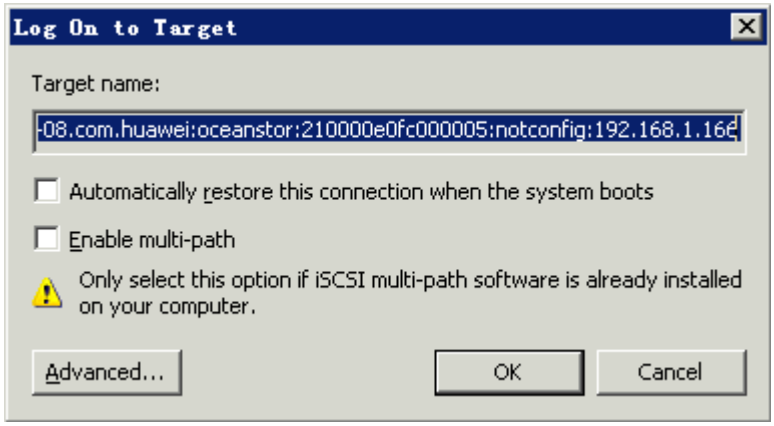
Figure 4-39 Advanced Settings dialog box



Step 12 Select **CHAP logon information**. In the **User name** text box and **Target secret text** text box, enter the CHAP user name and password allocated to the AS.

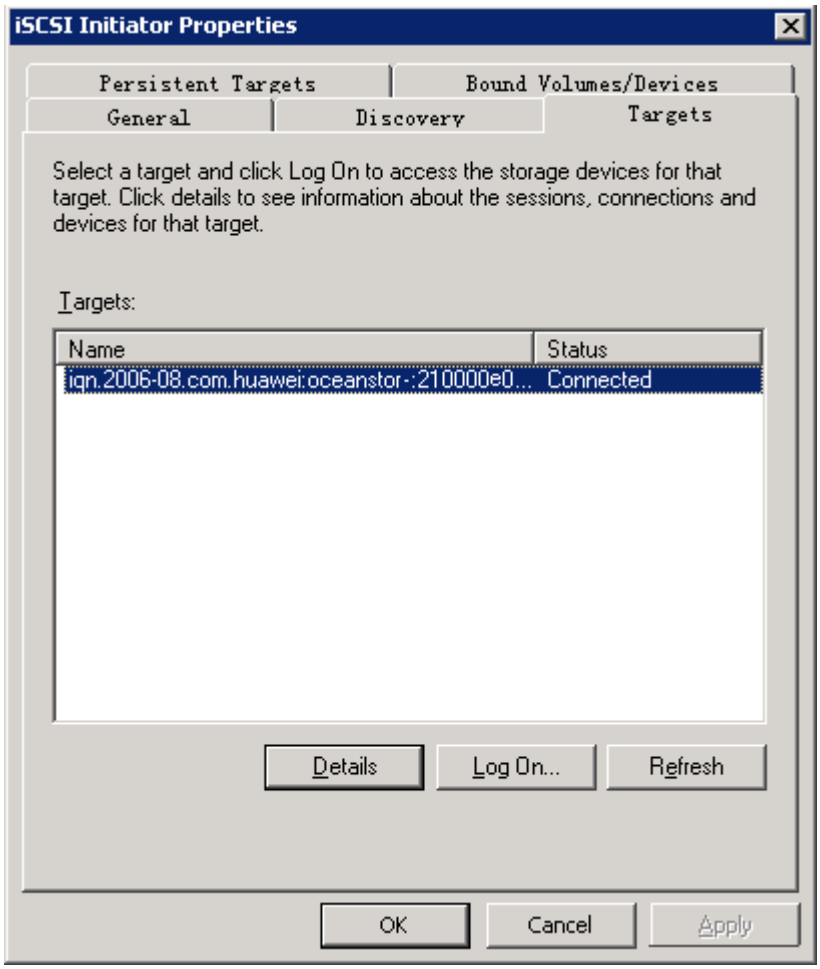
Step 13 Click **OK** to go back to the **Log On to Target** dialog box. See **Figure 4-40**.

Figure 4-40 Log On to Target dialog box



Step 14 Click **OK** to return to the **iSCSI Initiator Properties** dialog box. Click the **Targets** tab. Ensure that **Connected** is displayed in the **Status** column. See **Figure 4-41**.

Figure 4-41 Connection status of the target interface



----End

4.11 Adding an Initiator

An initiator is added to manage iSCSI host port. After the initiator is added, the AS can connect to the storage array through the iSCSI host port for data access.

Context

Ensure that there is an initiator available in the storage array.

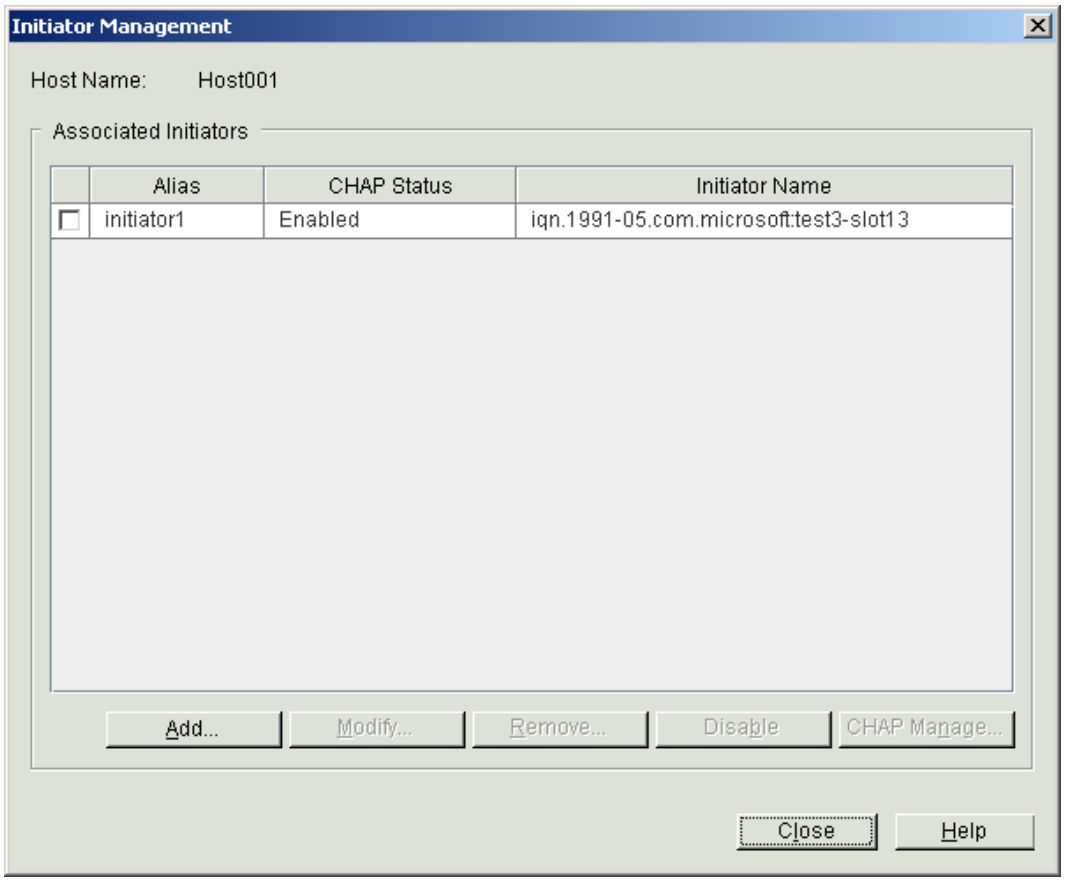
Procedure

Step 1 On the OceanStor ISM main interface, click the **Logical View** tab. In the navigation tree, click the host to which the initiator is to be added.

Step 2 On the menu bar, choose **Configuration** > **Host Initiator Management...**.

The **Initiator Management** interface is displayed, as shown in **Figure 4-42**.

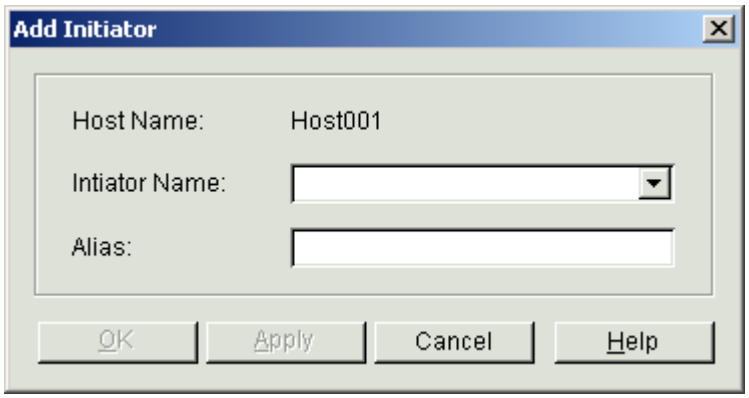
Figure 4-42 Initiator Management interface



Step 3 Click **Add...**.

The **Add Initiator** interface is displayed, as shown in **Figure 4-43**.

Figure 4-43 Add Initiator interface



Step 4 Set the initiator parameters.

Table 4-13 describes the parameters for an initiator.

Table 4-13 Parameters for an initiator

Parameter	Description
Initiator Name	This parameter indicates the name of the iSCSI initiator on the AS. **NOTE** In the **Initiator Name** drop-down list box, the initiator node names described in "**4.10 Setting Up the Connection from the AS to the Controller**" are displayed.
Alias	The parameter indicates the initiator name. When setting this parameter, note that: ● The initiator name must be unique. ● The value contains letters, digits, underscores, or hyphens only. ● The value contains a maximum of 32 characters.

Step 5 Click **OK**. The **Info** dialog box is displayed, stating "`Operation succeeded.`".

Step 6 Click **Cancel**.

----End

4.12 Adding a Mapping

Introduction to adding a mapping.

4.12.1 Mapping a LUN to a Host Group
Introduction to mapping a LUN to a host group.

4.12.2 Mapping a LUN to a Host
Introduction to mapping a LUN to a host.

4.12.1 Mapping a LUN to a Host Group

Introduction to mapping a LUN to a host group.

Context

- Before mapping a LUN to a host group, ensure that the LUN is not mapped to any host group or host.
- When you map a LUN to a host group, all the hosts in the host group can use the LUN.
- For the default host group of the system, you can map a LUN to the host group instead of any hosts in the default host group.

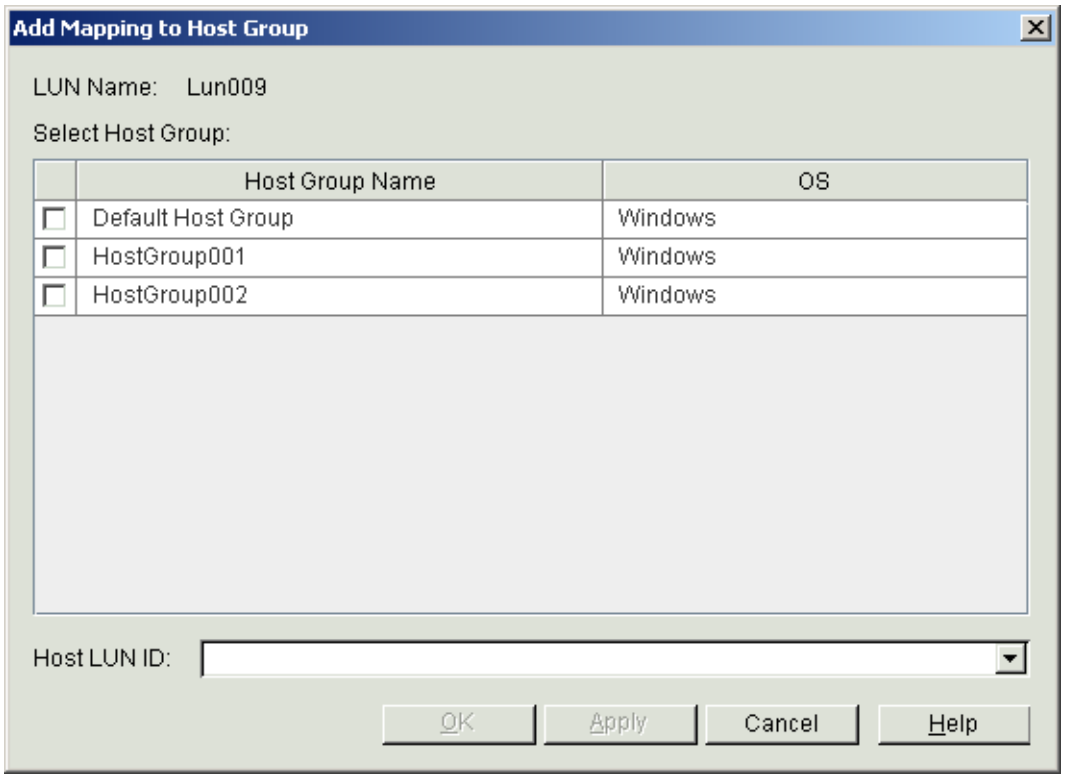
Procedure

Step 1 In the navigation tree, click the **Logical View** tab. Click the required LUN.

Step 2 On the menu bar, choose **Configuration** > **Add Mapping** > **To Host Group...**.

The **Add Mapping to Host Group** dialog box is displayed, as shown in **Figure 4-44**.

Figure 4-44 Add Mapping to Host Group dialog box



Step 3 Choose the host group to be mapped.

Step 4 In the **Host LUN ID** drop-down list box, choose a host LUN ID for the LUN to be mapped.

If you do not set a host LUN ID, the system uses a host LUN ID by default.

Step 5 Click **OK**. The **Info** dialog box is displayed, stating "`Operation succeeded.`".

Step 6 Click **OK**.

----End

4.12.2 Mapping a LUN to a Host

Introduction to mapping a LUN to a host.

Context

- Before mapping a LUN to a host, ensure that the LUN is not formatted to any host group or host.
- When you map a LUN to a host, only this host can use the LUN.

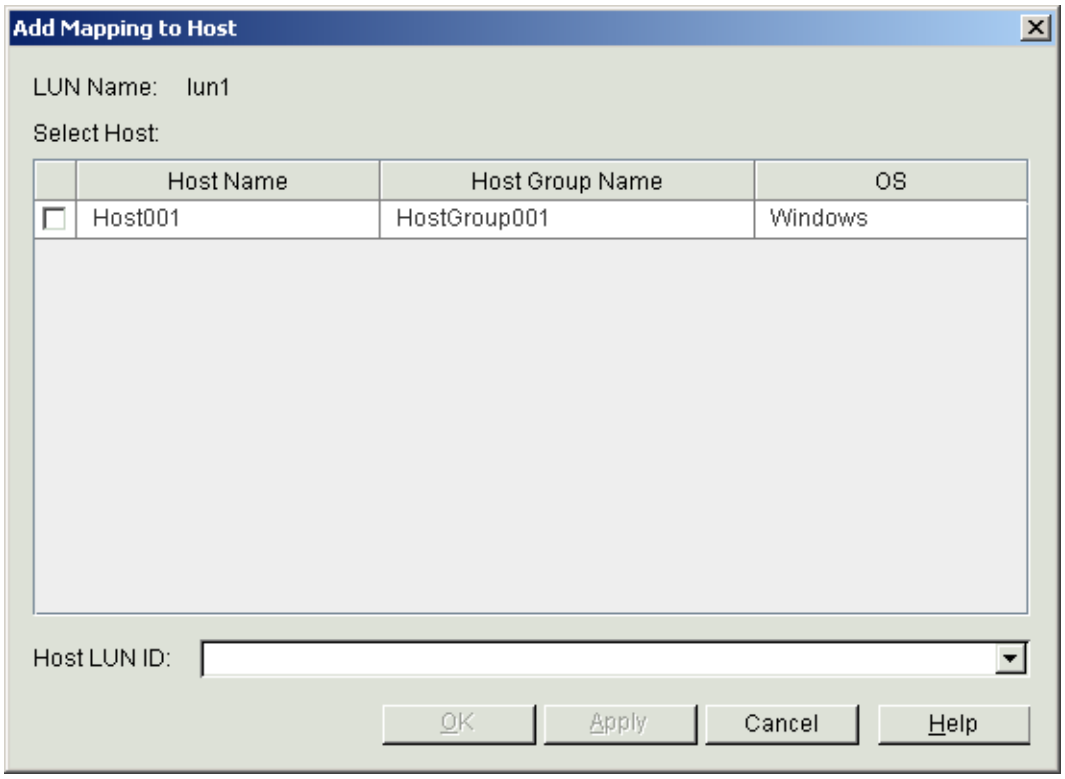
Procedure

Step 1 In the navigation tree, click the **Logical View** tab. Click the required LUN.

Step 2 On the menu bar, choose **Configuration** > **Add Mapping** > **To Host...**.

The **Add Mapping to Host** dialog box is displayed, as shown in **Figure 4-45**.

Figure 4-45 Add Mapping to Host dialog box



Step 3 Choose the host to be mapped.

Step 4 In the **Host LUN ID** drop-down list box, choose a host LUN ID for the LUN to be mapped.

If you do not set a host LUN ID, the system uses a host LUN ID by default.

Step 5 Click **OK**. The **Info** dialog box is displayed, stating "`Operation succeeded.`".

Step 6 Click **OK**.

----End

4.13 Adding an Interface

Introduction to adding a interface.

Context

Available FC or SAS interfaces are required for this operation.

The virtual host created on the OceanStor ISM can be mapped to the physical AS only after you add an interface to the host.

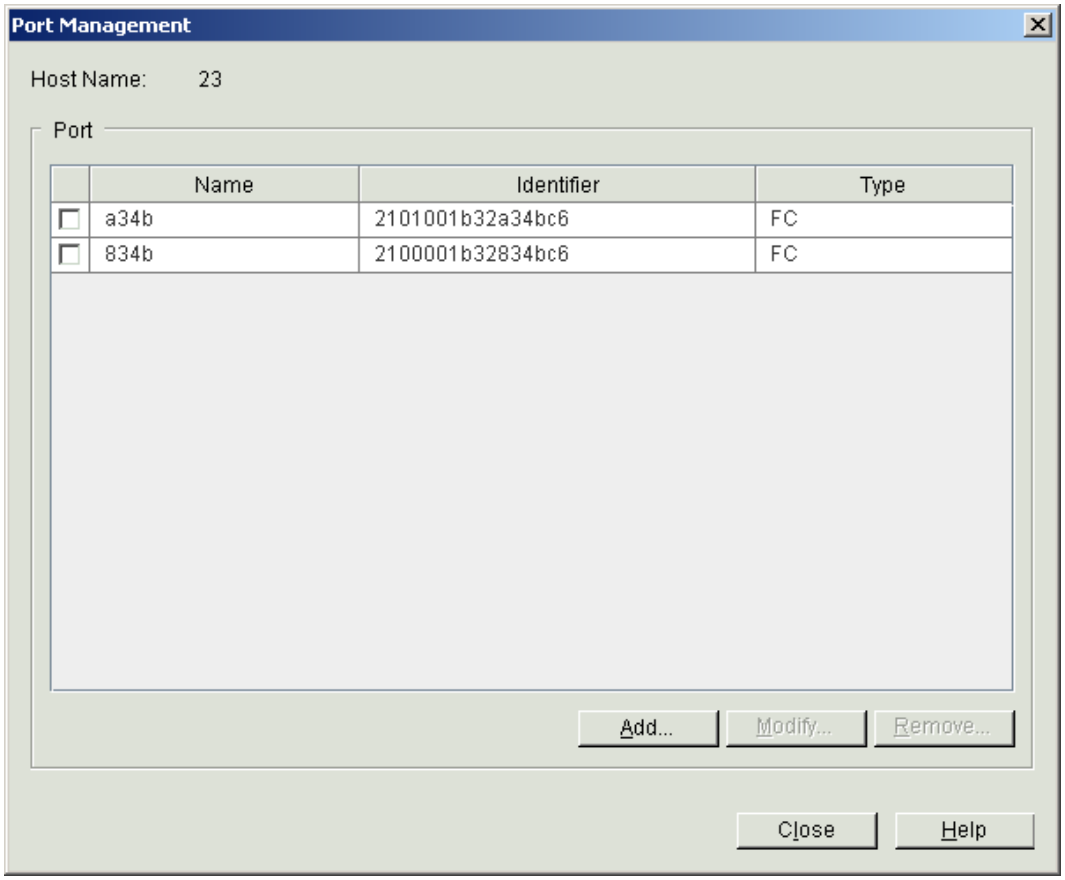
Procedure

Step 1 On the OceanStor ISM main interface, click the **Logical View** tab. In the navigation tree, click the host to which the interface is to be added.

Step 2 On the menu bar, choose **Configuration** > **Host Port Management...**.

The **Port Management** dialog box is displayed, as shown in **Figure 4-46**.

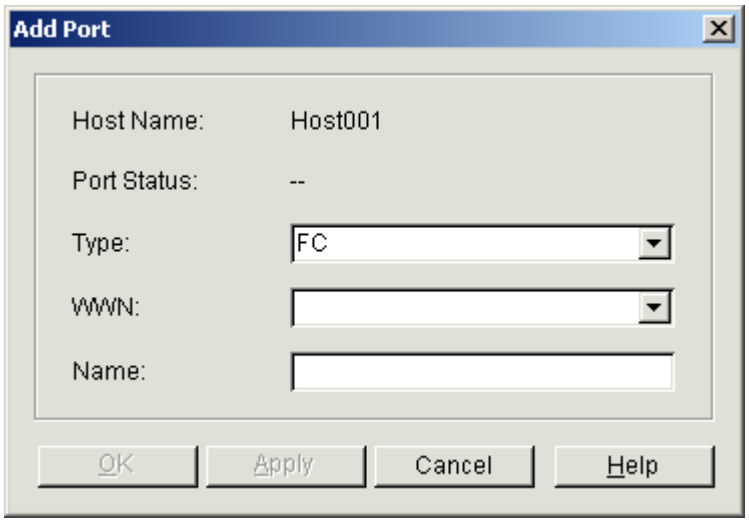
Figure 4-46 Port Management dialog box



Step 3 Click **Add...**.

The **Add Port** dialog box is displayed, as shown in **Figure 4-47**.

Figure 4-47 Add Port dialog box



Step 4 Set interface parameters.

Table 4-14 describes the parameters for the interface.

Table 4-14 Parameters for the interface

Parameter	Description
Type	This parameter indicates the type of the front-end host port. The value is **SAS**, **FC**.
WWN	The parameter indicates the information about an SAS or FC interface obtained from the host.
Name	This parameter indicates the interface name. When setting this parameter, note that: ● The interface name must be unique. ● The value contains letters, digits, underscores, or hyphens only. ● The value contains a maximum of 32 characters.

Step 5 Click **OK**. The **Info** dialog box is displayed, stating "`Operation succeeded.`".

Step 6 Click **OK**.

----End

4.14 Using a LUN on an AS

After mapping a device LUN to an AS, you must configure the LUN on the AS.

Context

The following section describes how to set a LUN on an AS in Windows.

Take the AS in Windows Server 2003 as an example.

NOTE

For an AS installed with other Windows OSs, perform the steps as required.

Procedure

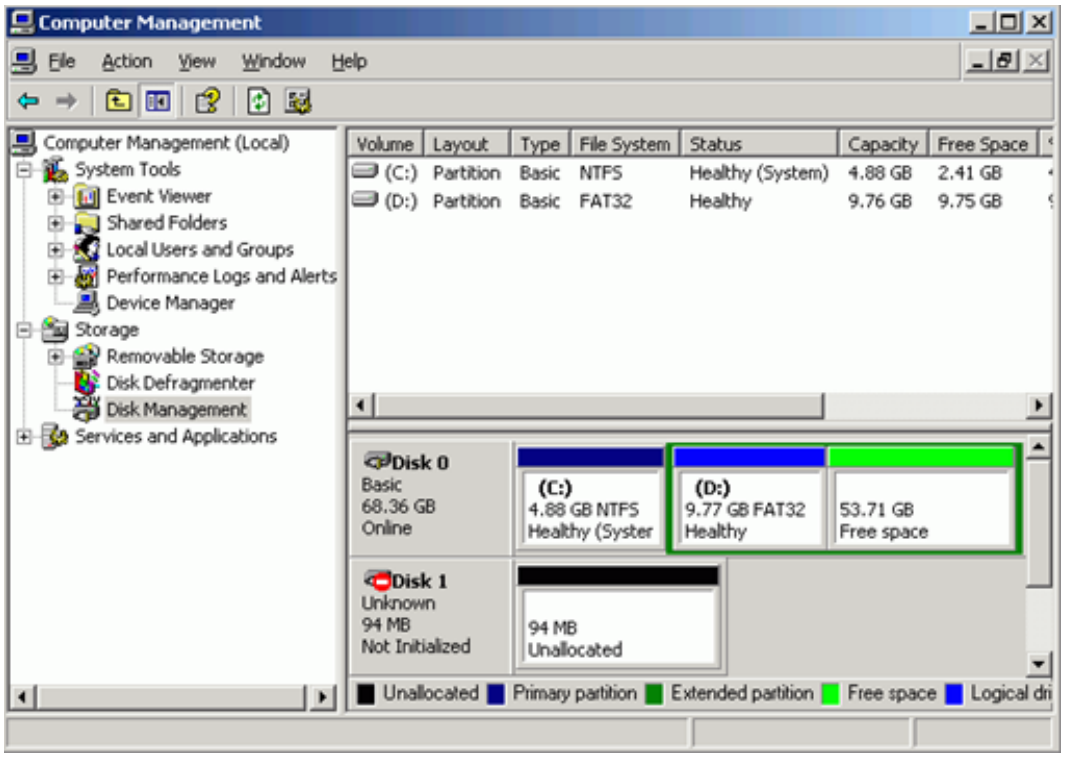
Step 1 Log in to the Windows AS as a user in the administrator group.

Step 2 Choose **Start** > **Control Panel** > **Administrative Tools** > **Computer Management**. The **Computer Management** window is displayed.

Step 3 In the navigation tree on the left, choose **StorageDisk Management** and right-click **Disk Management**. On the displayed shortcut menu, choose **Rescan Disks**. After the disk is scanned, the added logical disk (for example, Disk 1) is displayed on the right.

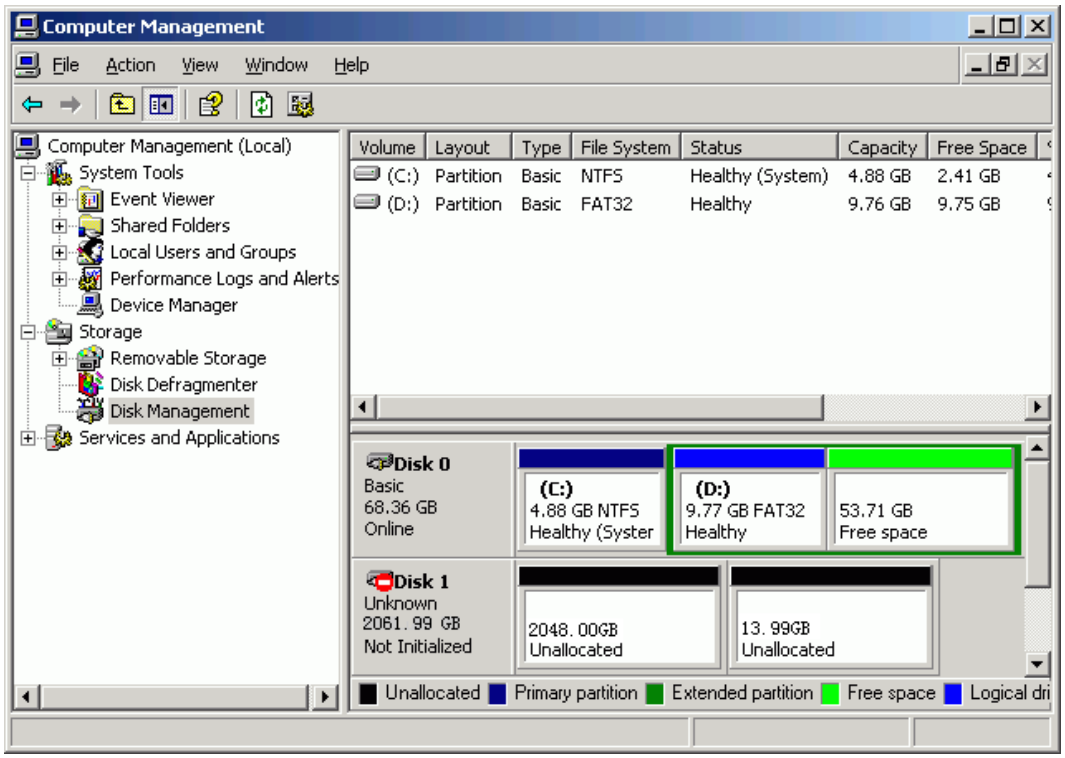
- **Figure 4-48** shows the situation that the disk capacity is not more than 2 TB.

Figure 4-48 Viewing the logical disks



- **Figure 4-49** shows the situation that the disk capacity is larger than 2 TB.

Figure 4-49 Viewing the logical disks



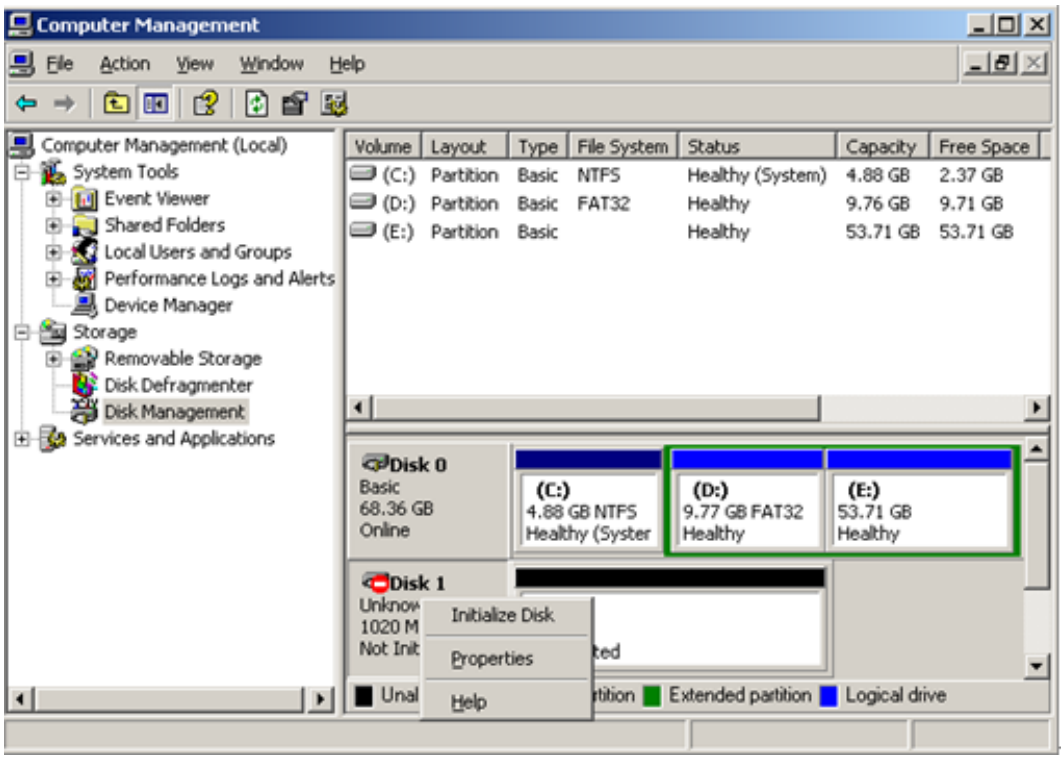
NOTE

If the logical disk is not displayed, choose **Device ManagerDisk drives**. Right-click **Disk drives** and choose **Scan for hardware changes** in the displayed shortcut menu. After scanning the disk, perform **Step 3**.

Step 4 Initialize the logical disks. Select **Disk 1** and right-click it.

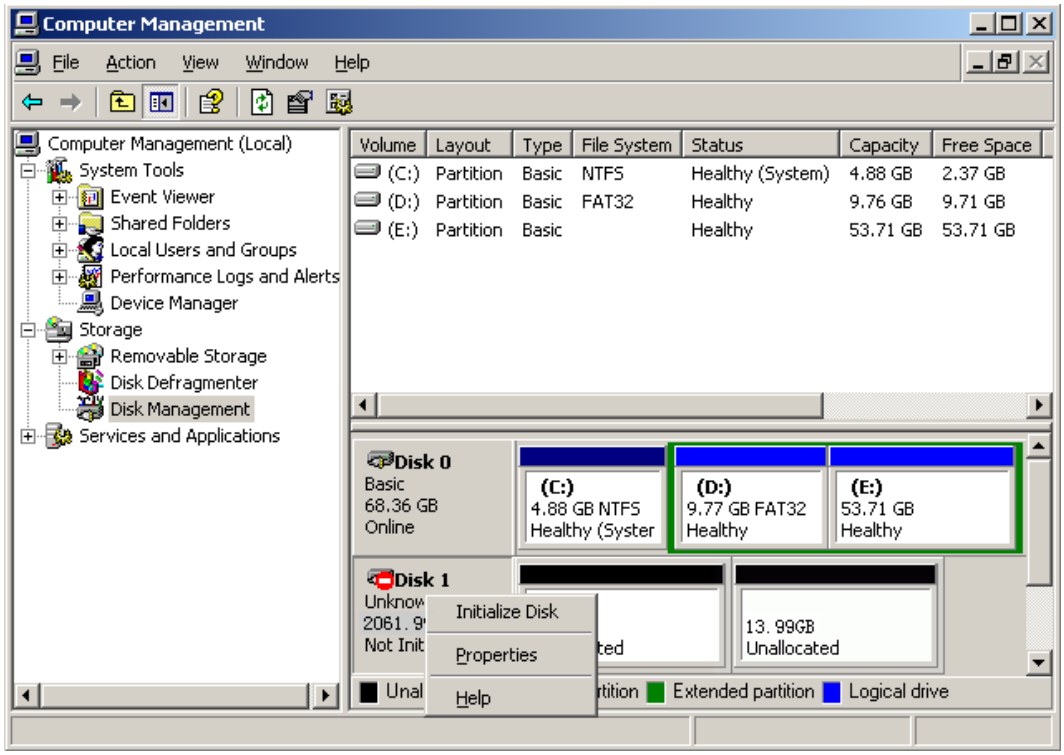
- **Figure 4-50** shows the situation that the disk capacity is not more than 2 TB.

Figure 4-50 Menu for initializing a disk



- **Figure 4-51** shows the situation that the disk capacity is larger than 2 TB.

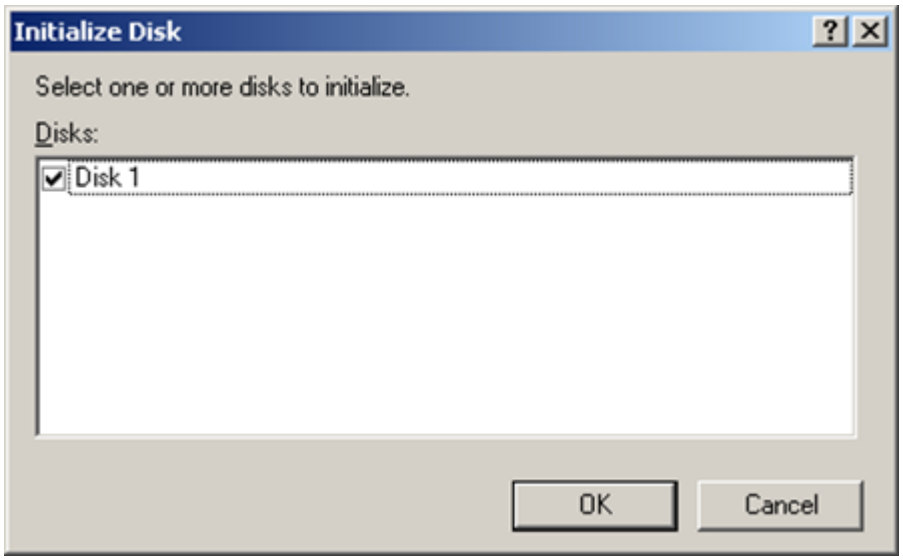
Figure 4-51 Menu for initializing a disk



Step 5 Click **Initialize Disk**.

The **Initialize Disk** interface is displayed, as shown in **Figure 4-52**.

Figure 4-52 Initialize Disk interface

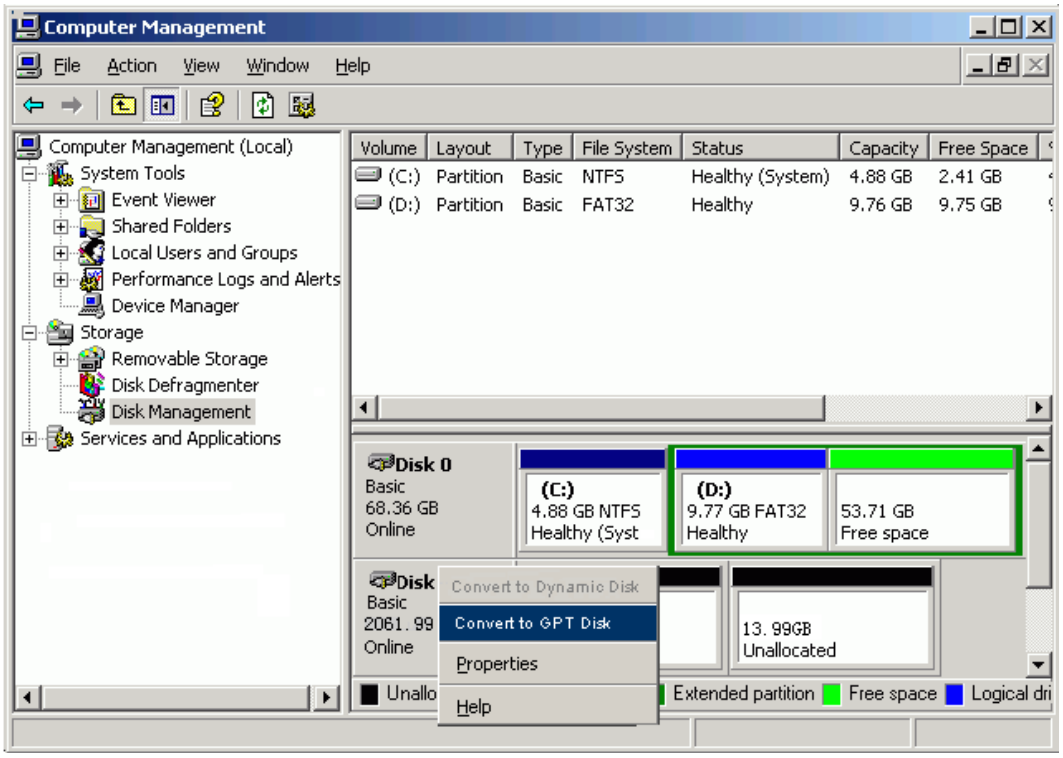


Step 6 Select **Disk 1**. Click **OK**.

- To initialize other logical disks, repeat **Step 4** to **Step 6**.
- If the disk capacity is not more than 2 TB, go to **Step 9**. If the disk capacity is larger than 2 TB, go to **Step 7**.

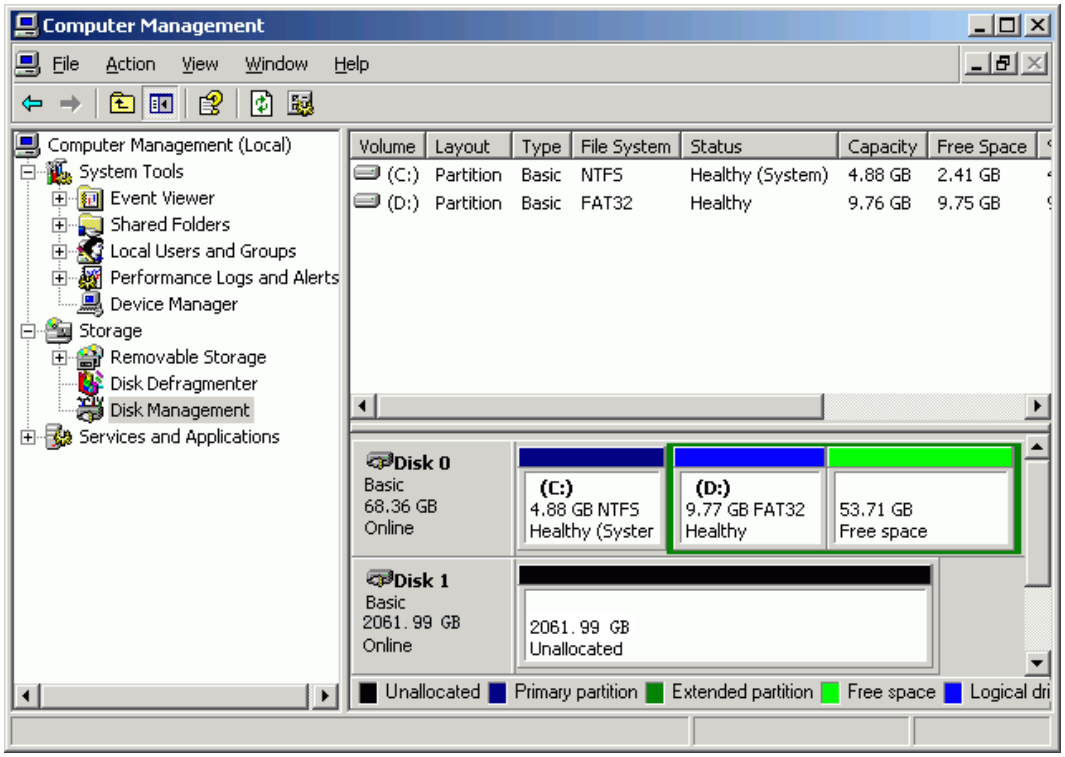
Step 7 Right click **Disk 1** to convert a normal disk to the GPT disk. See **Figure 4-53**.

Figure 4-53 Menu for convert to GPT disk



Step 8 Click Convert to GPT Disk. See **Figure 4-54**.

Figure 4-54 "Convert to GPT Disk" is finished



Step 9 Partition and format the disk.

----End

Result

Now, the S2600 can be used to access data.

5 Setting Additional Information

About This Chapter

This chapter describes how to set the system information and alarm information.

5.1 Setting the System Information

How to set basic information, synchronize time, perform primary/secondary switchover, lock, and unlock the system.

5.1.1 Setting Basic Information
Introduction to setting basic information.

5.1.2 Synchronizing Time
This section describes how to synchronize the time on the OceanStor ISM client to the arrays. If the time is not synchronized, the displayed time of related information is inconsistent, which might affect fault location.

5.1.3 Switching Over Primary and Secondary Controllers
If the storage array is configured with dual-controller, the operations such as system upgrade are relevant to the primary and secondary states of the controllers. The OceanStor ISM provides the function of primary/secondary switchover to facilitate routine configuration and maintenance.

5.1.4 Locking and Unlocking the System
Introduction to locking and unlocking the system.

5.1.1 Setting Basic Information

Introduction to setting basic information.

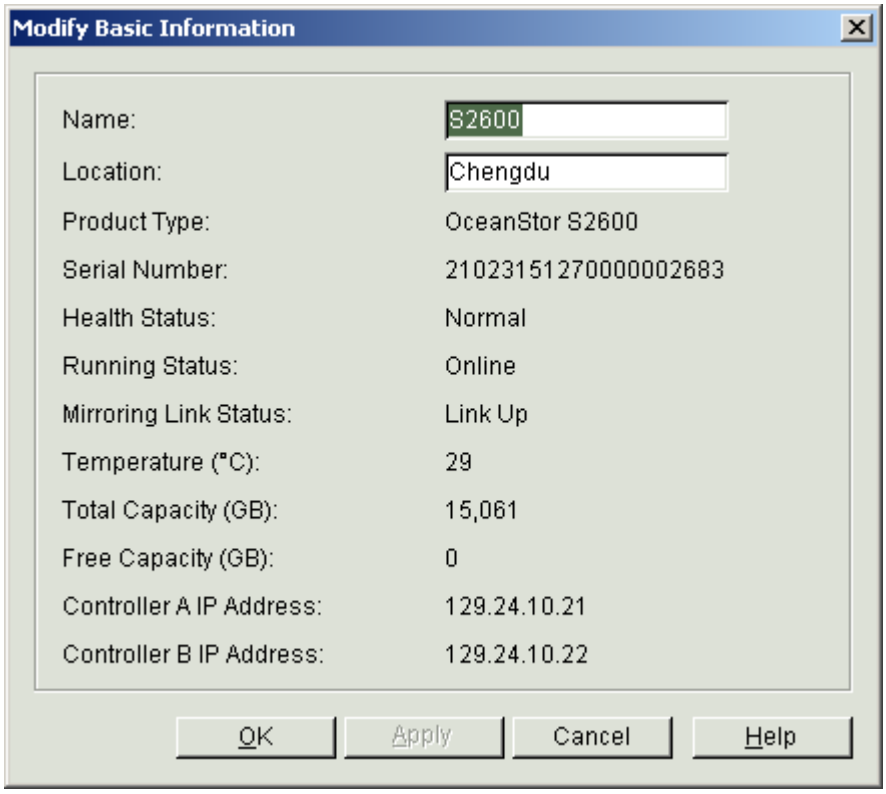
Procedure

Step 1 On the OceanStor ISM main interface, select the required storage array.

Step 2 On the menu bar, choose **Configuration** > **Modify Basic Information...**.

The **Modify Basic Information** interface is displayed, as shown in **Figure 5-1**.

Figure 5-1 Modify Basic Information interface



Step 3 Enter the array name and the location.

Step 4 Click **OK**. The **Info** dialog box is displayed, stating "`Operation succeeded.`".

Step 5 Click **OK**.

----End

5.1.2 Synchronizing Time

This section describes how to synchronize the time on the OceanStor ISM client to the arrays. If the time is not synchronized, the displayed time of related information is inconsistent, which might affect fault location.

Context

Synchronizing time might affect device services.

NOTE

To ensure that the synchronized time is valid, restart the OceanStor ISM after modifying the system time zone or the daylight saving time, and then perform time synchronization.

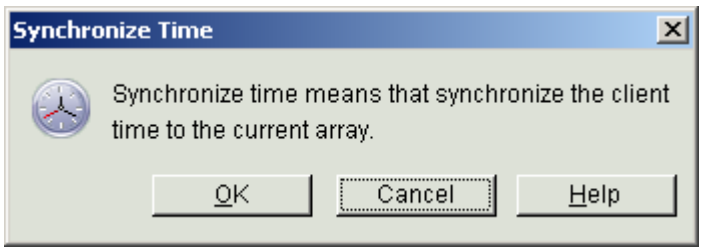
Procedure

Step 1 In the navigation tree of the OceanStor ISM main interface, select the required storage array.

Step 2 On the menu bar, choose **System** > **Synchronize Time**.

The **Synchronize Time** dialog box is displayed, as shown in **Figure 5-2**.

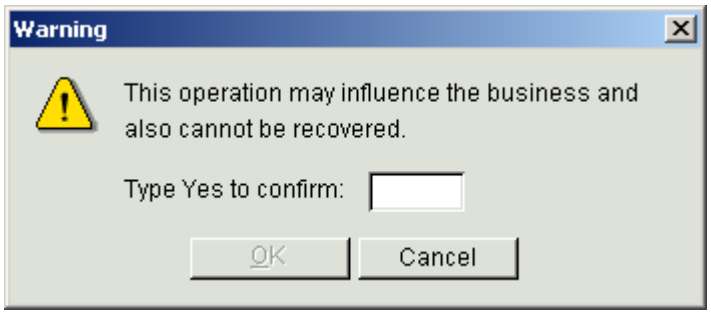
Figure 5-2 Synchronize Time dialog box



Step 3 Click **OK**.

The **Warning** dialog box is displayed, as shown in **Figure 5-3**.

Figure 5-3 Warning dialog box



Step 4 In the text box, enter **Yes**.

Step 5 Click **OK**. The **Info** dialog box is displayed, stating "`Operation succeeded.`".

Step 6 Click **OK**.

----End

5.1.3 Switching Over Primary and Secondary Controllers

If the storage array is configured with dual-controller, the operations such as system upgrade are relevant to the primary and secondary states of the controllers. The OceanStor ISM provides the function of primary/secondary switchover to facilitate routine configuration and maintenance.

Context

CAUTION

You cannot switch over primary and secondary controllers on a single-controller storage array.

When you perform primary/secondary switchover, notice that:

- You can switch over the primary and secondary controllers only when two controllers are running properly in the system.
- The switchover may affect the response speed of the S2600.
- The interval between two consecutive primary/secondary switchover operations is at least ten seconds.
- Guests cannot perform this operation.

CAUTION

During the switchover, other users can log in to the OceanStor ISM but cannot operate on it.

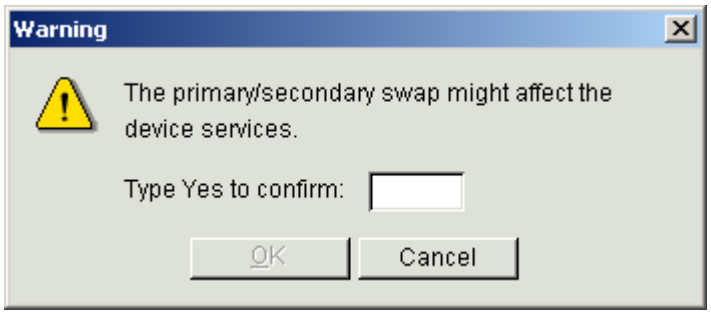
Procedure

Step 1 In the navigation tree of the OceanStor ISM main interface, select the required storage array.

Step 2 On the menu bar, choose **Configuration** > **Primary/Secondary Swap...**.

The **Warning** dialog box is displayed, as shown in **Figure 5-4**.

Figure 5-4 Warning dialog box



Step 3 Enter **Yes** in the text box.

Step 4 Click **OK**. After the switchover, the **Info** dialog box is displayed, stating "`Operation succeeded.`".

Step 5 Click **OK**.

----End

5.1.4 Locking and Unlocking the System

Introduction to locking and unlocking the system.

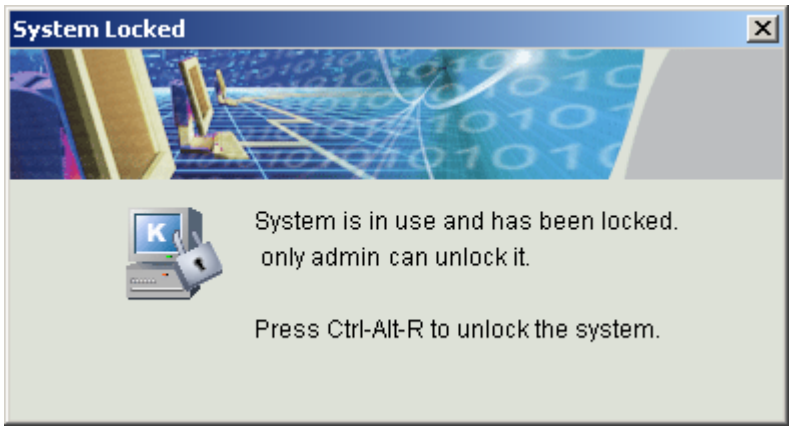
NOTE

- If you do not use the OceanStor ISM to manage the storage system for a long time, you can lock the system through the OceanStor ISM to prevent others against operating the system.
- If you log in to the OceanStor ISM and perform no operations within 10 minutes, the system locks automatically.

Locking the System

On the menu bar of the OceanStor ISM main interface, choose **System** > **Lock**. The **System Locked** interface is displayed. See **Figure 5-5**.

Figure 5-5 System Locked interface

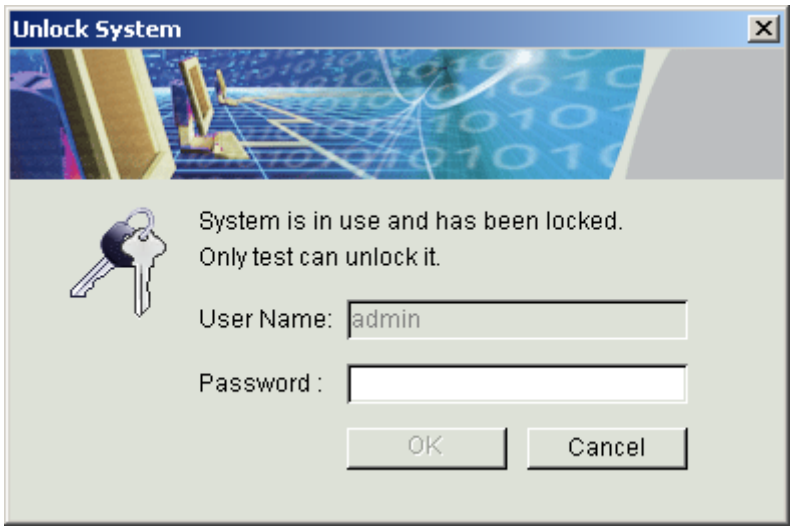


Unlocking the System

After the System Locked interface is displayed, if you want to log in to the OceanStor ISM interface, you need to unlock the system first.

1. On the interface as shown in **Figure 5-5**, press **Ctrl+Alt+R**. The **Release System Lock** dialog box is displayed, as shown in **Figure 5-6**.

Figure 5-6 Release System Lock dialog box



2. Enter the password and click **OK**. The OceanStor ISM interface is displayed.

5.2 Managing Alarms

Introduction to managing alarms.

5.2.1 Filtering Current Alarms
Though filtering current alarms, you can query the alarms conveniently. The system displays alarms that only meet the filtering conditions.

5.2.2 Filtering History Alarms
Though filtering history alarms, you can query the alarms conveniently. The system displays alarms that only meet the filtering conditions.

5.2.3 Blocking Current Alarms
You can make configurations to block unnecessary alarms. After configuration, the alarms meeting blocking conditions cannot be sent to the OceanStor ISM.

5.2.4 Clearing Current Alarms
Through this function, you can transfer current selected alarms to history alarms.

5.2.1 Filtering Current Alarms

Though filtering current alarms, you can query the alarms conveniently. The system displays alarms that only meet the filtering conditions.

Procedure

Step 1 In the navigation tree, select **All Arrays** or select the S2600 or component of the S2600.

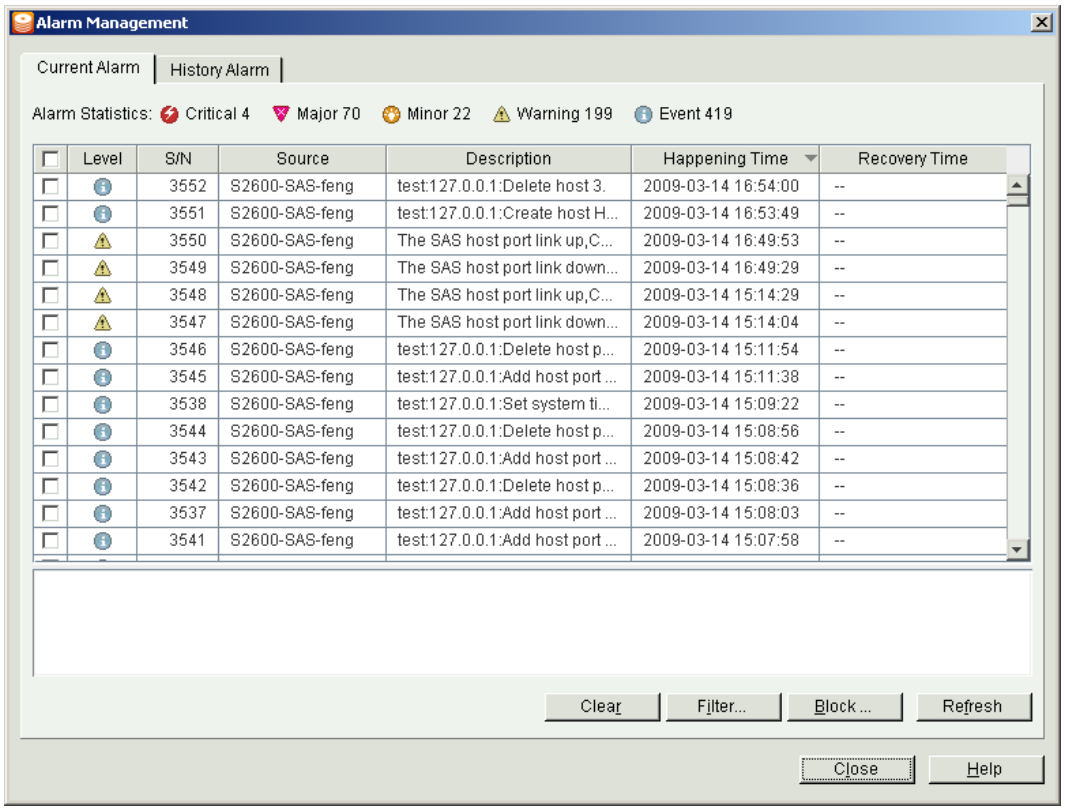
Step 2 On the menu bar, choose **Alarm** > **Alarm Management...**.

The **Alarm Management** interface is displayed.

Step 3 Click **Current Alarm**.

The **Current Alarm** interface is displayed. See **Figure 5-7**.

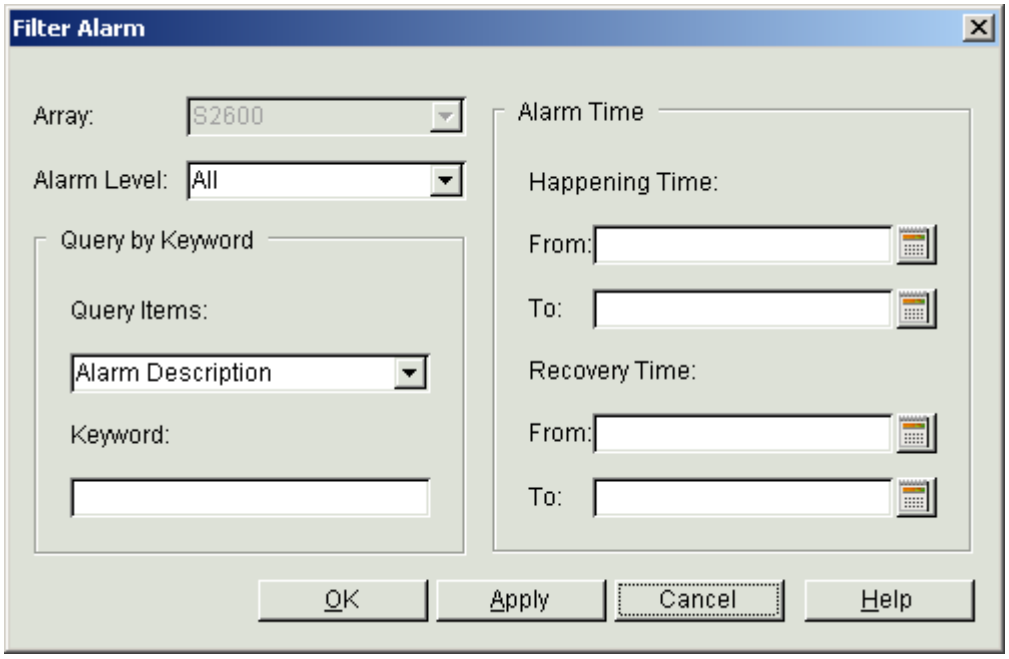
Figure 5-7 Alarm Management interface



Step 4 Click **Filter...**.

The **Filter Alarm** dialog box is displayed. See **Figure 5-8**.

Figure 5-8 Filter Alarm interface



Step 5 Set the conditions of querying alarms.

Table 5-1 describes the parameters for filtering current alarms.

Table 5-1 Parameters for filtering current alarms

Parameter	Description
Array	The parameter indicates the array that alarms belong to.
Alarm Level	The parameter indicates the severity of the alarm to be queried. The value is **Critical**, **Major**, **Minor**, **Warning**, **Event**, or **All**.
Query Items	The parameter indicates the information based on which alarms are to be queried. The value is **Alarm Description** or **Alarm Source**.
Keyword	The parameter indicates the information about the alarm to be queried. For example, the disk fails.
Happening Time	The parameter indicates selected the time range. You can query the alarms generated during this range. Click the icon after **From** and **To**. In the displayed **Select Data and Time** dialog box, choose the start time and end time of alarm happening time (the end time cannot be earlier than the start time). Then click **OK**.

Parameter	Description
Recovery Time	The parameter indicates selected the time range. You can query the alarms recovered during this range. Click the icon after **From** and **To**. In the displayed **Select Data and Time** dialog box, choose the start time and end time of alarm happening time (the end time cannot be earlier than the start time). Then click **OK**.

Step 6 Click **OK**.

----End

5.2.2 Filtering History Alarms

Though filtering history alarms, you can query the alarms conveniently. The system displays alarms that only meet the filtering conditions.

Procedure

Step 1 In the navigation tree, select **All Arrays** or select the S2600 or the component of the S2600.

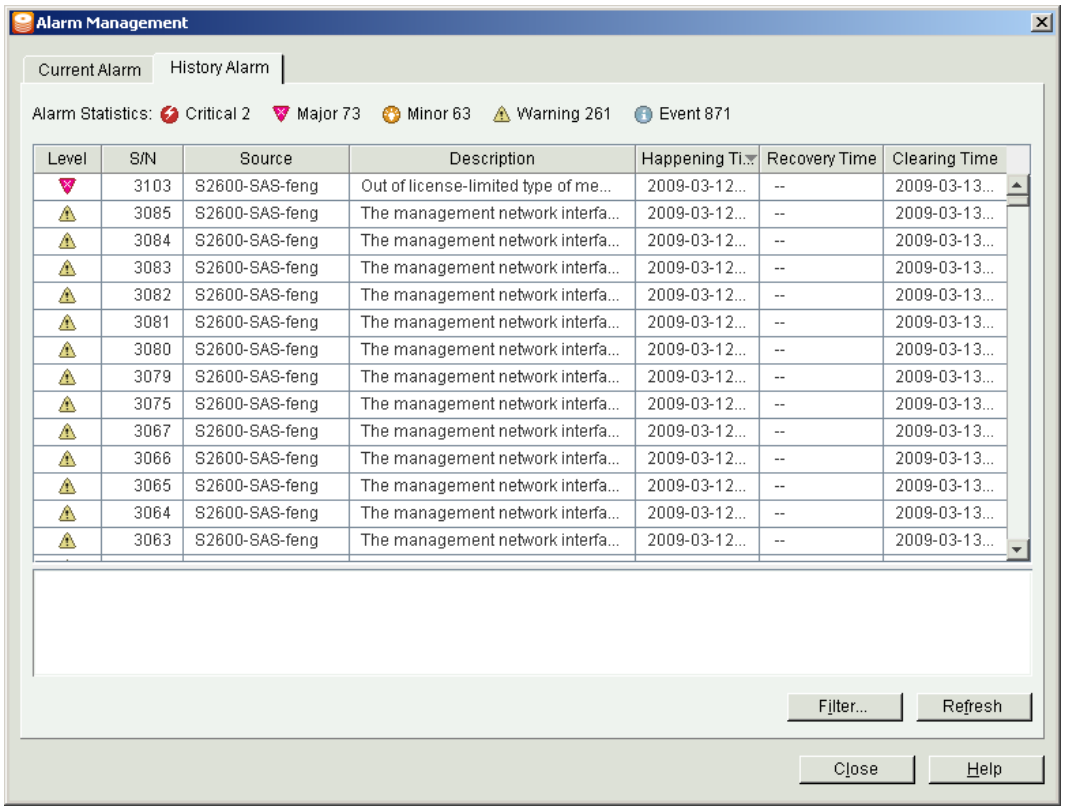
Step 2 On the menu bar, choose **Alarm** > **Alarm Management...**.

The **Alarm Management** interface is displayed.

Step 3 Click the **History Alarm** tab.

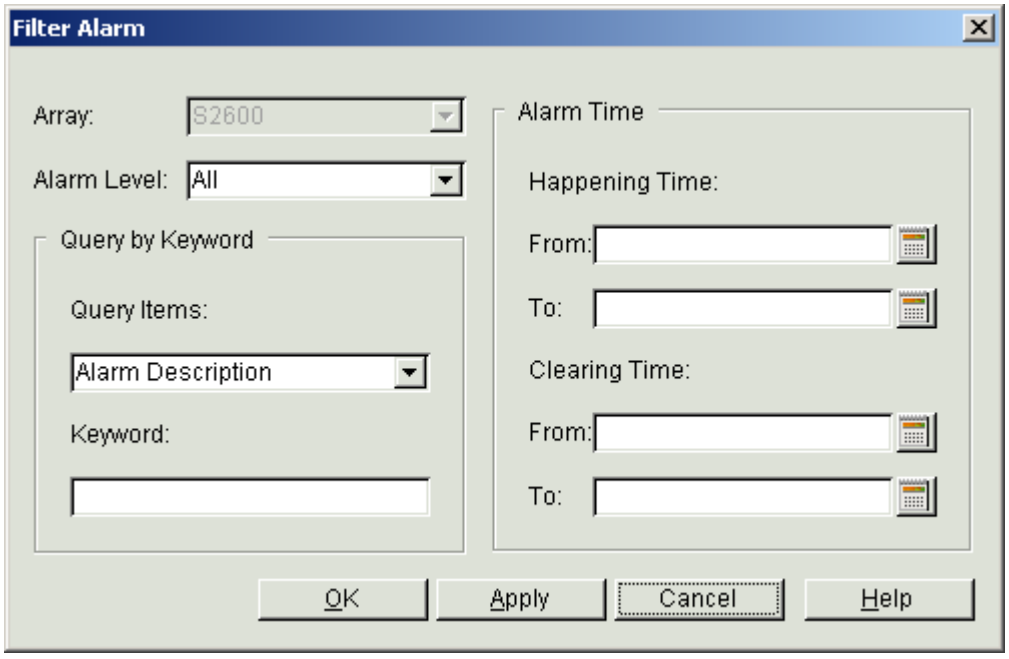
The Alarm Management interface is displayed. See **Figure 5-9**.

Figure 5-9 Alarm Management interface



Step 4 Click **Filter...**. The **Filter Alarm** dialog box is displayed. See **Figure 5-10**.

Figure 5-10 Filter Alarm dialog box



Step 5 Set the conditions of querying alarms.

Table 5-2 lists the parameters related to querying alarms.

Table 5-2 Parameter description for filtering history alarms

Parameter	Description
Array	The parameter indicates the array that alarms belong to.
Alarm Level	The parameter indicates the alarm severity that is to be queried. The value could be **Critical**, **Major**, **Minor**, **Warning**, **Event**, or **All**.
Query Items	The parameter indicates the information based on which alarms are to be queried. The value is **Alarm Description** or **Alarm Source**.
Keyword	The parameter indicates the keyword of the information about the alarm to be queried.
Happening Time	The parameter indicates selected the time range. You can query the alarms generated during this range. Click the icon after **From** and **To**. In the displayed **Select Data and Time** dialog box, choose the start time and end time of alarm happening time (the end time cannot be earlier than the start time). Then click **OK**.

Parameter	Description
Clearing Time	The parameter indicates selected the time range. You can query the alarms filtered during this range. Click the icon after **From** and **To**. In the displayed **Select Data and Time** dialog box, choose the start time and end time of alarm happening time (the end time cannot be earlier than the start time). Then click **OK**.

Step 6 Click **OK**.

----End

5.2.3 Blocking Current Alarms

You can make configurations to block unnecessary alarms. After configuration, the alarms meeting blocking conditions cannot be sent to the OceanStor ISM.

Procedure

Step 1 In the navigation, select **All Arrays** or select the S2600 or the component of the S2600.

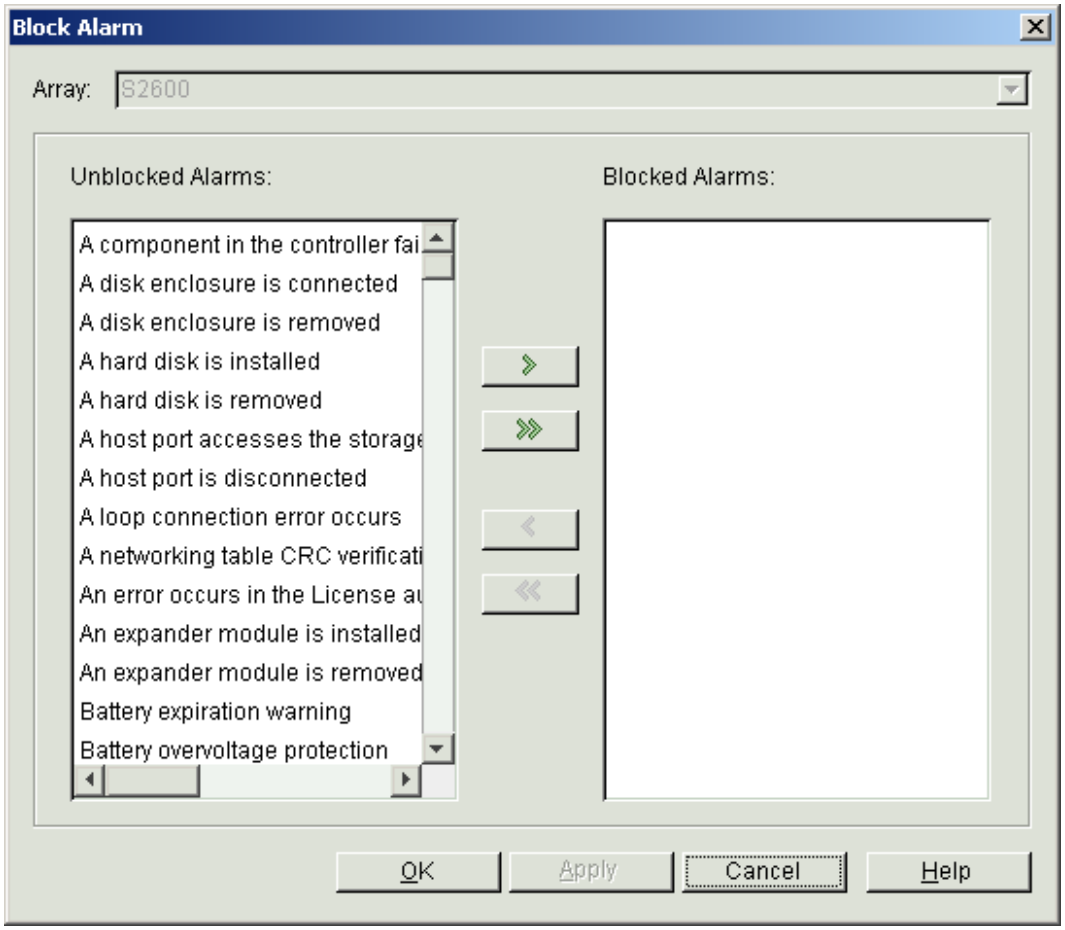
Step 2 On the menu bar, choose **Alarm** > **Alarm Management...**.

The **Alarm Management** interface is displayed, as shown in **Figure 5-7**.

Step 3 Click **Block...**.

The **Block Alarm** interface is displayed, as shown in **Figure 5-11**.

Figure 5-11 Block Alarm interface



Step 4 In the **Unblocked Alarms** list box, choose the alarms to be blocked and then click ›. These alarms are moved to the **Blocked Alarms** list box. You can also click » to move all the alarms in the **Unblock Alarms** list box to the **Blocked Alarms** list box.

NOTE

In the **Blocked Alarms** list box, choose the alarms to be unblocked and then click ‹. These alarms are moved to the **Unblocked Alarms** list box. You can also click « to move all the alarms in the **Blocked Alarms** list box to the **Unblocked Alarms** list box.

Step 5 Click **OK**.

The Info dialog box is displayed, saying "`Operation succeeded.`".

Step 6 Click **OK**.

----End

5.2.4 Clearing Current Alarms

Through this function, you can transfer current selected alarms to history alarms.

Procedure

Step 1 In the navigation tree, select **All Arrays** or select the S2600 or the component of the S2600.

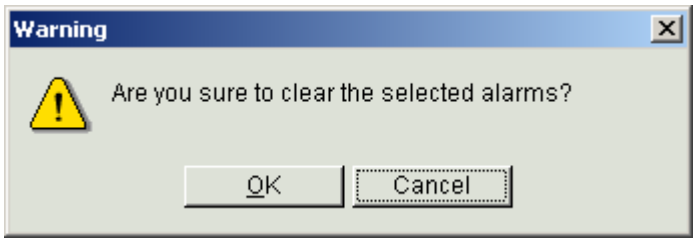
Step 2 On the menu bar, choose **Alarm** > **Alarm Management...**. The **Current Alarm** interface is displayed, as shown in **Figure 5-7**.

Step 3 Select the alarms.

Step 4 Click **Clear**.

The **Warning** dialog box is displayed. See **Figure 5-12**.

Figure 5-12 Warning dialog box



Step 5 Click **OK**. The **Info** dialog box is displayed, saying "`Operation succeeded.`".

Step 6 Click **OK**.

----End

5.3 Creating a Trap IP

This topic describes how to create a Trap IP.

Context

The S2600 supports alarm messages over Simple Network Management Protocol (SNMP). By creating a Trap IP, Trap alarms can be sent to the network management system. The Trap alarms can be saved for ever even in the case of power failure.

CAUTION

- A system can create two Trap IPs.
- If the Trap IPs are not in the subnet of the management segment, you can set the controller route information to send Trap alarms. For details, see the *OceanStor S2600 Storage System User Guide*.

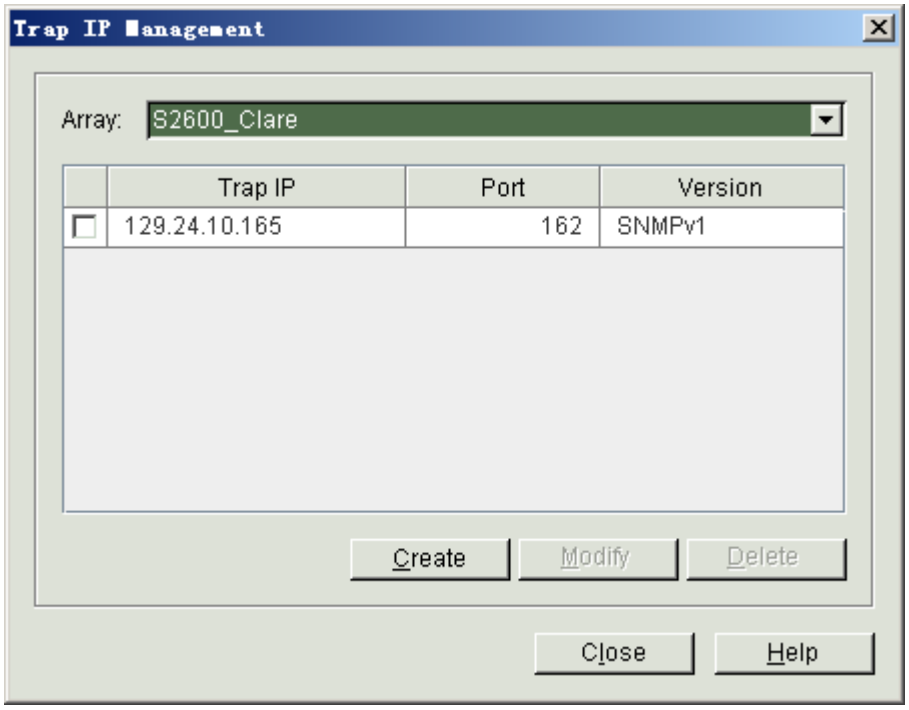
Procedure

Step 1 In the navigation tree, click the **Physical View** tab, and choose the storage array whose Trap IP is to be created.

Step 2 On the menu bar, choose **Configuration** > **Trap IP Management...**.

The **Trap IP Management** dialog box is displayed as shown in **Figure 5-13**.

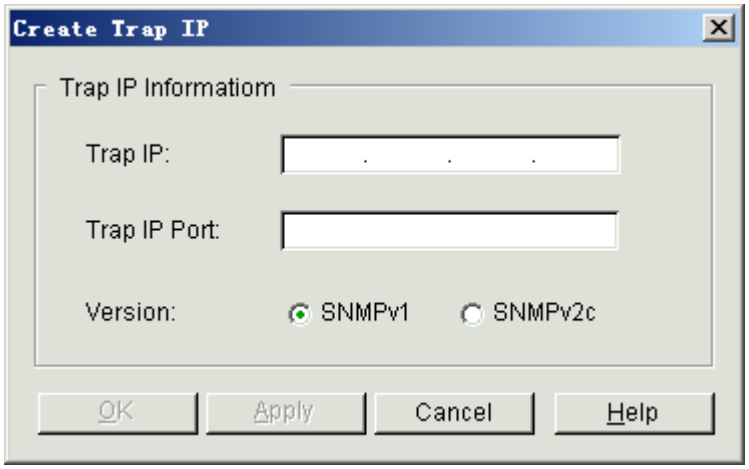
Figure 5-13 Trap IP Management dialog box



Step 3 Click **Create**.

The **Create Trap IP** dialog box is displayed as shown in **Figure 5-14**.

Figure 5-14 Create Trap IP dialog box



Step 4 Enter the Trap IP information.

Table 5-3 lists the parameters for creating a Trap IP.

Table 5-3 Parameters for creating a Trap IP

Parameter	Description
Trap IP	This parameter indicates the address of the Trap IP to be created. When setting the Trap IP address, note the following: ● Each field in the IP address cannot be empty and can only be an integer. ● The value of the first field on the left ranges from 1 to 223 (excluding 127), and the value of the last field ranges from 1 to 254. The value of any other field ranges from 0 to 255.
Trap IP Port	This parameter indicates the port of the Trap IP to be created. When setting the Trap IP port, note the following: ● The port value cannot be empty and must be an integer. ● The value must range from 1 to 65535.
Version	This parameter indicates the information the Trap IP version. The value is **SNMPv1** or **SNMPv2c**.

Step 5 Click **OK**.

The **Info** dialog box is displayed, stating **Operation succeeded.**.

Step 6 Click **OK**.

----End

5.4 Monitoring Settings

Introduction to monitoring settings.

5.4.1 Notification by Emails

Introduction to notification by emails.

Context

You can set whether to send an alarm notification by email, and set the IP address of the Simple Mail Transfer Protocol (SMTP) server, email address of the sender, severity of alarms, and email addresses of receivers.

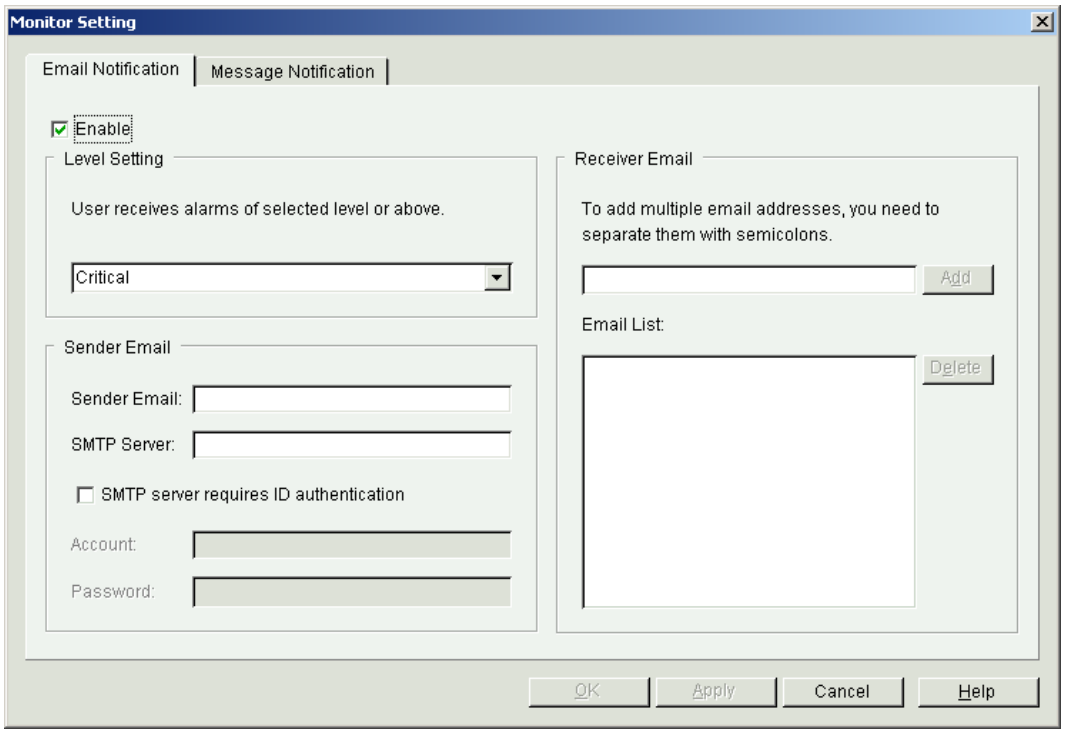
Procedure

Step 1 In the navigation tree of the OceanStor ISM main interface, click the storage array or storage array component on which the alarm notification is to be set.

Step 2 On the menu bar, choose **Alarm** > **Monitor Setting...**.

The **Monitor Setting** interface is displayed, as shown in **Figure 5-15**.

Figure 5-15 Monitor Setting interface



Step 3 Select **Enable**.

Step 4 Set the parameters for email notification.

Table 5-4 describes the parameters for email notification.

Table 5-4 Parameters for email notification

Parameter	Description
Level Setting	The parameter indicates the alarm severity. The alarms whose severity is the same as and above the set value are sent. The value is **Critical**, **Major**, **Minor**, or **Warning**. When you select one severity, users receive alarms with the selected severity and above. For example, if Major is selected, users receive alarms with the severity Critical and Major.
Sender Email	The parameter indicates the sender email address.

Parameter	Description
SMTP Server	The parameter indicates the IP address of the SMTP server.
Account	The parameter indicates the SMTP user account of the sender. The parameter is available only when you select **SMTP server requires ID authentication**.
Password	The parameter indicates the SMTP user password of the sender. The parameter is available only when you select **SMTP server requires ID authentication**.
Receiver Email	The parameter indicates the sender email address. You can enter a maximum of five email addresses at once and separate them with semicolons.
Email List	You can click **Add** to add receiver email addresses to **Email List**. In **Email List**, choose an email address and then click **Delete**. The email address is deleted from **Email List**.

Step 5 Click **OK**. The **Info** dialog box is displayed, stating "`Operation succeeded.`".

Step 6 Click **OK**.

----End

5.4.2 Notification by Messages

When setting message notification, you can set whether to send an alarm notification by messages, to send the message service number and receiver number.

Procedure

Step 1 In the navigation tree of the OceanStor ISM main interface, click the storage array or storage array component on which the alarm notification is to be set.

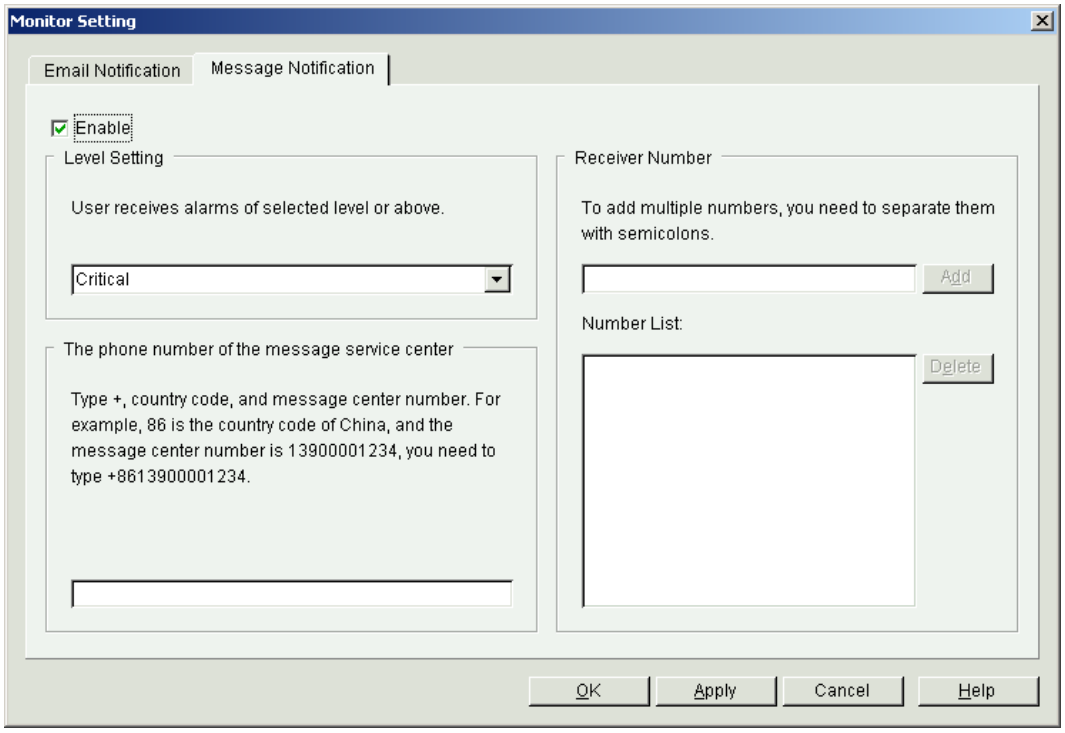
Step 2 On the menu bar, choose **Alarm** > **Monitor Setting...**.

The **Monitor Setting** interface is displayed, as shown in **Figure 5-15**.

Step 3 Click the **Message Notification** tab and select **Enable**.

The **Monitor Setting** interface is displayed. See **Figure 5-16**.

Figure 5-16 Monitor Setting interface



Step 4 Select **Enable**.

Step 5 Set the parameters for message notification.

Table 5-5 describes the parameters for message notification.

Table 5-5 Parameters for message notification

Parameter	Description
Level Setting	The alarms whose severity is the same as and above the set value are sent. The value is **Critical**, **Major**, **Minor**, or **Warning**. After you specify the alarm severity, you can receive all alarms that are of the specified severity and above. For example, if you select **Major**, you can receive alarms of **Critical**, and **Major**.
The phone number of the message service center	The parameter indicates the message service number. The number ranges from 0 to 9. You must add the plus sign "+" and the country code before the number, for example, **+8613000000000**.
Receiver Number	The parameter indicates the numbers for receiving alarm messages. You can enter a maximum of 10 mobile phone numbers at once and separate them with semicolons.

Parameter	Description
Number List	Click **Add** to add a mobile phone number to **Number List**. In **Number List**, choose a mobile phone number and then click **Delete**. The mobile phone number is deleted from **Number List**.

Step 6 Click **OK**. The **Info** dialog box is displayed, stating "`Operation succeeded.`".

Step 7 Click **OK**.

----End

A How to Obtain Help

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

A.1 Preparations For Contacting Huawei

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

A.1.1 Collecting Troubleshooting Information

You need to collect troubleshooting information before troubleshoot.

You need to collect the following information:

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

A.1.2 Making Debugging Preparations

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

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

A.2 How to Use the Document

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

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

A.3 How to Obtain Help from Website

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

Contents of the Huawei technical support system are as follows:

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

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

A.4 Ways to Contact Huawei

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

Huawei Technologies Co., Ltd.

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

Website: http://www.huawei.com

Telephone number: 86-755-28780808

Customer Service Center

Phone: 86-755-28560000; 4008302118

Huawei Service fax: 86-755-28560111

Service E-mail: support@huawei.com

B Glossary

A

Active network port	The service port that is working currently on the AS.
Active/Active Mode	The I/O operation can be performed on either of the two controllers.
Alarm buzzer	A component of the controller subrack. When a critical fault occurs in the OceanStor storage system, the alarm buzzer can generate some buzz.
Application server	The computer system that is connected to the storage system, stores data, and implements I/O access.
Application server LUN	The LUN that is mapped from storage devices to the application server.
Array LUN	To differentiate the number between the device LUN and the host LUN.

B

Back-end disk port	The port for the connection between the controller subrack and the disk subrack.
Baud rate	The maximum rate of signal state changes per second on a communications circuit. In low-speed communications, each signal state corresponds to a code bit, then the baud rate and the bit rate are the same, that is, the reciprocal of code bits in one second.
Bit error rate	The percentage of bits that have errors relative to the total number of bits received in a transmission.
Boundary scan	A test methodology that uses shift registers in the output connections of integrated circuits. One IC often is connected to the next. A data pattern is passed through the chain and the observed returned data stream affected by the circuit conditions gives an indication of any faults present. The system is defined under IEEE standard 1149.1 and is also often known as JTAG (Joint Test Action Group).

Browser / Server	An architecture that defines the roles of browser and server, where the browser is the service request party and the server is the service provider.

C

Cache	A special area of memory, managed by a cache controller, which improves performance by storing the contents of frequently accessed memory locations and their addresses.
Cache hit ratio	The ratio of directly accessed I/O from Cache to all the I/O operation during the read operation.
Cache prefetch strategy	According to the operation in which data has been read or is being read, the required data is read from a disk into the cache in advance.
CALL HOME	The function that devices send the detected critical events, such as faults, to maintenance engineers through an E-mail or a message.
Captive screw	After the screw is loosened, screw caps and bolts do not fall off the main body.
Cascade	Connect the OceanStor storage system to more disk subracks through connection cables, thus expanding the capacity of the OceanStor storage system.
Cascaded module	A component used for expanding.
CHAP	Challenge handshake authentication protocol. An authentication protocol based on the password. This protocol checks that a user has the right to access a system by using a challenge.
Coffer	A technology for ensuring data security and integrity in the OceanStor storage system. The hard disks in slots 0 to 3 serving as coffers, which store the data of system configuration, data of alarm logs, and the data in the cache that is not written to the disk when the system power is off for emergency and alarm log data.
Coffer disk	Physical storage media. It refers to the hard disks in slots 0 to 3 of the controller subrack.
Command device	Command device for OceanStor Command Line Interface.
Connected LUN	Logically consecutive LUNs are connected through connecting multiple LUN space.
Consistency check	LUN consistency check is an advanced maintenance function of the controller. Through the consistency check, the controller can check the consistency of data on arrays in advance, that is, the validity and integrity of data.
Constant prefetch	A cache prefetch strategy. The size of the data to be prefetched is the size as set. This strategy applies to the applications that require reading data of a fixed size in a certain order. An example is the streaming media demanded by multiple subscribers who use the same bit rate.

Controller subrack	It is the core component of the OceanStor storage system, and is mainly responsible for the storage service. A controller subrack consists of the controller, hard disk, interface card, power entry module (PEM)/fan module, battery, and dual in-line package (DIP) switch board.
Conversion board	A circuit board in the OceanStor storage system for the conversion of disks ports.
Cookie	A technology that allows a Web site server to store a bit of data in the disk or memory of a client or read data from the disk of a client.
Copyback	The process of copying the data from the hot-spare disk back to the previous disk when the faulty member disk is restored or replaced by a new one.
Create RAID group	To organize free disks into a RAID group with a certain RAID level.
Cyclic redundancy check	CRC consists of a great number of bits computed as the data to be protected and append to the data.

D

Data disk	The disk for saving service data in RAID groups.
Defragment	The process of rewriting LUN data on disks, which helps to continue the unoccupied free space among LUNs.
Degraded RAID group	When member disk in a RAID group fails, part or all of the redundancy is lost
Delete RAID group	To delete a RAID group so that member disk in a RAID group becomes a free disk.
DIP switch board	It is used to adjust the FC cascading rate and FC disk rate, and can mute the alarm buzzer.
Dirty page	The data that is stored in only the cache but not written into disks.
Disk array	A set of disks from one or more commonly accessible disk subsystem, combined with a body of control software. The control software presents the disks' storage capacity to hosts as one or more virtual disks.
Disk location	Locate a hard disk, that is, determine the subrack number and slot number of the hard disk in the OceanStor storage system.
Disk subrack	It consists of the following parts: expander board, hard disk, PEM/fan module, and DIP switch board. System capacity can be expanded by cascading multiple disk subracks.
Disk utilization	The percentage of used capacity in the total available capacity.
Dynamic LUN	During the operations of defragment, expanding the member disk of RAID group, modifying the stripe unit size and transferring the level of RAID group dynamically, create a temporary LUN that can help data transfer.

E

Expand the member disk of RAID group dynamically	To add member disk in a RAID group without interrupting the normal services of RAID group.
Expander module	A component used for expanding.
Expansion master LUN	The first LUN composing the connected LUNs is called expansion master LUN.

F

Failed RAID group	The number of failed member disk in a RAID group exceeds the maximum number, which causes data loss.
Failure tolerance	The storage system can provide storage resources normally (system performance may be compromised) when its one or multiple components fail.
Field replaceable unit (FRU)	A module or component which will typically be replaced in its entirety as part of a field service repair operation. Any entity that can be replaced by a user in the field. Examples of this type of FRU might include: backplane (the Shelf housing, for all practical purposes), PEM/fan module, optical module, and battery module. (Not all FRU supports hot swapping.)
Firmware	The program that is embedded in a programmable non volatile memory.
Fragment	The free physical space that has not been divided among different LUNs on a disk.
Free hot-spare disk	A hot-spare disk that is available.
Front-end host port	The port on the controller subrack to connect to the application server and transmit service data. There are three types of the front-end host port: SAS, FC and iSCSI.

G

Gateway	The entrance node on another network.
Global hot-spare disk	A type of hot spare disk. A global spare disk can serve as the spare disk for multiple RAID groups of an array while a local hot spare disk can only serve as the spare disk for only one RAID group.
GSM modem	A wireless modem used to send the information about alarms.

H

Hard disk tray	The tray that bears the hard disk.
Heartbeat cable	The heartbeat cable is a dedicated line on the backplane. It can check the running state of the remote controller in real time. Once the running controller is in the abnormal state, the remote controller can use the heartbeat cable to check the related state and take proper measures.
High watermarks	The high level of the dirty page stored in cache. When the amount of the dirty page in cache reaches the high level, cache begins to store the dirty page into disks.
High-low watermarks	The low level and high level of the dirty page stored in cache. When the amount of the dirty page in cache reaches the high level, cache begins to store the dirty page into disks. When the amount of the dirty page reaches the low level, cache stops storing the dirty page into disks.
Host	The "host" displayed in the OSM3.0 interface is a created virtual host. After a port is added to the host, the host can correspond to a physical application server.
Host port module	A module that bears the various types of host ports, for example, SAS host port, FC host port, and iSCSI host port.
Hot backup/ Online backup	A form of backup in which the data being backed up may be accessed by applications during the backup.
Hot swap	In a running system, inserting or removing a blade does not affect normal running of the system.
Hot-spare disk	The disk that is used to replace the damaged member disk in a RAID group. A spare disk carries the data that is saved on faulty disks.
Hot-spare disk reconstruction	A function of the OceanStor storage system. It refers to the process of restoring the data from the faulty member disk in a RAID group to the spare disk.

I

I/O	Data movement process between memory and peripheral devices in the computer system. I/O is a collective name, indicating the operations reading data into the memory and writing data to other places from computer memory.
Inband management	A method of transmission between the management control information on the network and the bearer service information on the user network through the same logical channel. Inband management enables users to manage disk arrays through commands. Management commands are sent through the service channel, that is, the I/O read-and-write channel. The advantage is quick and stable transmission, which requires no other management network port.
Inconsistent stripe	The protection of the check data block in a redundancy group stripe for the protected space in the stripe is invalid.

Initialize	The process of writing 0 bits in the data area on the logical drive and generating related parity bits so that the logical drive can be in the ready state.
initiator	A system component that can initiate an I/O operation on an I/O bus or on a network.
Intelligent prefetch	A cache prefetch strategy. The system software calculates a proper size of prefetched data. This strategy applies to a read application involving a single bit stream or to the situations where you do not know whether the data is read in a certain order. An example is reading or writing a file.
iSCSI host port	A port which is on the controller subrack connects to the AS. The port transmits service data (used in the network and bearing the SCSI protocol in the IP packet).

L

Link	A physical connection between two nodes of a network.
Logical unit	The entity is located inside the SCSI object, and can execute I/O commands. After a SCSI I/O command is sent to an object, the logic unit inside the object executes this command. Usually, each SCSI physical disk has one logic unit. A tape drive and array controller may have multiple logic units, which process different I/O commands. Each logic unit inside an array controller corresponds to a virtual disk.
Logical unit number	The SCSI identifier of the internal logical unit of a target.
Loose coupling	A system based on messages in which the client and the remote services do not know how the peer side is realized. The communication between the client and the services is based on message architecture. As long as the messages comply with the negotiated architecture, the realization of the client or services can be changed as required without damaging the peer side.
LUN format	The process of preparation for enabling LUNs. During the process, necessary information is written to member disks where LUNs are located.
LUN mapping	The OceanStor storage system maps LUNs to ASs so that the ASs can access the storage reorganization.

M

Maintenance terminal	The computer that is connected through a serial port or management network port and maintains the OceanStor storage system.
Management network	An entity that provides a means to transmit and process the information related to network management.

Management network port	The network port on the controller subrack that is connected to the maintenance terminal. It is provided for the remote maintenance terminal.
Medium scanning	A background program that is run by controllers and provides the function of detecting disk errors. The medium scanning program detects and reports errors to the event log module.
Member disk	A disk in a redundant array of inexpensive disks (RAID) group in the OceanStor storage system.
Member disk reconstruction	A function of the OceanStor storage system. It refers to the process of restoring the data from the faulty disk to the new disk after you replace a faulty member disk in a RAID group with a new one.
Mirroring	A form of storage array in which two or more identical copies of data are maintained on separate media. This prevents data loss due to disk errors.
Mirroring group	In a group of RAID at the RAID 10 level, the member disks that are mirrors of each other are known as a mirroring group.
Modify the stripe unit size dynamically	To modify the stripe unit size without interrupting the normal services of LUN.

N

Native devices	The application server LUN viewed through the device management software on the application server. The application server can access the same array LUN through multiple physical paths. Therefore, for the same array LUN, the number of the application server that is displayed as the local device is consistent with the number of physical paths.

O

OceanStor	A trademark of Huawei storage device.
Outband management	A management mode used during outband networking. In the outband management mode, the management and control information of the network and the bearer service information of the user network are transmitted through different logical channels.
Owning controller	For a LUN, the user configures the owing controller, that is, specified the created LUN to a certain controller. When the owning controller of the LUN is invalid, another controller manages the LUN automatically. When the owning controller of the LUN is restored, the original controller manages the LUN again.

P

Parity disk	The disk for saving check data in RAID groups.

PEM/fan module	The PEM/fan module consists of power supply, fans, power switches, and power sockets.
Physical path	The actual path from the HBA card of the application server to the front-end host port of storage arrays. Regardless of switches on the path, the physical path is only decided by the corresponding relation between the host HBA card and the array port.
Port module	Port module connects various types of front-end host port, such as the front-end host ports of SAS, FC and iSCSI.
Power failure protection	When the external power failure occurs, the alternating circuit (AC) power entry module in the OceanStor storage system can use the battery to supply power. This ensures that dirty page in cache can be written into the coffer safely and avoids data inconsistency caused by data lost.
Primary Storage Controller	The controller which plays a leading role in controlling the management is primary storage controller. It can perform relevant management operations on the controller subrack.
Primary/ Secondary switchover	A procedure during which the two controllers of the OceanStor storage system change their master/slave states.
Prior controller	For the application server LUN, prior controller means that the working controller is the owner controller of the corresponding array LUN.

R

RAID level	The application of different redundant types in the logical drive. The RAID level can improve the fault tolerance and performance and reduce the available capacity of the logical drive. You must specify a RAID level for each logical drive.
Reconstruct	To restore the data in a member disk, when the member disk in a RAID group is faulty.
Reconstruct hot-spare disk	To restore the data from the faulty member disk in a RAID group to the spare disk.
Reconstruct member disk	To restore the data from the faulty disk to the new disk after you replace a faulty member disk in a RAID group with a new one.
Reconstruction	A function of the OceanStor storage system. It refers to the process of restoring the data saved in the faulty member disk in a RAID group.
Redhat package manager	Redhat package manager widely applied in Linux.
Redundancy	The inclusion of extra components of a given type in a system (beyond those required by the system to carry out its function) for the purpose of enabling continued operation in the event of a component failure.
Redundant Array of Independent Disks	A family of techniques for managing multiple disks to deliver desirable cost, data availability, and performance characteristics to host environments.

Redundant copy	When the system monitors that a member disk in the RAID groups is about to fail, the system copies the data in the disk to a hot-spare disk. This technology is called redundant copy.
Repair inconsistent stripe	To correct the invalid protection of the check data block in a redundancy group stripe for the protected space in the stripe.

S

Script	A collection of data statements used to perform an operation.
Secondary Storage Controller	In relation to the primary storage controller, the secondary storage controller is the backup for the primary storage controller. When the primary storage controller fails, the secondary controller can be replaced to be the primary storage controller and performs management operations on the controller subrack.
Serial port	An input/output location (channel) that sends and receives data to and from a computer's CPU or a communications device one bit at a time. Serial ports are used for serial data communication and as interfaces with some peripheral devices, such as mouse and printers.
Service data	Data which is saved in data disk. Service data is the data source for computing check data in parity disk.
SFP optical module	A component that can make data conversion between optical signals and electrical signals and that can receive and transmit data.
Simple network management protocol (SNMP)	An internet engineering task force(IETF) protocol used to monitor and manage the systems and devices on a network. The monitored and managed data is defined by the management information base(MIB). The protocol supports the following functions: data request, data retrieval, data setting or data writing, and trap.
Single point failure	Since some components or channels are not redundant, the failure of a device or component causes the breakdown of all devices or components.
Smooth expansion	A process of expanding capacity online without interrupting services.
Standby network port	In relation to the active network port, the standby network port is a redundant network port on an AS. When the active network port fails, the standby network port is activated to work.
Storage controller	The component performs the following functions: operation conversion, RAID, LUN mapping, disk-striping setting, and other service and fault alarm. It consists of the controller board and port module.
Storage system	An integrated system. It consists of the following parts: controller, storage array, host bus adaptor, physical connection between storage devices, and all control software.
Streaming media	A transmission mode in which data is consumed (read, listened to, or watched) while it is being sent.

Stripe	The process of dividing the consecutive data into the same-sized data blocks and writing the data on each block into different disks. This technology provides a faster read/write speed than a single disk can provide.
Stripe depth	The number of blocks in a strip in a disk array which uses striped data mapping. Also, the number of consecutively addressed virtual disk blocks mapped to consecutively addressed blocks on a single member extent of a disk array.
Stripe unit	The physical extent block that consists of stripes in each physical extent of a redundancy group.
Stripe verify	To verify whether the check data block in a redundancy group stripe protects the protected space in the stripe.
Subnet mask	The technology used by the IP protocol to determine where network segment packets are destined for. The subnet mask is in binary format. Stored in a client, server, or router. The subnet mask matches the IP address.
System bus	A mechanism of the computer system to achieve connections between devices. It is characterized by the signal transmission between two devices on the bus. One device sends commands and data and the other device receives commands and data. Only one transmission can be operated on the bus at any time. Transmission requests of each device are ranked according to their priorities.

T

target	A system component that can receive SCSI I/O operation commands.
topology	The logical layout where computer systems and network components are interconnected with one another. The topological structure gives the interconnection relationship among the components from the viewpoint of communication, but the topological structure does not specify the exact locations of components and the interconnection mode.
Transfer the level of RAID group dynamically	To transfer the level of RAID group dynamically without interrupting the normal services of RAID group.
Trap	A type of SNMP message that indicates the occurrence of an event. This type of message is transmitted to the received through UDP. The transmission process is not completely reliable.
Trunk	It refers to port trunking which aggregates multiple physical ports into a logical path through setting configuration software. By combining the bandwidth of multiple ports, the bandwidth between switches and network nodes are expanded and the ports are provided an wholly occupied bandwidth with the speed several times higher than an independent port.

U

Used hot-spare disk	A hot-spare disk that is in use.
User interface	The interface on which users enter commands for operation.

V

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

W

Working controller	The controller used by the array LUN to read and write a disk.
Write hole	A potential data corruption problem for parity RAID technology resulting from any array failure while application I/O is outstanding, followed by an unrelated member disk failure (some time after the array has been returned to service). Data corruption can occur if member data and parity become inconsistent due to the array failure, resulting in a false regenerating when data failed member disk is subsequently requested by an application.
Write-back cache	A cache technology. When the write operation is completed, the data continues to be stored in the cache and therefore, the operation of writing the data to disks will be delayed. No need to access disks during each write operation.
Write-back cache mirroring	A cache technology. Data is written to the local cache and at the same time written to the opposite cache.
Write-through cache	A cache technology. Data is written to disks. And only when the data is safely written to disks, the procedure of write requests can be ended. Disks need to be accessed during each write operation.

C Acronyms and Abbreviations

A

UPS	Uninterrupted Power Supply ATA
ATA	Advanced Technology Attachment

C

CHAP	Challenge Handshake Authentication Protocol
CLI	Command Line Interface

H

HBA	Host Bus Adapter
HTTPS	Hypertext Transfer Protocol Secure

I

IE	Internet Explorer
IP	Internet Protocol
iSCSI	internet small computer systems interface
ISM	Integrated Storage Management

J

JWS	Java Web Start

L

LAN	Local Area Network

LUN	Logical Unit Number
M	
MAC	Media Access Control
N	
NIC	network interface card
R	
RAID	Redundant Array of Independent Disks
S	
SAN	Storage Area Network
SAS	Serial Attached SCSI
SATA	Serial Advanced Technology Attachment
SCSI	Small Computer Systems Interface
SFP	Small Form-Factor Pluggable
SMI-S	Storage Management Initiative Specification
SMTP	Simple Mail Transfer Protocol
SP	Service Pack
U	
UPS	Uninterrupted Power Supply
V	
VLAN	Virtual LAN
W	
WWN	World Wide Name