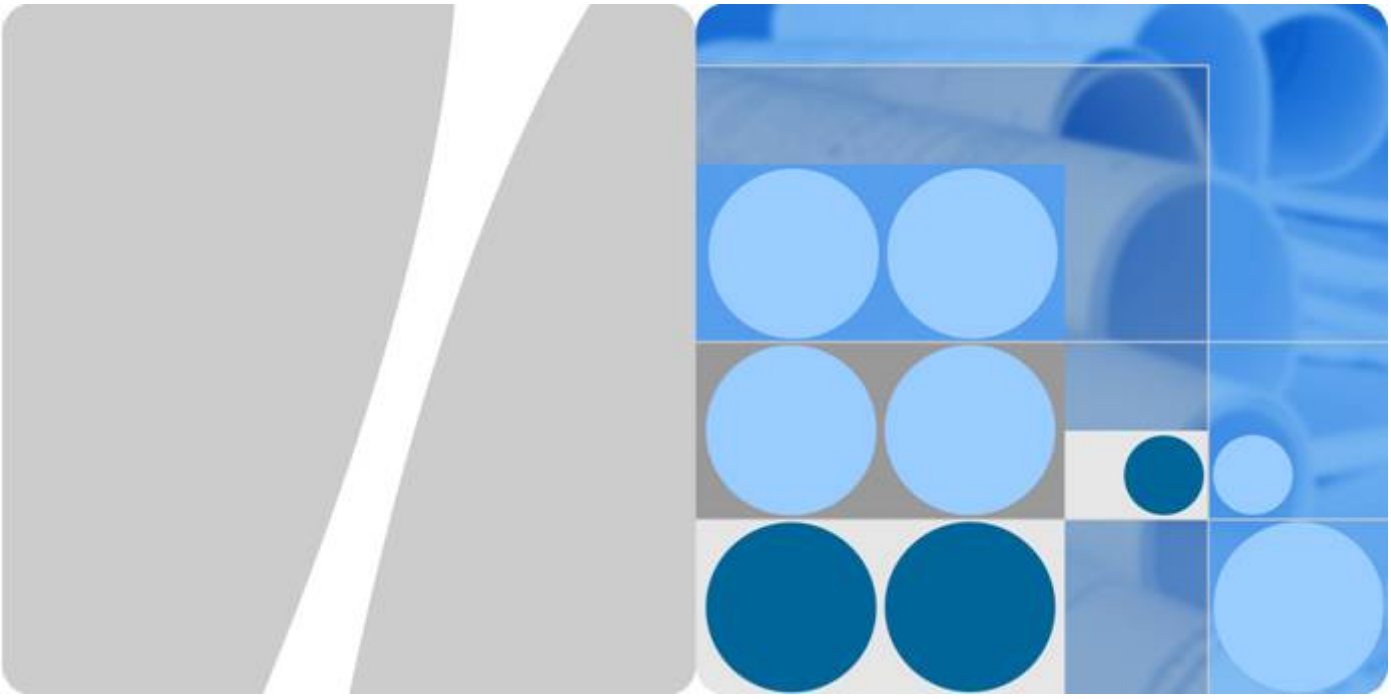


iManager U2000 Unified Network Management System

V100R002C01

High Availability System (Veritas) Software Installation Guide (Solaris)

Issue 06

Date 2010-11-19

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

Trademarks and Permissions


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

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: http://www.huawei.com

Email: support@huawei.com

About This Document

Related Version

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

Product Name	Version
iManager U2000	V100R002C01

Intended Audience

This document describes how to install the U2000 HA system on the Solaris OS and obtain the reference information required during the installation.

This document is intended for:

- Technical support engineers
- Maintenance engineers
- Installation and commissioning engineers

Symbol Conventions

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

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

Symbol	Description
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.

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**.

Change History

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

Changes in Issue 06 (2010-11-19)

The sixth commercial release has the following updates:

Fixed some bugs.

Changes in Issue 05 (2010-10-20)

The fifth commercial release has the following updates:

Fixed some bugs.

Changes in Issue 04 (2010-09-24)

The fourth commercial release has the following updates:

Fixed some bugs.

Changes in Issue 03 (2010-08-16)

The third commercial release has the following updates:

Fixed some bugs.

Changes in Issue 02 (2010-07-16)

The second commercial release has the following updates:

Fixed some bugs.

Changes in Issue 01 (2010-05-18)

Initial release.

Contents

Figures

Tables

1 Installation Overview

This topic explains the terms involved with installing the U2000 Veritas hot standby high availability system into a Solaris operating system (OS).

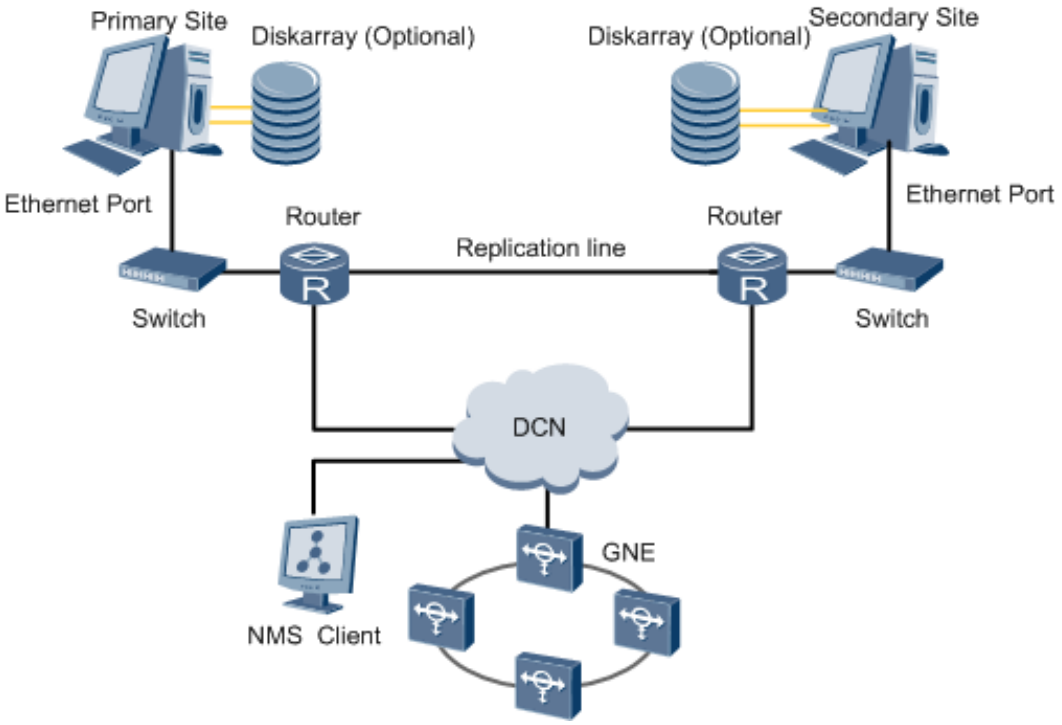
CAUTION

Servers are pre-installed with software from Huawei and can be commissioned immediately. For more information, see the *iManager U2000 Commissioning Guide*. If servers are purchased from other suppliers, install software according to the U2000 deployment.

Definitions for terms as used in this document before introducing the high availability system (Solaris) scheme:

- Server: A server can refer to the hardware and/or software. In the client/server structure, a server refers to the server program. The term refers to hardware when used in reference to a computer where a server program runs.
- Client: Refers to the client application of the software in a client/server structure. The client application can run on a computer along with the server application or on a separate computer. The term refers to hardware when used in reference to the computer where a client application runs.
- Workstation and host: A workstation functions the same as a host. Generally, a workstation or host refers to the computer where services run in a Solaris OS.
- Primary (Secondary) site: Used for the high availability system, the primary (secondary) site refers to the physical primary (secondary) site. Whether a site is a primary site or a secondary site is specified when it is installed, and the role does not change when the system switching occurs. In most of the time, a primary site is in the active state, whereas a secondary site is in the standby state for protecting the primary site.
- Active (Standby) site: It is used for the high availability system. The active (standby) site refers to the site in the active (standby) state. The site in the standby state protects the site in the active state.
- Active (Standby) state: It is used for the high availability system. The active (standby) state refers to the working (protection) state. For example, if all the relevant applications on a site run normally, this site is in the active state.
- Centralized system: Refers to the core processes of the U2000 and database service that are deployed on a server.

Figure 1-1 Network diagram of a high availability system (Solaris)



- Component: Refers to a functional unit of software that you can select to install. A component can consist of multiple deployment packages.
- Deployment package: Refers to a software unit that is deployed on a computer.

  Deployment packages are classified into the following types:
  - System single-instance: These types of deployment packages can be installed on only one server and each component can be deployed with only one instance.
  - Single-server single-instance: These types of deployment packages can be installed on multiple servers and each component can be deployed with only one instance on each server.
  - Single-server multi-instance: These types of deployment packages can be installed on multiple servers and each component can be deployed with multiple instances on each server.

2 Installation Process

This topic describes how to install the high availability system (Solaris).

TIP

Installation engineers not familiar with Solaris OS should read **D Getting Started** to learn about the basic operations of the system.

Table 2-1 lists the steps, reference chapters, and the time required for each step.

Table 2-1 Description about the process of installing the high availability system (Solaris)

Stage	Installation Operation	Chapter	Duration (Min)
1	Prepare for the installation.	**3 Installation Preparations**	30
2	Set controller IP addresses for hardware.	**4 Configuring Controller IP Addresses**	60
3	Power on the system.	**5 Powering On a Server**	20
4	Install Solaris OSs on the primary and secondary sites.	**6 Installing a Solaris 10 OS Using a Quick Installation DVD**	80
5	Install the U2000 on the primary and secondary sites.	**7 Installing the U2000 Software**	250
6	Connect the primary and secondary sites.	**8 Connecting the Primary and Secondary Sites**	20
7	(Optional) Install the license.	**9 Loading or Updating a License File**	10
8	Verify installation.	**10 Checking System Installation**	40

3 Installation Preparations

About This Chapter

This topic describes how to prepare for installation. Before you install a high availability system (Veritas hot standby), ensure that the preparations for the software, hardware, and environment are ready.

This topic describes how to apply for a formal Veritas license. The Veritas license used during U2000 installation is a demo license. After the U2000 server is delivered to the installation site, you must replace the demo license with a formal one in time.

3.1 Configuration Requirements

This topic describes hardware and software requirements for the high availability system (Solaris).

Requirements for Hardware Configuration

The high availability system (Solaris) is deployed on the Solaris platform and requires hardware configurations listed in the **Table 3-1**.

Table 3-1 Configuration requirements on the hardware of the U2000 server

Server Name	Server Description
Sun T5220 (with low-end configuration)	Server, Sun T5220, 4 Core/16 GB memory, 6 x 146 GB
Sun T5220 (with high-end configuration)	Server, Sun T5220, 8 Core/32 GB memory, 6 x 146 GB
M4000 (recommended configuration)	Server, Sun M4000, 4 CPU x 4Core /32 GB memory, 2 x 300 GB
M4000 (compatible configuration)	Server, Sun M4000, 4 CPU x 4Core /32 GB memory, 2 x 146 GB
Disk array	Recommended configuration: OceanStor S2600 (6 x 300 GB)
	Compatible configuration: StorageTek 2540 (6 x 300 GB)
	Compatible configurations: OceanStor S3100 (6 x 146 GB)

NOTE

Disk arrays must meet the preceding configuration requirements. To use disk arrays with other configurations, contact Huawei engineers to check whether such disk arrays are applicable to the high availability system (Solaris).

The disk array stores data to improve database performance. The server must be configured with a disk array if the U2000 manages a moderate amount of network elements (NEs). See chapter 3 Network Scale Planning in the *iManager U2000 Planning Guide* for specific definitions of management scales.

Requirements for Software Configuration

The **Table 3-2** lists the software configuration requirements for the high availability system (Solaris).

Table 3-2 Configuration requirements on the server software

Software	Description
OS	Solaris 10 (10/08) with Huawei Patch 9.0.1
Veritas software	Recommended configurations: Veritas 5.1 Compatible configurations: Veritas 5.0
Database	SYBASE 15.0.3 with EBF16476 and EBF16548
NMS software	U2000 software **NOTE** The U2000 software can be installed on the OS with either the English version or simplified Chinese version.

CAUTION

- If you install a U2000 high availability system for the first time, the Veritas version must be Veritas 5.1 or Veritas 5.0.
- If the current Veritas license is earlier than release 5.0, the license cannot be installed on the Veritas 5.0 or later and you must apply for a new Veritas license of release 5.1. For details about how to apply for a new license, see **3.8 Applying for a Veritas License**.

3.2 Installation Environment Requirements

This topic describes the environment conditions required before you install a U2000, including the telecommunications room environment, cable condition, and networking condition of the telecommunications room.

Before installing a U2000, check the environment according to the following table.

Table 3-3 Installation environment requirements

Check Item	Requirement
Temperature	The required temperature range must be from 15°C to 30°C for long-term working conditions and from 0°C to 45°C for short-term working conditions
Humidity	The required humidity range must be from 40% to 65% in long-term working conditions and from 20% to 90% in short-term working conditions
Dust	The density of the dust whose diameter must be larger than 5 μm is less than or equal to $3 \times 104/m^3$.
Floor	The floor must be anti-static, movable, and grounded.
Space	The telecommunication room must have good ventilation and enough space for operation and maintenance.

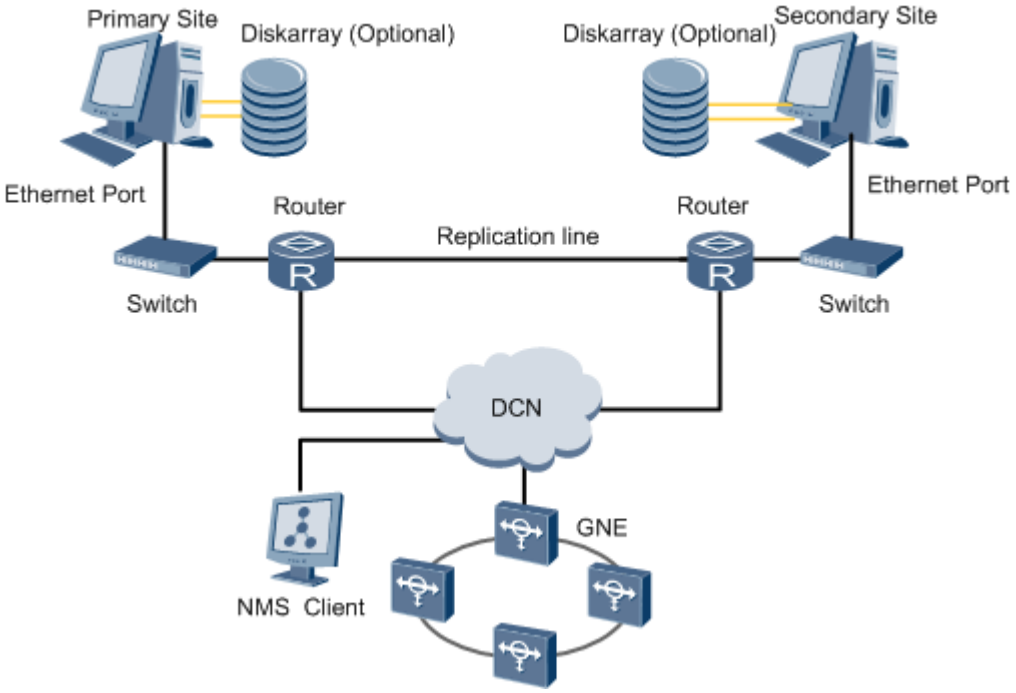
Check Item	Requirement
Power supply	The power supply must be an independent external power supply system that can offer stable electricity. The uninterrupted power supply (UPS) is recommended.
Cable	The network where the server is located must be normal and can be accessed successfully.
Network	The routers for connecting each server must be configured. For the installation of routers, see the installation manual delivered with routers, or contact router suppliers. The networks of routers in every telecommunication room must be connected, including routers and DCNs.

3.3 Networking Structure

This topic describes the networking structure of a high availability system (Solaris). Before installing a high availability system (Solaris), you must get familiar with the networking structure of a high availability system (Solaris).

The following figure shows the networking structure of a high availability system (Solaris).

Figure 3-1 Networking structure of a high availability system (Solaris)



Networking Description About a high availability system (Solaris)

- A high availability system (Solaris) consists of the primary site and secondary site. One Sun workstation is located at each site.

- Configuring a disk array is optional. A disk array is used to store database data to improve database performance.
- The primary and secondary sites communicate with each other using a DCN. The IPMP feature can be configured on the primary and secondary sites to prevent a single NIC from becoming invalid.
- A U2000 client and a network management system maintenance suite client communicate with the server using a DCN.
- NEs and the upper-layer NMS (OSS) communicate with the server using a DCN.

3.4 Collecting Installation Information

This topic describes how to collect installation information. Before installing the high availability system (Solaris), collect required information, including the host name, IP address, route, time zone and time, user password, installation path, component quantity, and instance quantity.

Complete planning for the information listed in the following tables according to the *iManager U2000 Planning Guide*. Collect and record the installation information in the tables.

TIP

Print the following tables and fill in the blanks with the site-specific planning information.

Examples provided in the tables are the default values of servers that come pre-installed with software from Huawei.

Table 3-4 Host name list

Site	Item	Example	Plan
Primary Site	Host name	Primaster	
Secondary Site	Host name	Secmaster	

CAUTION

To ensure that the NMS can run properly, host name planning must comply with the following rules and restrictions:

- The host name of the U2000 server must be unique on the network.
- The host name must be a string consisting of no more than 24 characters that can only be letters (A to Z), digits (0 to 9) and hyphen (-).
- The first character must be a letter and the last character cannot be a hyphen.
- The host name must be case-sensitive.
- The host name cannot contain any space.
- The host name cannot contain only one character.
- The host name cannot contain **--**.
- The host name cannot be any of the following keywords in the high availability system.

```
action  false  keylist  static  after  firm  local  stop    requires
remotecluster
system  group  resource global  Start  str   temp   set     heartbeat
ArgListValues
System  Group  boolean  hard    Name   soft  before online  condition
MonitorOnly
remote  start  cluster  event   VCShm  type  Path   offline Signaled
HostMonitor
Probed  state  Cluster  IState  int    Type  State  VCShmg   NameRule
ConfidenceLevel
```

You need to plan the following types of IP addresses:

- IP address of the workstation controller: This type of IP address is used to remotely log in to a workstation to manage and maintain workstation hardware. For example, you can use it to remotely install the OS or log in to a workstation to perform operation and maintenance if the OS fails to start properly.
- IP address of the disk array controller: This type of IP address is used to remotely manage and maintain equipment.
- System IP address: This type of IP address is used to log in to a server to manage and maintain the OS. It is the IP address of the OS.
- IP address of the heartbeat network service: This type of IP address is used to detect status of the network connection between the primary and secondary sites.
- IP address of the replication network service: This type of IP address is used to replicate data between Primary and secondary sites.
- NMS application IP address: This type of IP address is used to provide external NMS services, such as the communication between the NMS server and the clients or NEs.

NOTE

- During the network planning, the heartbeat network, replication network, and NMS application network can be planed separately or in reuse mode. Planning the heartbeat network, replication network, and NMS application network separately is not recommended.
- The heartbeat network, replication network, and NMS application network can be configured with network protection, that is, IPMP. It is not recommended that IPMP be configured.
- IPMP is short for IP network multipathing. In this mode, two NICs work in 1+1 backup mode. During configuration, an IP address is assigned to each of the NICs and a floating IP address is also set. When the active NIC is faulty, services can be switched to the standby NIC. Configuring IPMP requires two NICs and three IP addresses, and the three IP addresses must be on the same network segment.

According to the number of required NICs, function types of configured IP addresses, and whether IPMP is configured, multiple IP address planning schemes are available for the HA system (Solaris). The typical IP address planning schemes are as follows.

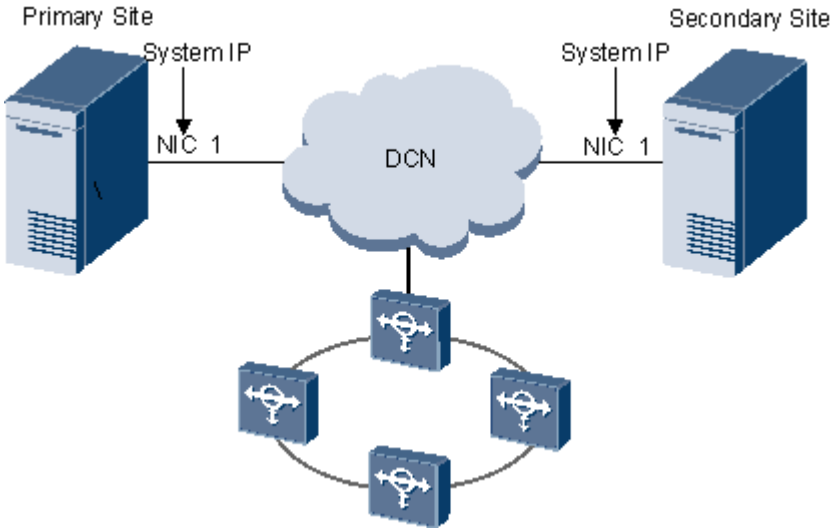
NOTE

In the HA system, the primary and secondary sites can be deployed either in the same place (local deployment) or in different cities (remote deployment). The following uses local deployment as an example to describe IP address planning. If remote deployment is required, ensure that routes between the primary and secondary sites are reachable.

Single-NIC Scheme (Recommended)

Single-NIC scheme: Only one NIC is required. **Figure 3-2** shows the networking diagram. The single-NIC scheme is recommended.

Figure 3-2 Networking example (single-NIC scheme)



IP planning description: Only the System IP address needs to be planned. Heartbeat detection, data replication, and external NMS services between primary and secondary sites are all implemented through NIC 1.

- Advantage: The networking is simple and IP addresses can be saved.
- Disadvantage: All data is transmitted over one link and faults cannot be isolated.

IP planning example: Table 3-5 shows the planning example.

Table 3-5 Example of IP address planning of the single-NIC scheme

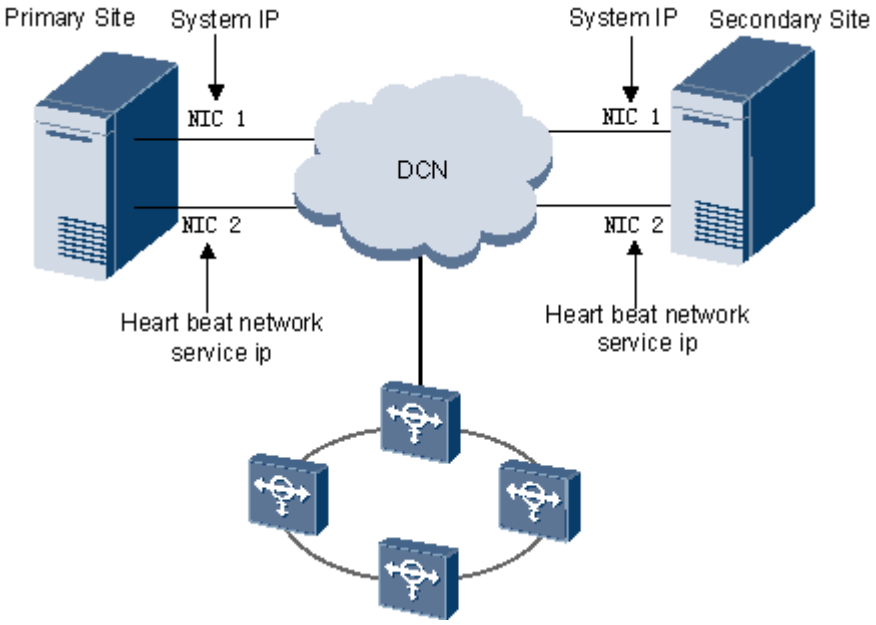
Site	Item	Example (IP Address/ Subnet Mask/Gateway)	Description
Primary site	IP address of the workstation controller	T5220 workstation: 129.9.1.20/255.255.255.0/129.9.1.254	● Plan the IP address according to the model of the selected workstation.

Site	Item	Example (IP Address/ Subnet Mask/Gateway)	Description
		M4000 workstation: ● Primary controller: 129.9.1.21/255.255.255.0/129.9.1.254 ● Secondary controller: 129.9.2.21/255.255.255.0/129.9.2.254	● The M4000 has the primary controller and secondary controller. The IP addresses of the primary controller and secondary controller cannot be on the same network segment.
	IP address of the disk array controller	OceanStor S2600: ● Primary controller: 129.9.1.22/255.255.255.0/129.9.1.254 ● Secondary controller: 129.9.1.23/255.255.255.0/129.9.2.254	-
	System IP address	● 129.9.1.1/255.255.255.0/129.9.1.254 ● Used NIC: e1000g0	-
Secondary site	IP address of the workstation controller	T5220 workstation: 129.9.1.24/255.255.255.0/129.9.1.254 M4000 workstation: ● Primary controller: 129.9.1.25/255.255.255.0/129.9.1.254 ● Secondary controller: 129.9.2.25/255.255.255.0/129.9.2.254	● Plan the IP address according to the model of the selected workstation. ● The M4000 has the primary controller and secondary controller. The IP addresses of the primary controller and secondary controller cannot be on the same network segment.
	IP address of the disk array controller	OceanStor S2600: ● Primary controller: 129.9.1.26/255.255.255.0/129.9.1.254 ● Secondary controller: 129.9.1.27/255.255.255.0/129.9.2.254	-
	System IP address	● 129.9.1.2/255.255.255.0/129.9.1.254 ● Used NIC: e1000g0	-

Double-NIC Scheme (Without IPMP)

Double-NIC scheme (without IPMP): Two NICs are required. **Figure 3-3** shows the networking diagram.

Figure 3-3 Networking example (double-NIC scheme (without IPMP))



IP planning description: Only the System IP address and IP address of the heartbeat network service need to be planned.

- OS management and NMS application are implemented through NIC 1.
- Heartbeat services and data replication services between primary and secondary sites are implemented through NIC 2.

CAUTION

IP addresses of NIC 1 and NIC 2 must be on different network segments.

- Advantage: NMS management and HA system application are implemented through different routes, and thus faults can be isolated.
- Disadvantage: Configurations are complex.

IP planning example: Table 3-6 shows the planning example.

Table 3-6 Example of IP address planning of the double-NIC scheme (without IPMP)

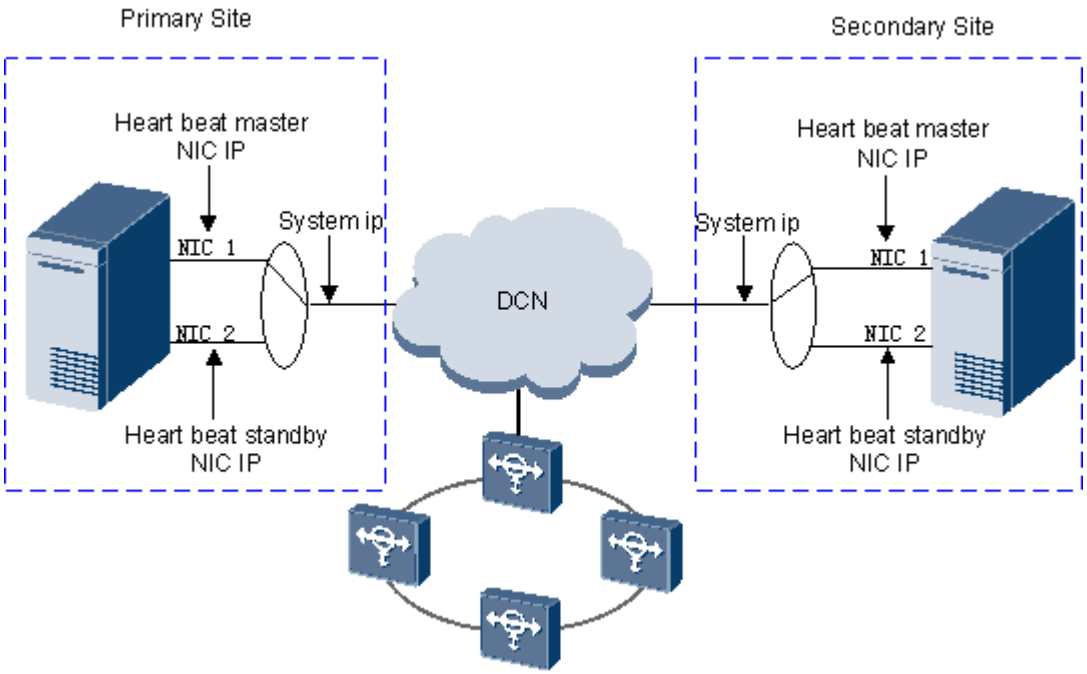
Site	Item	Example (IP Address/ Subnet Mask/Gateway)	Description
Primary site	IP address of the workstation controller	T5220 workstation: 129.9.1.20/255.255.255.0/129.9.1.254	● Plan the IP address according to the model of the selected workstation. ● The M4000 has the primary controller and secondary controller. The IP addresses of the primary controller and secondary controller cannot be on the same network segment.
		M4000 workstation: ● Primary controller: 129.9.1.21/255.255.255.0/129.9.1.254 ● Secondary controller: 129.9.2.21/255.255.255.0/129.9.2.254	
	IP address of the disk array controller	OceanStor S2600: ● Primary controller: 129.9.1.22/255.255.255.0/129.9.1.254 ● Secondary controller: 129.9.1.23/255.255.255.0/129.9.2.254	-
	System IP address	● 129.9.1.1/255.255.255.0/129.9.1.254 ● Used NIC: e1000g0	-
	IP address of the heartbeat network service	● 129.9.2.3/255.255.255.0/129.9.2.254 ● Used NIC: e1000g1	-
Secondary site	IP address of the workstation controller	T5220 workstation: 129.9.1.24/255.255.255.0/129.9.1.254	● Plan the IP address according to the model of the selected workstation. ● The M4000 has the primary controller and secondary controller. The IP addresses of the primary controller and secondary controller cannot be on the same network segment.
		M4000 workstation: ● Primary controller: 129.9.1.25/255.255.255.0/129.9.1.254 ● Secondary controller: 129.9.2.25/255.255.255.0/129.9.2.254	

Site	Item	Example (IP Address/ Subnet Mask/Gateway)	Description
	IP address of the disk array controller	OceanStor S2600: ● Primary controller: 129.9.1.26/255.255.255.0/129.9.1.254 ● Secondary controller: 129.9.1.27/255.255.255.0/129.9.2.254	-
	System IP address	● 129.9.1.2/255.255.255.0/129.9.1.254 ● Used NIC: e1000g0	-
	IP address of the heartbeat network service	● 129.9.2.4/255.255.255.0/129.9.2.254 ● Used NIC: e1000g1	-

Double-NIC Scheme (with IPMP)

Double-NIC scheme (with IPMP): Two NICs are required. **Figure 3-4** shows the networking diagram.

Figure 3-4 Networking example (double-NIC scheme (with IPMP))



IP planning description:

- NIC 1 and NIC 2 work in 1+1 backup mode. The System IP address, IP address of the active heartbeat NIC, and IP address of the standby heartbeat NIC need to be planned.
- If the NICs are running properly, the System IP address maps to the IP address of the active heartbeat NIC. Heartbeat detection, data replication, and external NMS services between primary and secondary sites are all implemented through the System IP address. If the active NIC is faulty, the System IP address automatically maps to the IP address of the standby heartbeat NIC. Heartbeat detection, data replication, and external NMS services between primary and secondary sites are still implemented through the System IP address, thereby implementing NIC protection.

CAUTION

The System IP address, IP address of the active heartbeat NIC, and IP address of the standby heartbeat NIC must be on the same network segment.

- Advantage: The NICs work in 1+1 backup mode and network security is high.
- Disadvantage: The networking is complicated and many IP addresses are required. Future maintenance is complex and switch performance must be high.

IP planning example: Table 3-7 shows the planning example.

Table 3-7 Example of IP address planning of the two-NIC scheme (with IPMP)

Site	Item	Example (IP Address/ Subnet Mask/Gateway)	Description
Primary site	IP address of the workstation controller	T5220 workstation: 129.9.1.20/255.255.255.0/129.9.1.254	• Plan the IP address according to the model of the selected workstation. • The M4000 has the primary controller and secondary controller. The IP addresses of the primary controller and secondary controller cannot be on the same network segment.
		M4000 workstation: • Primary controller: 129.9.1.21/255.255.255.0/129.9.1.254 • Secondary controller: 129.9.2.21/255.255.255.0/129.9.2.254	
	IP address of the disk array controller	OceanStor S2600: • Primary controller: 129.9.1.22/255.255.255.0/129.9.1.254 • Secondary controller: 129.9.1.23/255.255.255.0/129.9.2.254	-
	System IP address	129.9.1.1/255.255.255.0/129.9.1.254	-

Site	Item	Example (IP Address/ Subnet Mask/Gateway)	Description
	IP address of the active heartbeat NIC	● 129.9.1.2/255.255.255.0 /129.9.2.254 ● Used NIC: e1000g0	-
	IP address of the standby heartbeat NIC	● 129.9.1.3/255.255.255.0 /129.9.3.254 ● Used NIC: e1000g1	-
Secondary site	IP address of the workstation controller	T5220 workstation: 129.9.1.24/255.255.255.0/129.9.1.254	● Plan the IP address according to the model of the selected workstation. ● The M4000 has the primary controller and secondary controller. The IP addresses of the primary controller and secondary controller cannot be on the same network segment.
		M4000 workstation: ● Primary controller: 129.9.1.25/255.255.255.0/129.9.1.254 ● Secondary controller: 129.9.2.25/255.255.255.0/129.9.2.254	
	IP address of the disk array controller	OceanStor S2600: ● Primary controller: 129.9.1.26/255.255.255.0/129.9.1.254 ● Secondary controller: 129.9.1.27/255.255.255.0/129.9.2.254	-
	System IP address	129.9.1.4/255.255.255.0/129.9.1.254	-
	IP address of the active heartbeat NIC	● 129.9.1.5/255.255.255.0 /129.9.2.254 ● Used NIC: e1000g0	-
	IP address of the standby heartbeat NIC	● 129.9.1.6/255.255.255.0 /129.9.3.254 ● Used NIC: e1000g1	-

Other Schemes

Contact Huawei engineers for scheme design.

Table 3-8 Route list

Item	Example	Plan
Routing network segment 1	129.9.10.0\255.255.255.0	
Routing network segment 2	10.71.6.0\255.255.255.0	
...	...	
Routing network segment N	10.121.124.0\255.255.255.0	

NOTE

Installation engineers need to add routes to the client and management network to ensure communication between the U2000 and the client, and between the U2000 and the management network.

Table 3-9 Time zone and time list

Item	Example	Plan
Time zone	PRC	
Time	14:00	

Table 3-10 User and password list

User	Example	Plan
T5220 controller (ILOM) user **root**	changeme	
M4000 controller (XSCF) monitoring user **eis-installer**	eis-installer	
OS user **root**	root	
OS user **nmsuser**	admin123	
OS user **sybase**	No password	
Database superuser (sa)	changeme	
Database user	NMSuser	
U2000 user **admin**	admin123	
network management system maintenance suite user **admin**	admin	

User	Example	Plan
VCS Client User **admin**	password	

Table 3-11 Quantity list of configured components and instances

Example	Plan
● One instance for SDH NE management ● One instance for PTN NE management ● One instance for router NE management ● ...	

Before manually install an OS, determine the disk partitioning scheme. If a quick installation DVD is used to install an OS, the installation software automatically partitions disks according to the disk size. For details about disk partitioning planning, see **G Planning Disk Partitions**.

3.5 Checking Required Software

This topic describes the software required to be checked. Ensure that the required software is on-hand and meets the installation requirements before installing the U2000.

Installation engineers can install the U2000 in either of the following ways:

- Using software packages: Required software packages must be on-hand.
- Using DVDs: Required DVDs must be on-hand.

Using Software Packages

Before installing the U2000, ensure that the Solaris OS installation DVD and software packages are available.

Do as follows:

TIP

Read the **Read Me** file before downloading the software packages. The **Read Me** file is stored in the same path as software packages.

1. Access **http://support.huawei.com** and choose **Software Center** > **Version Software** > **Network OSS&Service** > **iManager U2000** > **iManager U2000** > **iManager U2000** > **iManager U2000 V100R002**.
2. Select the version to be installed.
3. Download required software packages listed in **Table 3-12**. It is recommended that installation engineers use the download tool (for example, Flashget). If they use Windows Internet Explorer, some software packages may be renamed automatically after being

downloaded to the local computer. In this case, change the software package names to the same as those on the **http://support.huawei.com**.

4. Use the MD5 to verify correctness of the software packages. For details, see **B.4.12 How to Check Downloaded Software Packages by Using MD5 Software**.
5. **http://support.huawei.com** can store files with a maximum size of 1.8 GB. The file with the size larger than 1.8 GB will be separated into different software packages. The file name extension is part1.rar for the first package, part2.rar for the second, part3.rar for the third, and so on.
   - Download all the required packages. Read the Read Me file before downloading the software package. The Read Me file contains key instructions and restrictions on downloaded files.
   - Before selecting the part1.rar file to decompress, obtain the WinRAR tool from Web site **http://www.winrar.com** and install the tool.

NOTE

- The Solaris OS can be installed only by using DVDs. Therefore, if you install the U2000 by using software packages, ensure that the Solaris OS installation DVD is available.
- In an installation DVD or installation package, *Version* indicates the detailed version number of the U2000. For example, V100R002C01SPCxxx.

Table 3-12 Software package list

Software	Medium Name	Description
Solaris OS installation DVD	You can install the Solaris 10 OS by using the quick installation DVD or the common installation DVD. Using the quick installation DVD is recommended. ● Quick installation DVD: U2000***version***_server_os_solaris_SPARC_sun4v_dvd2 or U2000***version***_server_os_solaris_SPARC_sun4u_dvd1 **NOTE** ● Ensure that the quick installation DVD U2000***version***_server_os_solaris_SPARC_sun4v_dvd2 is available if the hardware type of the selected server is sun4v (the T5220 server for example). ● Ensure that the quick installation DVD U2000***version***_server_os_solaris_SPARC_sun4u_dvd1 is available if the hardware of the selected server is sun4u (the M4000 server for example). Installation engineers can run the **uname -m** command to view the hardware type of a server after logging in to the server OS as user **root**. ● Common installation DVD: Solaris 10 Software (10/08 SPARC Platform Edition) **NOTE** To install the Solaris 10 OS by using the common installation DVD, you also need to prepare the OS patch DVD: U2000***version***_server_patch_solaris_SPARC_dvd3, or OS patch software package U2000***version***_server_ospatch_solaris_SPARC.tar.	It is used to install Solaris OS. **It must be available.**
StorageTek 2540 disk array manager CAM	Installation package: U2000***version***_server_ospatch_solaris_SPARC.tar	**It is required only if you configure the StorageTek 2540 disk array**.

Software	Medium Name	Description
Database software package	Installation package: U2000***version***_ server_db_solaris_SPARC.tar	**It must be available.** It is used to install the database.
Veritas software package	To install the Veritas 5.1, make the following software available: 1. Veritas software installation package: veritas5.1_solaris.tar.gz 2. Veritas patch package:U2000***version***_ server_veritas5-1_patch_solaris_ SPARC.tar To install the Veritas 5.0, make the following software available: 1. Veritas software installation package: veritas5.0MP3_solaris.tar.gz 2. Veritas patch package:U2000*Version*_ server_veritas5-0_patch_solaris_ SPARC.tar	**It must be available.** It is used to install the Veritas.
U2000 server software package	Basic component: U2000***version***_ server_nmsbase_solaris_SPARC.tar	**It must be available.** It is used to install the U2000.
	Core component: U2000***version***_ server_nmscore_solaris_SPARC.tar	**It must be available.** It is used to install the U2000.
	Transport component: U2000***version***_ server_nmstrans_solaris_SPARC.tar	**It is required only if the U2000 needs to manage Huawei transport equipment**. Huawei transport equipment includes: ● MSTP equipment ● WDM equipment ● NA WDM equipment ● Submarine equipment ● RTN equipment ● PTN equipment

Software	Medium Name	Description
	IP component: U2000*version*_ server_nmsip_solaris_SPARC.tar	**It is required only if the U2000 needs to manage Huawei IP equipment**. Huawei IP equipment includes: ● Routers ● Switches ● Metro service equipment ● Broadband access equipment ● VoIP gateways ● Firewalls ● Service inspection gateway ● SVN equipment
	Access component: U2000*version*_ server_nmsaccess_solaris_SPARC.tar	**It is required only if the U2000 needs to manage Huawei access equipment**. Huawei access equipment includes: ● FTTx equipment ● MSAN equipment ● DSLAM equipment

Using DVDs

Ensure that the following DVDs are on-hand before installing the U2000 by using DVDs.

Table 3-13 DVD list

Software	DVD Name
Solaris OS installation DVD	You can install the Solaris 10 OS by using the quick installation DVD or the common installation DVD. Using the quick installation DVD is recommended. ● Quick installation DVD: U2000***version***_server_os_solaris_SPARC_sun4v_dvd2 or U2000***version***_server_os_solaris_SPARC_sun4u_dvd1 **NOTE** ● Ensure that the quick installation DVD U2000***version***_server_os_solaris_SPARC_sun4v_dvd2 is available if the hardware type of the selected server is sun4v (the T5220 server for example). ● Ensure that the quick installation DVD U2000***version***_server_os_solaris_SPARC_sun4u_dvd1 is available if the hardware of the selected server is sun4u (the M4000 server for example). Installation engineers can run the **uname -m** command to view the hardware type of a server after logging in to the server OS as user **root**. ● Common installation DVD: Solaris 10 Software (10/08 SPARC Platform Edition) **NOTE** To install the Solaris 10 OS by using the common installation DVD, you also need to prepare the OS patch DVD: U2000***version***_server_patch_solaris_SPARC_dvd3, or OS patch software package U2000***version***_server_ospatch_solaris_SPARC.tar.
StorageTek 2540 disk array manager CAM (Select it when you configure the StorageTek 2540 disk array)	U2000***version***_server_patch_solaris_SPARC_dvd3
Database software DVD	U2000***version***_server_db_solaris_SPARC_dvd4
Veritas software DVD	1. Veritas software installation DVD: Storage Foundation and HA Solutions 5.1 for Solaris SPARC or VERITAS Storage Foundation and High Availability Solution, 5.0 Maintenance Pack 3 for Solaris 2. Veritas patch installation DVD: U2000***version***_server_patch_solaris_SPARC_dvd3
U2000 server software	U2000***version***_server_nms_solaris_SPARC_dvd5

3.6 Checking Hardware Connections

This topic describes how to check that hardware is installed and connected properly.

Prerequisite

The server hardware must have been installed and equipment cables must have been connected.

Procedure

1. Ensure that the power cables and ground wires for all components are tightly connected and in good contact and that the polarities are properly placed.
2. Ensure that all cables are bundled and free of visible damage.
3. Check hardware connections and network cable connections according to the hardware connection diagram.

   NOTE

   - Configuring disk arrays is optional. If no disk array is configured, skip the connection to disk arrays.
   - The following hardware connection diagrams are based on a single-NIC network configuration scheme. For details about a single-NIC network configuration scheme, see **3.4 Collecting Installation Information**. The hardware connections based on other network configuration schemes are similar.
   - The following figure shows the hardware connection of the T5220 server.

   Figure 3-5 Hardware connection between the T5220 server and the OceanStor S2600

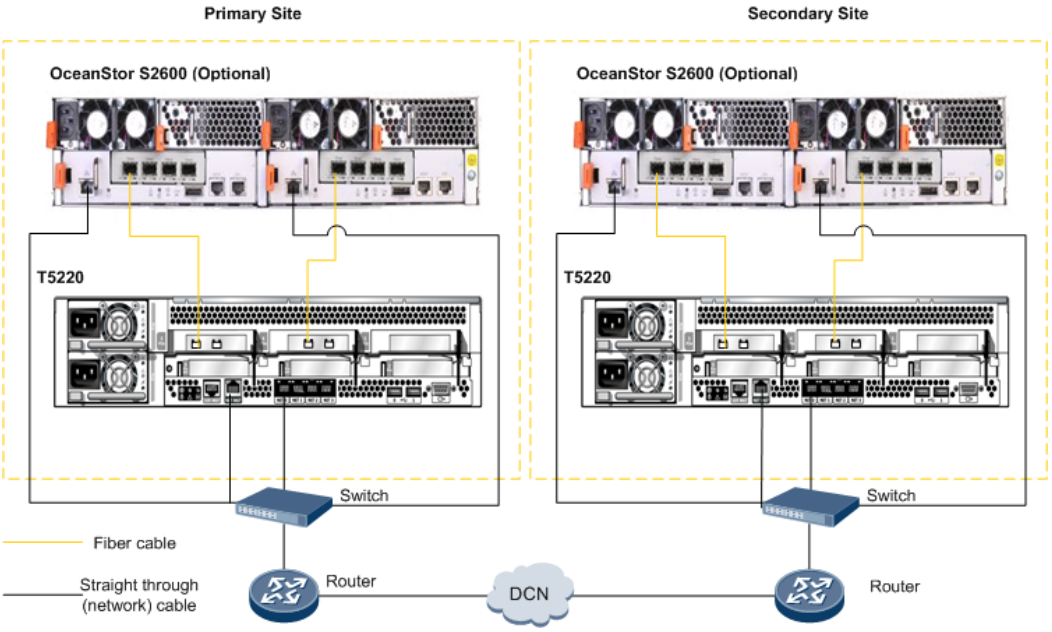


Figure 3-6 Hardware connection between the T5220 server and the OceanStor S3100

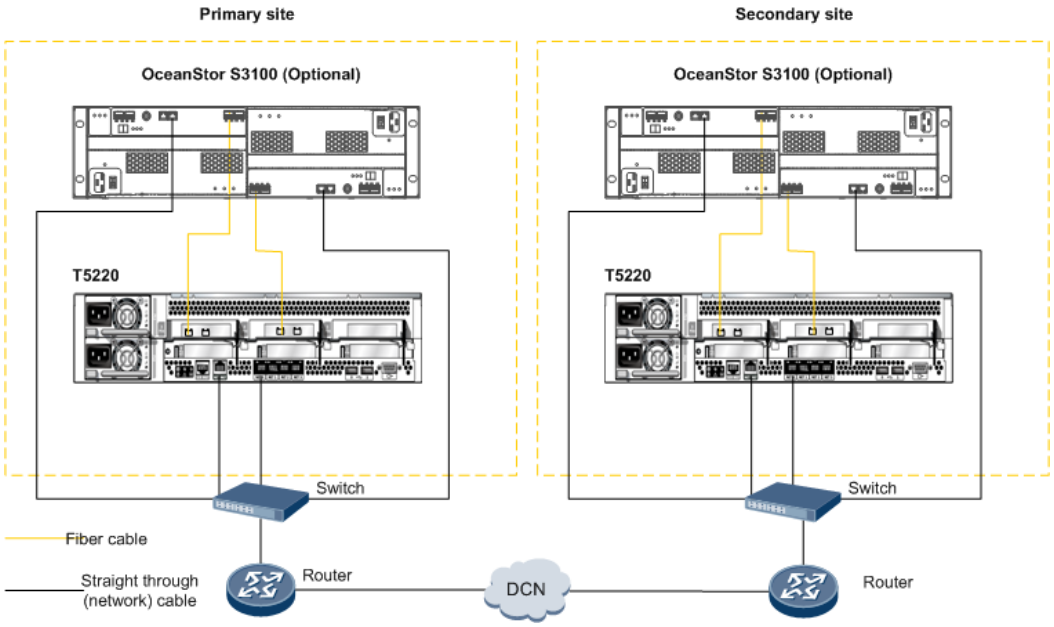
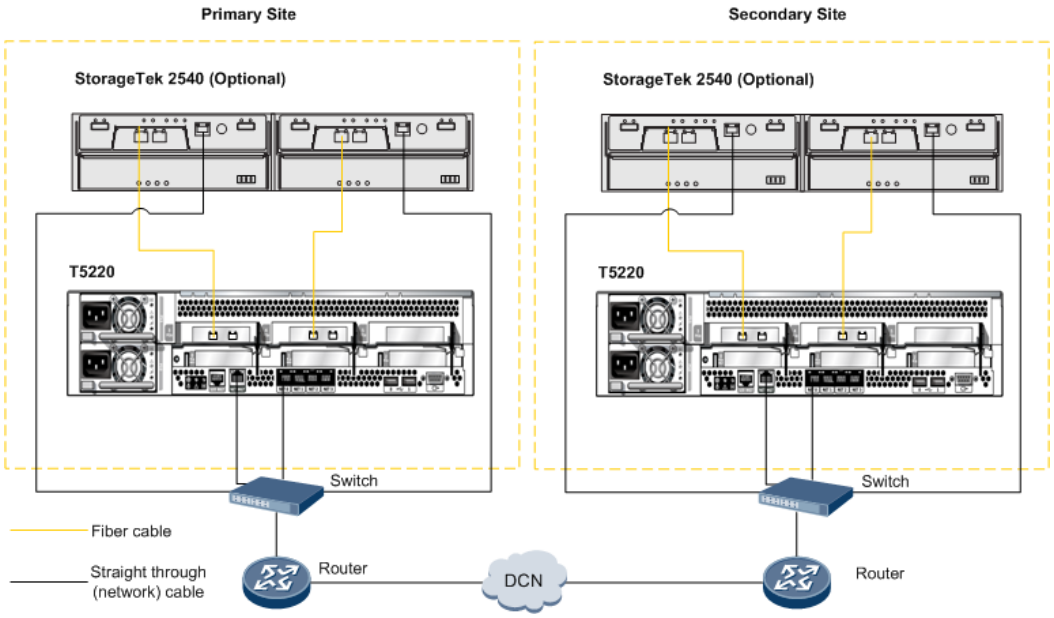


Figure 3-7 Hardware connection between the T5220 server and the StorageTek 2540



- The following figure shows the hardware connection of the M4000 server.

Figure 3-8 Hardware connection between the M4000 server and the OceanStor S2600

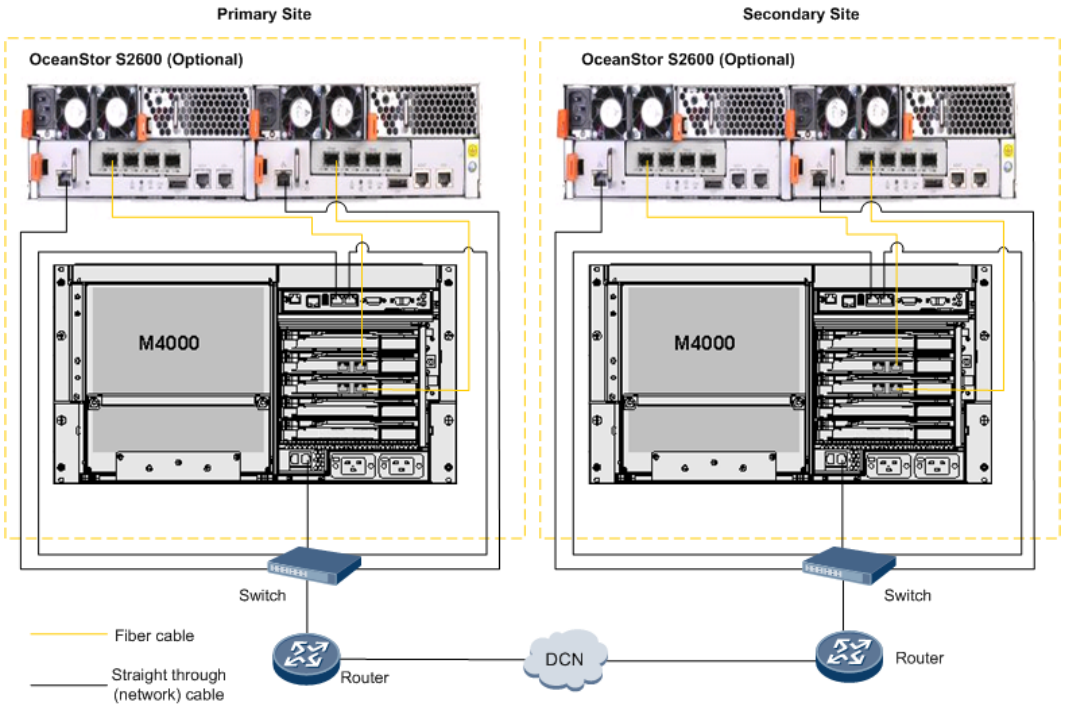


Figure 3-9 Hardware connection between the M4000 server and the OceanStor S3100

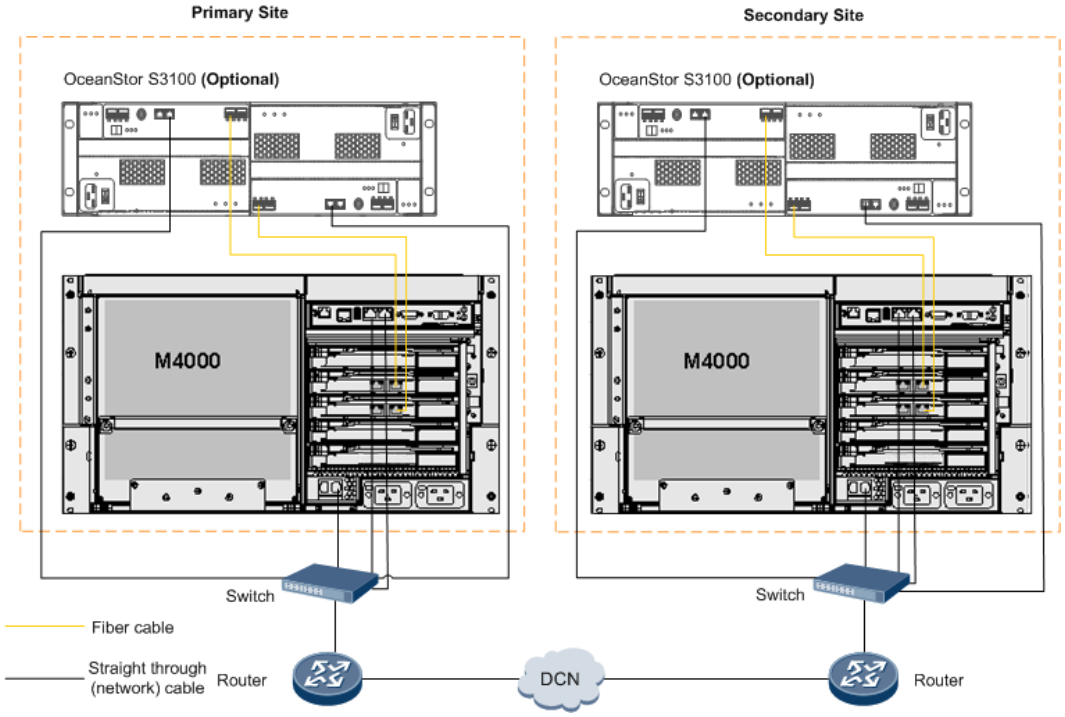
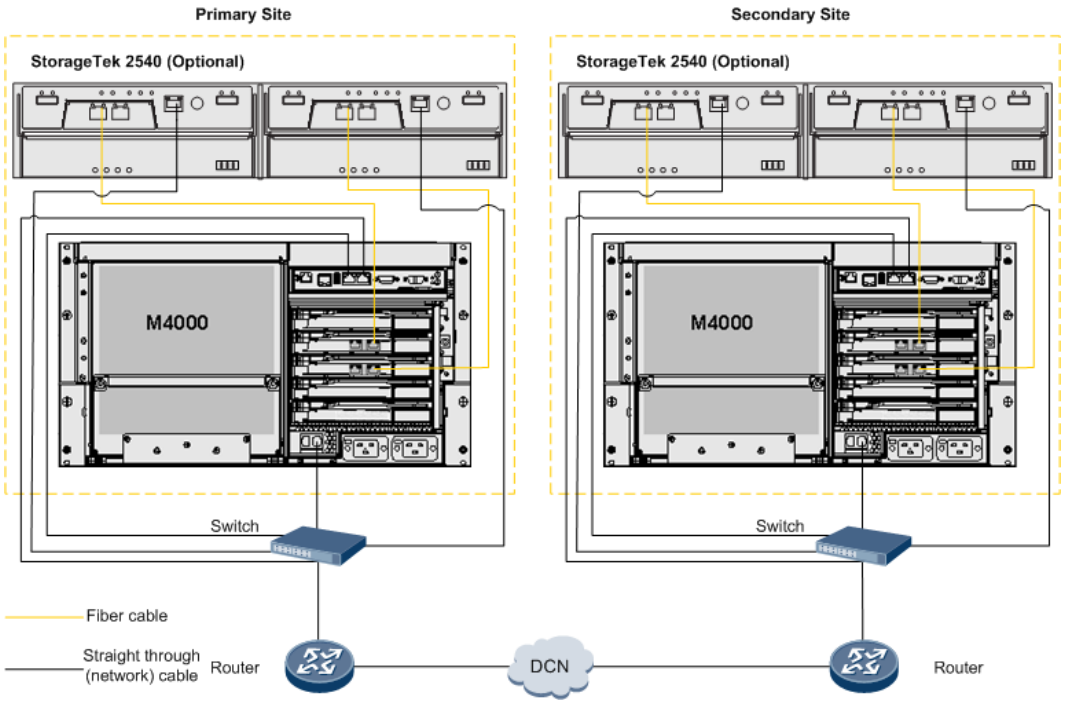


Figure 3-10 Hardware connection between the M4000 server and the StorageTek 2540



4 Check the plugs and sockets.

1. Ensure that the latches of cable plugs are locked fast and the plugs of coaxial cables are secured tightly.
2. Ensure that the pins in each socket are complete and in good order. Curved pins may cause short circuits.

5 Ensure that all debris (cable straps, stubs, or moisture-absorbent packets) are picked up.

6 Remove unnecessary items from the telecommunications room. The workbench must be neat and the movable floor must be level and clean.

----End

3.7 Applying for a U2000 License

This topic describes how to apply for a U2000 license.

Context

- The license file is not delivered to customers along with a U2000 installation DVD. Contact Huawei engineers for the application of a U2000 license according to the contract number and ESNs of the primary and secondary sites.
- An ESN is a string consisting of 40-digit numerals or letters obtained through encrypted calculation on the MAC addresses of the U2000 server network interface. The number of ESNs is the same as the number of network interfaces on the U2000 server.

The U2000 license is valid as long as it is bound to any of the server ESNs. To avoid applying for a new license due to replacing certain network interface cards (NICs), save all the ESNs to ensure proper use of the U2000 license.

- In a high availability system (Veritas hot standby) scheme, the primary and secondary sites share a U2000 license. The U2000 license file is bound to the ESNs of the primary and secondary sites. When applying for a U2000 license, you must save the ESNs of the primary and secondary sites separately.

Procedure

1. Obtain the contract number.
2. View ESNs of the primary and secondary sites by using the ESN tool carried by the NMS.

   Mode 1: Use the ESN tool to generate ESNs before installing the U2000.

   NOTE

   Make the following preparations:

   - Obtain the ESN tool released with U2000 version from **http://support.huawei.com**. The ESN tool name is **U2000*version*_ESN_solaris_SPARC.tar**.
   - Copy the ESN tool package to the computer.

   1. FTP the ESN tool to the U2000 server in binary mode. For example, upload the ESN tool to the **/opt** path. Details are as follows:
      a. Log in to the computer where the ESN tool is stored.
      b. Choose **start** > **Run**. Enter **ftp** ***system IP address of the server*** and click **OK**. The FTP connection will be established and the command line interface (CLI) will be displayed.
      c. Enter **root** as the name of the OS user.
      ```
      User (IP_address:(none)):root
      ```
      d. Enter the password of user **root**.
      ```
      Password:
      ```
      e. Set the format of the file to be transferred by means of FTP to **bin**.
      ```
      ftp> bin
      ```
      f. Access the directory on the computer where the ESN tool is stored.
      ```
      ftp> lcd PC_directory
      ```
      g. Access the **/opt** directory.
      ```
      ftp> cd /opt
      ```
      h. Run the **put** command to upload the ESN tool to the server.
      ```
      ftp> put ""
      ```
      i. Run the following command to exit the FTP program:
      ```
      ftp> quit
      ```
   2. Run the following commands to decompress the ESN tool package:
      ```
      # cd /opt
      # tar xvf U2000version_ESN_solaris_SPARC.tar
      ```
   3. Run the following command to view the ESN:
      ```
      # ./esn
      ```

      Information similar to the following is displayed:

      ```
      ESN0:EBB74B99612CEDC82AD0A59886EC5018CE44DDD4
      ESN1:BDA706C825FE0543DC028209778AA66396545412
      ESN2:E1B00EEF6947DD95687AA5C608B72ACC532AB2BD
      ```

```
ESN3:F72F9EC08AEE78AA05A42EFD7BFD89F5E03139C4
...
```

Mode 2: View the ESN using the ESN tool of the NMS after installing the U2000.

1. Log in to the OSs of the primary and secondary sites as the **root** user.
2. Run the following commands to view the ESN:

```
# . /export/home/nmsuser/.profile
# cd /opt/U2000/server/lbin
# ./esn
```

NOTE

Leave a space between the dot (.) and the command **/export/home/nmsuser/.profile**.

Information similar to the following is displayed:

```
ESN0:EBB74B99612CEDC82AD0A59886EC5018CE44DDD4
ESN1:BDA706C825FE0543DC028209778AA66396545412
ESN2:E1B00EEF6947DD95687AA5C608B72ACC532AB2BD
ESN3:F72F9EC08AEE78AA05A42EFD7BFD89F5E03139C4
...
```

3 Send the contract number and the ESNs of the primary and secondary sites to the related Huawei engineer or the local office of Huawei.

NOTE

Huawei engineers need the contract number and ESN to procure the license from **http://license.huawei.com**. For details about how to apply for the license file, see the *iManager U2000V100R002C01 License Instructions*.

4 Huawei engineers will send the license file after it is procured.

The NMS license file is stored in the .dat format.

----End

3.8 Applying for a Veritas License

This topic describes how to apply for a formal Veritas license. The Veritas license used during U2000 installation is a demo license. After the U2000 server is delivered to the installation site, you must replace the demo license with a formal one in time.

Context

CAUTION

The Veritas licenses for the primary and secondary sites are different and thus must be applied for separately.

NOTE

If the version of the current Veritas license is earlier than 5.0 but the license does not expire, apply for a Veritas license with the version of 5.1 free of charge according to the information about the current license.

Procedure

1. Collect the following information according to the Veritas license application form:
   - Serial number of the license confirmation form
   - Contract number
   - Software item
   - License item quantity

   CAUTION

   - The license confirmation form is delivered together with the DVD. The license confirmation form functions as a license file and should be kept properly on site.
   - If there are multiple serial numbers and the software items are the same, you must fill in **Software Item Qty** with the total number of license confirmation forms.
   - For the licenses whose BOMs start with 9904, no license confirmation form is available for on-site delivery. Therefore, Huawei engineers need to fill in **Serial No.** with a back slash (\) when applying for such a license.

2. Send the information to the related Huawei engineer or the local office of Huawei.
3. With the provided information, the related Huawei engineer accesses **http://support.huawei.com** and chooses **Software Center** > **Software License** > **Outsourcing License** > **License Application**. The page for applying for purchased software licenses is displayed.
4. Huawei engineer enters the license application information to apply for a Veritas license.
5. Huawei engineer sends you the Veritas license.

----End

4 Configuring Controller IP Addresses

About This Chapter

Controller IP addresses are used to manage and maintain equipment remotely. Configure controller IP addresses for equipment before installing the operating system (OSs).

4.1 Configuring Controller IP Addresses for Workstation

This topic describes how to configure controller IP addresses for the T5220 and M4000 servers. System controller IP addresses are used to install, manage, and maintain servers remotely. After servers are powered on, installation engineers can set system controller IP addresses.

4.1.1 Configuring the IP Address for a System Controller on a T5220 Server

This topic describes how to configure the IP address for a system controller on a T5220 server. After the IP addresses are configured, installation engineers can install, manage, and maintain servers remotely by using this IP address.

Prerequisite

- The controller IP addresses are obtained.
- The server is powered on.

Context

Installation engineers can configure server connections through system controllers so that Sun servers can be remotely controlled and maintained.

In the high availability (HA) system, operations must be performed at the primary and secondary sites.

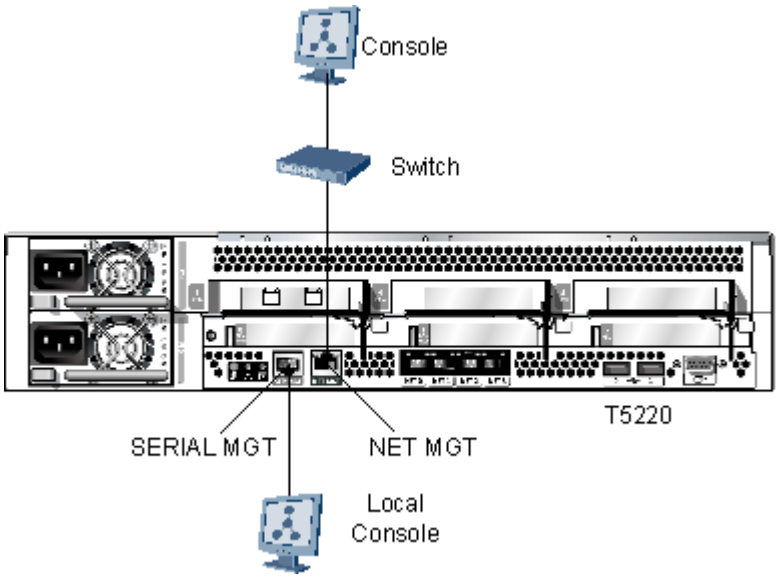
Procedure

1 Connect the computer and the server physically.

1. Use a serial port (DB9-RJ45) to connect the serial port of the local console and the serial port (SERIAL MGT) of the server.

   Use an RJ-45 connector at one end of the serial port cable to connect to the serial port (SERIAL MGT) of the server and use a DB-9 connector at the other end of the cable to connect to the serial port (COM1 or COM2) of the computer.
2. Use a network cable to connect the network management port (NET MGT) of the system controller and the switch.

Figure 4-1 Connections between the T5220 server and the controller



2 Set up a logical connection between the computer and the server.

1. Start the computer and enter Windows OS.
2. Choose **start** > **Programs (P)** > **Accessories** > **Communications** > **HyperTerminal**.
3. In the **Connection Description** dialog box, enter the name of the new connection, such as **NMS**, and click **OK**.
4. In the dialog box that is displayed, select the serial port of the computer that is used to connect to the server, such as **COM1**, and click **OK**.
5. In the dialog box that is displayed, click **Restore Defaults**.
6. Click **OK**.

3 Press **Enter**.

Enter the user name and password. The default user name is **root** and the default password is **changeme**.

NOTE

The OS will be started after this step is complete if the OS is installed on the workstation. Run the **#.** command to display the prompt of the controller.

4 Perform the following operations to configure hardware at the **->** prompt:

1. Enter **cd /SP/network**.

   The following message will be displayed:

   ```
   /SP/network
   ```

2. Enter **set state=enabled**.

   The following message will be displayed:

   ```
   Set 'state' to 'enabled'
   ```

3. Enter **set pendingipaddress=*controller IP address***.

   The following message will be displayed:

```
Set 'pendingipaddress' to 'controller IP address'
```

4. Enter **set pendingipdiscovery=static**.

   The following message will be displayed:

   ```
   Set 'pendingipdiscovery' to 'static'
   ```

5. Enter **set pendingipnetmask=*controller subnet mask***.

   The following message will be displayed:

   ```
   Set 'pendingipnetmask' to 'controller subnet mask'
   ```

6. Enter **set pendingipgateway=*gateway IP address of controller***.

   The following message will be displayed:

   ```
   Set 'pendingipgateway' to 'gateway IP address of controller'
   ```

7. Enter **set commitpending=true**.

   The following message will be displayed:

   ```
   Set 'commitpending' to 'true'
   ```

8. Enter **exit** to complete configuration.

5 Disconnect the serial port of the system controller from the HyperTerminal. Configuration is complete.

----End

4.1.2 Configuring the IP Address for a System Controller on an M4000 Server

This topic describes how to configure the IP address for a system controller on an M4000 server. After the IP addresses are configured, installation engineers can install, manage, and maintain servers remotely by using this IP address.

Prerequisite

- The controller IP addresses are obtained.
- The server is powered on.
- The OS of the server is shut down.

Context

Installation engineers can configure server connections through system controllers so that Sun servers can be remotely controlled and maintained.

In the high availability (HA) system, operations must be performed at the primary and secondary sites.

Procedure

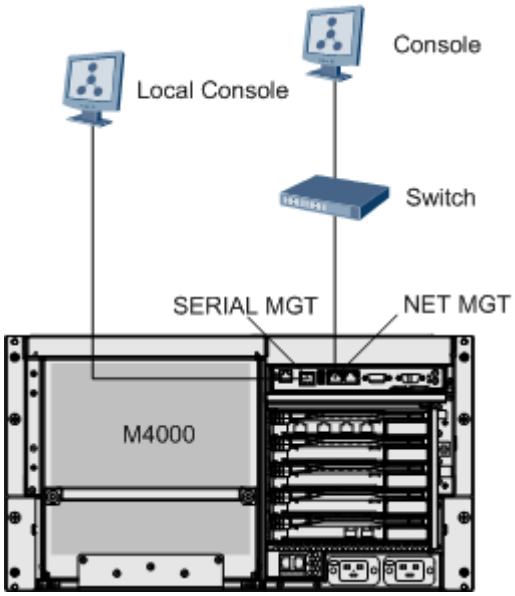
1 Connect the computer and the server physically.

1. Use a serial port (DB9-RJ45) to connect the serial port of the local console and the serial port (SERIAL MGT) of the server.

Use an RJ-45 connector at one end of the serial port cable to connect to the serial port (SERIAL MGT) of the server and use a DB-9 connector at the other end of the cable to connect to the serial port (COM1 or COM2) of the computer.

2. Use a network cable to connect the network management port (NET MGT) of the system controller and the switch.

Figure 4-2 Connections between the M4000 server and the controller



2 Set up a logical connection between the computer and the server.

1. Start the computer and enter Windows OS.
2. Choose **start** > **Programs (P)** > **Accessories** > **Communications** > **HyperTerminal**.
3. In the **Connection Description** dialog box, enter the name of the new connection, such as **NMS**, and click **OK**.
4. In the dialog box that is displayed, select the serial port of the computer that is used to connect to the server, such as **COM1**, and click **OK**.
5. In the dialog box that is displayed, click **Restore Defaults**.
6. Click **OK**.

3 Press **Enter**.

Enter the user name. Enter the default user name (**default**) if the system is being logged in to for the first time.

```
login: default
```

A message similar to the following will be displayed:

```
Change the panel mode switch to Service and press return...
```

4 Within 5 to 10 seconds, insert the key into the key slot in the front panel of the M4000. Turn the switch to **Service** labeled with  and press **Enter**.

A message similar to the following will be displayed:

```
Leave it in that position for at least 5 seconds. Change the panel mode switch to
Locked, and press return...
```

5 Within 5 to 10 seconds, turn the switch to **Locked** labeled with  and press **Enter**.

A message similar to the following will be displayed:

```
XSCF>
```

NOTE

If the event that XSCF> is not displayed (which means that login has failed), attempt to log in again.

6 Run the following commands to create a monitor user:

```
XSCF> adduser eis-installer
XSCF> setprivileges eis-installer platadm useradm auditadm fieldeng
XSCF> password eis-installer
New XSCF password:
Retype new XSCF password:
```

NOTE

The password must contain the following:

- At least two letters
- At least one number or one special character
- At least 8 to 16 characters

The **eis-installer** user has complete access rights and can run all commands after the password is set. The default password is **eis-installer**.

7 Run the following commands to log in to the system as the new user:

```
XSCF> exit
logout
login: eis-installer
```

8 Enter the password.

9 Run the following command to set the time for automatic logout:

```
XSCF> setautologout -s 60
60min
```

10 Run the following command to set the time zone:

```
XSCF> settimezone -c settz -s name_of_the_time_zone
```

NOTE

Run the following command to query the name of the time zone:

```
XSCF> settimezone -c settz -a -M
```

11 Run the following command to set the time:

```
XSCF> setdate -s time
```

NOTE

System time is entered in **year.month.date-hour:minute:second** (for example, **2008.03.25-17:13:00**). System time will be displayed in the following format:

```
Tue Mar 25 17:13:00 CST 2008
```

A message similar to the following will be displayed:

```
The XSCF will be reset. Continue? [y|n]:
```

12 Enter **n**.

13 Run the following command to set the altitude:

```
XSCF> setaltitude -s altitude=1000
```

A message similar to the following will be displayed:

```
1000m
```

14 Run the following command to enable SSH:

```
XSCF> setssh -c enable
```

A message similar to the following will be displayed:

```
Continue? [y|n]:
```

15 Enter **y**.

A message similar to the following will be displayed:

```
Please reset the XSCF by rebootxscf to apply the ssh settings.
```

16 Run the following command to enable the Telnet function:

```
XSCF> settelnet -c enable
```

17 Run the following command to configure the DSCP of the controller:

```
XSCF> setdscp
DSCP network [0.0.0.0] > 192.168.224.0
DSCP netmask [255.255.255.0] >
```

Press **Enter** to continue.

```
XSCF address [192.168.224.1] >
```

Press **Enter** to continue.

```
Domain #00 address [192.168.224.2] >
```

Press **Enter** to continue.

```
Domain #01 address [192.168.224.3] >
```

Press **Enter** to continue.

NOTE

If the configuration is being performed for the first time, the following message will be displayed: **Commit these changes to the database? [y|n]**. Enter **y** to accept the settings.

18 Run the following commands to set the IP addresses of the controllers:

```
XSCF> setnetwork -c up xscf#0-lan#0
XSCF> setnetwork -c up xscf#0-lan#1
XSCF> setnetwork xscf#0-lan#0 -m Subnet_mask IP_address_of_the_primary_controller
XSCF> setnetwork xscf#0-lan#1 -m Subnet_mask IP_address_of_the_secondary_controller
XSCF> sethostname -d huawei.com
XSCF> setroute -c add -n 0.0.0.0 -g
IP_address_of_the_network_gateway_of_the_primary_controller xscf#0-lan#0
XSCF> setroute -c add -n 0.0.0.0 -g
IP_address_of_the_network_gateway_of_the_secondary_controller xscf#0-lan#1
```

19 Run the following command:

```
XSCF> sethostname xscf#0 sc
```

20 Run the following command to apply network settings:

```
XSCF> applynetwork
```

A message similar to the following will be displayed:

```
The following network settings will be applied:
  xscf#0 hostname  :sc
  DNS domain name  :huawei.com

  interface        :xscf#0-lan#0
  status           :up
  IP address       :IP_address_of_the_primary_controller
  netmask          :255.255.255.0
  route            :-n 0.0.0.0 -m 0.0.0.0 -g
IP_address_of_the_network_gateway_of_the_primary_controller

  interface        :xscf#0-lan#1
  status           :up
  IP address       :IP_address_of_the_secondary_controller
  netmask          :255.255.255.0
```

```
  route            :-n 0.0.0.0 -m 0.0.0.0 -g
IP_address_of_the_network_gateway_of_the_secondary_controller

Continue? [y|n]
```

21 Enter **y**.

A message similar to the following will be displayed:

```
Please reset the XSCF by rebootxscf to apply the network settings.
Please confirm that the settings have been applied by executing
showhostname, shownetwork, showroute and shownameserver after rebooting
the XSCF.
```

22 Run the following command to restart the system controller so that the settings take effect:

```
XSCF> rebootxscf
```

A message similar to the following will be displayed:

```
The XSCF will be reset. Continue? [y|n]:
```

23 Enter **y** to restart the controller.

A message similar to the following will be displayed:

```
XSCF> Mar 25 09:13:02 localhost XSCF[105]: XSCF shutdown sequence start
execute K000end  --  complete
execute K100end  --  complete
execute K101end  --  complete
......
login:
```

Restarting the system controller takes about three minutes. Wait patiently.

24 **Optional:** Perform the following to test the connection of the network management port of the primary controller.

TIP

- The port of the primary controller on the M4000 server is on the right.
- Before the test, the console must communicate properly with the primary controller on the M4000 server. If the console is directly connected to the primary controller of the M4000 server by a network cable, you must change the IP address of the console to ensure that the IP addresses of the console and the primary controller are on the same network segment. For example, if the IP address of the primary controller is **129.9.1.21**, the IP address of the console must be changed to **129.9.1.121**.

1. Run the following command on the console:

   ```
   # telnet IP_address_of_the_primary_controller
   ```

   A message similar to the following will be displayed:

   ```
   login:
   ```

2. Enter the user name **eis-installer**.

   A message similar to the following will be displayed:

   ```
   password:
   ```

3. Enter the password of user **eis-installer**.
4. Run the following command to exit the connection to the primary controller:

   ```
   XSCF> exit
   ```

   If installation engineers cannot log in to the network management port (NET MGT), check the network cable and the IP address settings on the console. If the problem persists, configure the server through the serial port cable of the local console again.

25 **Optional:** Perform the following to test the connection of the network management port of the secondary controller.

TIP

- The port of the secondary controller on the M4000 server is on the left.
- Before the test, the console must communicate properly with the secondary controller on the M4000 server. If the console is directly connected to the secondary controller of the M4000 server by a network cable, you must change the IP address of the console to ensure that the IP addresses of the console and the secondary controller are on the same network segment. For example, if the IP address of the primary controller is **129.9.2.21**, the IP address of the console must be changed to **129.9.2.121**.

1. Run the following command on the console:
   ```
   # telnet IP_address_of_the_secondary_controller
   ```
   A message similar to the following will be displayed:
   ```
   login:
   ```
2. Enter the user name **eis-installer**.
   A message similar to the following will be displayed:
   ```
   password:
   ```
3. Enter the password of user **eis-installer**.
4. Run the following command to exit the connection to the primary controller:
   ```
   XSCF> exit
   ```
   If you cannot log in to the network management port (NET MGT), check the network cable and the IP address settings on the console. If the problem persists, configure the server through the serial port cable of the local console again.

26 Disconnect the serial port of the system controller from the HyperTerminal. Configuration is complete.

----End

4.2 Configuring Controller IP Addresses for Disk Arrays

This topic describes how to configure controller IP addresses for the OceanStor S2600, and StorageTek 2540 disk array.

4.2.1 Configuring the SC IP Address of the OceanStor S2600 Disk Array
This topic describes how to configure the SC IP address of OceanStor S2600 disk array.

4.2.2 Configuring the SC IP Address of the StorageTek 2540 Disk Array
This topic describes how to configure SC IP address of the StorageTek 2540 disk array.

4.2.1 Configuring the SC IP Address of the OceanStor S2600 Disk Array

This topic describes how to configure the SC IP address of OceanStor S2600 disk array.

Prerequisite

- The controller IP addresses are obtained.
- The power cable of the disk array is connected.

Context

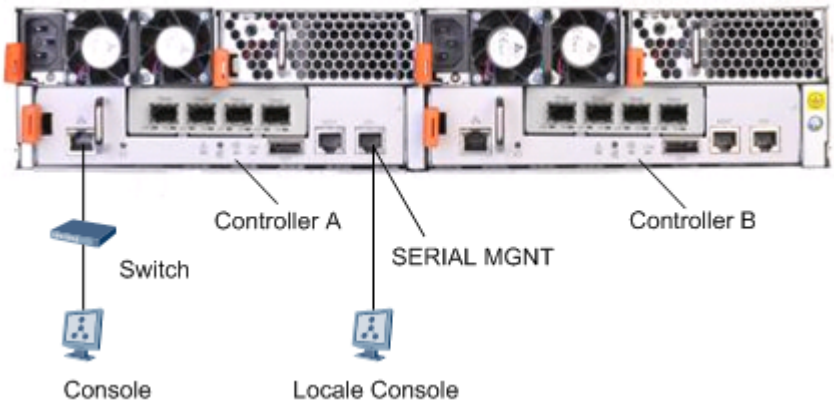
Each OceanStor S2600 disk array has two controllers that need to be configured with management interfaces separately.

Procedure

1 Connect the computer and controller A of the disk array physically.

Use a serial port cable (DB9-RJ45) to connect the serial port of the local controller to the serial port of the disk array (SERIAL MGT).

Use an RJ-45 connector at one end of the serial port cable to connect to the serial port of the disk array (SERIAL MGT) and a DB-9 connector at the other end of the cable to connect to the serial port of the computer (COM1 or COM2).



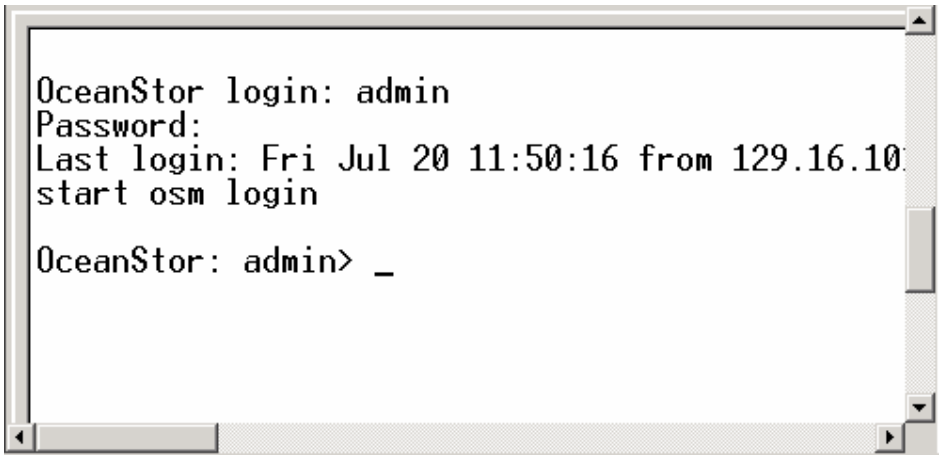
2 Set up a logical connection between the computer and controller A.

1. Start the computer and enter Windows OS.
2. Choose **start** > **Programs (P)** > **Accessories** > **Communications** > **HyperTerminal**.
3. In the **Connection Description** dialog box, enter the name of the new connection, such as **NMS**, and click **OK**.
4. In the dialog box that is displayed, select the serial port of the computer that is used to connect to the disk array, such as COM1, and click **OK**.
5. In the dialog box that is displayed, set the attributes of the serial port as follows:
   - Bits per second: 115200 bps
   - Data bits: 8 bit
   - Parity: None
   - Stop bits: 1 bit
   - Flow control: None
6. Click **OK**.

   The following message will be displayed on the Windows management terminal if the connection was established:
   ```
   Login:
   ```
7. Enter the user name and password to log in.

   NOTE

   The default user name and password of the system administrator are **admin** and **123456**.



After login authentication, the system will display the CLI.

3 In the CLI, run the **chgctrlip** command to configure the IP address for the network interface of controller A. See **Table 4-1**.

Table 4-1 Command format and parameter description of the **chgctrlip** command

Command Format	Parameter Description
chgctrlip -c *controller ID* { **-a** *IP address* | **-s** *subnet mask* | **-g** *gateway* }	● **-c** *controller ID*: Indicates the controller ID. The value of this parameter is **a** or **b**, where, **a** represents controller A and **b** represents controller B. ● **-a** *IP address*: Indicates the IP address of the management network interface of the controller. ● **-s** *subnet mask*: Indicates the subnet mask. ● **-g** *gateway*: Indicates the gateway.

The following is an example:

Configure the IP address for the management network interface of controller A. Specifically, the IP address is *129.9.1.10*, the subnet mask is *255.255.255.0*, and the gateway IP address is *129.9.1.254*. Run the following command:

```
OceanStor: admin> chgctrlip -c a -a 129.9.1.10 -s 255.255.255.0 -g 129.9.1.254
```

4 Disconnect the serial port from controller A.

1. In the CLI, run the **logout** command.
2. On the computer, exit the HyperTerminal software.
3. Remove the serial port cable on the disk array.

5 Repeat Step 1 to Step 4 to configure the network interface of controller B.

1. Connect the computer and controller B physically.
2. Establish a logical connection between the computer and controller B.
3. Configure the IP address of the network interface of controller B on the local console.

TIP

Run the **showctrlip** command to query the IP address of the management network interface of a controller after the **chgctrlip** command. Table 4-2 provides the format and parameter description of the **showctrlip** command.

Table 4-2 Command format and parameter description of the **showctrlip** command

Command Format	Parameter Description
showctrlip [**-c** *controller ID*]	● **-c** *controller ID*: Indicates the controller ID. The value of this parameter is **a** or **b**, where, **a** represents controller A and **b** represents controller B.

Precautions for running the **showctrlip** command are as follows:

- Run the **showctrlip** command to query the IP addresses of the management network interfaces of all controllers.
- Run the **showctrlip -c** *controller ID* command to query the IP address of the management network interface of a specified controller.

The following is an example for querying the IP addresses of the management network interfaces of all controllers:

```
OceanStor: admin> showctrlip
  Controller  IP Address       Subnet Mask      Gateway          MAC Address
           A  129.9.1.10     255.255.255.0      0.0.0.0
00:12:34:56:70:46
           B  129.9.1.11     255.255.255.0      0.0.0.0
00:12:34:56:79:92
```

6 Disconnect the serial port from controller B.

1. In the CLI, run the **logout** command.
2. On the computer, exit the HyperTerminal software.
3. Remove the serial port cable on the disk array.

----End

4.2.2 Configuring the SC IP Address of the StorageTek 2540 Disk Array

This topic describes how to configure SC IP address of the StorageTek 2540 disk array.

Prerequisite

- The controller IP addresses are obtained.
- The power cable of the disk array is connected.

Context

Each StorageTek 2540 disk array has two controllers that need to be configured separately.

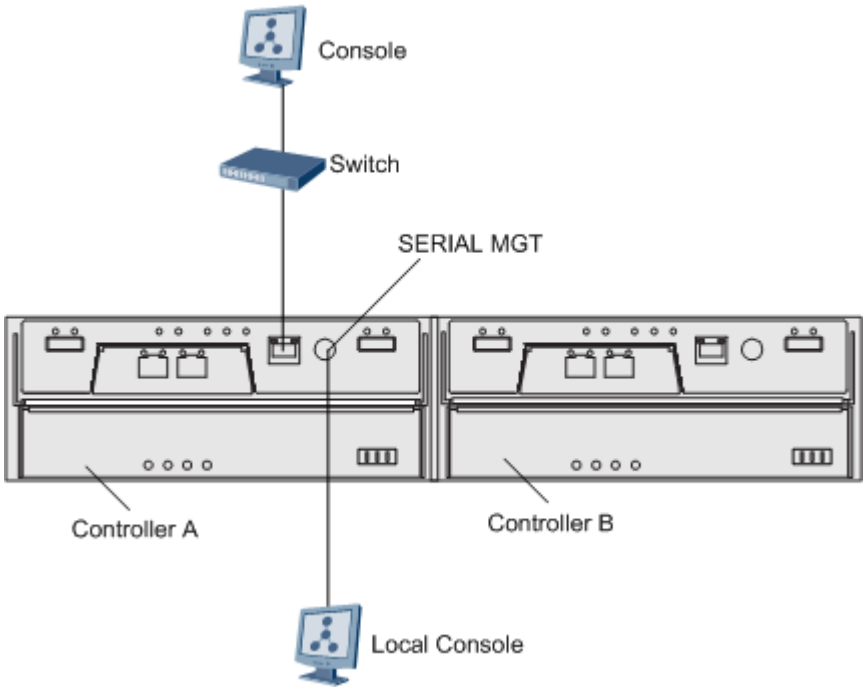
Procedure

1 Connect the computer and controller A of the disk array physically.

Use a serial port cable (DB9-PS/2) to connect the serial port of the local controller to the serial port of the disk array (SERIAL MGT).

Use a PS/2 connector at one end of the serial port cable to connect to the serial port of the disk array (SERIAL MGT) and a DB-9 connector at the other end of the cable to connect to the serial port of the computer (COM1 or COM2).

Figure 4-3 Connections between the local console and the controller on the StorageTek 2540 disk array



2 Set up a logical connection between the computer and controller A.

1. Start the computer and enter Windows OS.
2. Choose **start** > **Programs (P)** > **Accessories** > **Communications** > **HyperTerminal**.
3. In the **Connection Description** dialog box, enter the name of the new connection, such as **NMS**, and click **OK**.
4. In the dialog box that is displayed, select the serial port of the computer that is used to connect to the disk array, such as COM1, and click **OK**.
5. In the dialog box that is displayed, set the attributes of the serial port as follows:
   - Bits per second: 38400 bps
   - Data bit: 8 bit
   - Parity check: none
   - Stop bit: 1 bit
   - Data flow control: none
6. Click **OK**.

3 Configure the IP address of the network interface of controller A of the disk array on the local console.

NOTE

Each StorageTek 2540 disk array has two controllers that need to be configured separately.

1. Send a break signal from the computer by pressing **Ctrl+Pause Break**.

```
Press within 5 seconds: <S> for Service In press <space> within 5 seconds
Baud rate set to 38400
```

2. Enter **S** to open the service window.

```
03/28/08-05:21:18 (GMT) (utlTimer): WARN:  Extended Link Down Timeout on
channel 2
03/28/08-05:21:18 (GMT) (utlTimer): WARN:  Extended Link Down Timeout on
channel 3
Current date: 03/28/08  time: 05:22:11
Enter Password to access Service Interface (60 sec timeout):
```

3. Enter a password. Enter the default password **kra16wen** to access the disk array if the configuration is being performed for the first time.

NOTE

In the default password, **1** is the number one and not the letter **l**.

```
->
Service Interface Main Menu
===========================

 1) Display IP Configuration
 2) Change IP Configuration
 3) Reset Storage Array (SYMbol) Password
 Q) Quit Menu

    Enter Selection:
```

4. Enter **2** to set the IP address of the first controller.

```
Enable IPv4? (Y/N):
```

5. Enter **y** to enable IPv4.

```
Configure using DHCP? (Y/N): n
```

6. Enter **n** to disable DHCP.

```
    Press '.' to clear the field;
    Press '-' to return to the previous field;
    Press <ENTER> and then ^D to quit (Keep Changes)

                          Current Configuration   New Configuration
IP Address         if0  :
Subnet Mask        if0  :
Gateway IP Address if0  :
```

7. Enter the IP address, subnet mask, and gateway IP address of the controller.

```
The IP Configuration is getting changed to:

IP Address          : IP address of the controller
Subnet Mask         : Subnet mask of the controller
Gateway IP Address  : Gateway IP address of the controller

Are you sure that you want to change IP Configuration ? (Y/N): y
```

8. Enter **y** if you want to modify the IP address.

```
Network Configuration successfully changed.

Enable IPv6? (Y/N):
```

9. Enter **n** to disable IPv6.

```
Change port configuration (speed & duplex) ? (Y/N):
```

10. Enter **n** so that the port configuration will not be modified.

```
Reboot to have the settings take effect? (Y/N)
```

11. Enter **y** to restart the system and make the configuration take effect.

```
...
Send <BREAK> for Service Interface or baud rate change
```

4 Disconnect the serial port cable from controller A.

1. On the computer, exit the HyperTerminal software.
2. Remove the serial port cable on the disk array.

5 Repeat Step 1 to Step 4 to configure the network port of controller B.

1. Establish a physical connection between the computer and controller B.
2. Establish a logical connection between the computer and controller B.
3. Configure the IP address of the network interface of controller B on the local console.
4. Disconnect the serial port from controller B.

----End

5 Powering On a Server

This topic describes how to power on a server. The T5220 server, M4000 server, and disk array are taken as examples to show how to power on a server according to the server type and disk array type.

T5220 Server

1. Connect the power supply to a T5220 server.
2. Wait for 2 to 3 minutes until the indicator on the front of the server turns on. Press the power button of the T5220 server to start it.

   NOTE

   The power button is on the left of the server's front panel. It is labeled with , as shown in the following figure.

Figure 5-1 Power button of the T5220 server

NOTE

- The server will display an **OK** prompt if a Solaris OS has not been installed on it.
- The server will automatically start a Solaris OS after power-on if the OS has been installed on it. Enter **boot** to start a Solaris OS manually if the server displays an **OK** prompt.

M4000 Server

1. Connect the power supply to an M4000 server.
2. Insert the key delivered with the server into the key slot in the front panel of the M4000 server, and then turn the switch to the **Service** position labeled with  , as shown in the following figure.

   Figure 5-2 Power button of the M4000 server

3. Press the power button of the server. The switch is labeled with  . The server starts and then operates diagnosis.

   NOTE

   - Ensure that the green LED power indicator on the operation panel is on.
   - If the server has not been installed with a Solaris OS, the server accesses the OK prompt state.
   - If the server has been installed with a Solaris OS, the server automatically starts the Solaris OS after power-on. If the server does not automatically start the Solaris OS but accesses the OK prompt state, enter **boot** to start the Solaris OS manually.

4. After the server is started, turn the rotary switch to the **Locked** position labeled with  .

Disk Arrays

CAUTION

- Ensure that main power switch of the rack and the power switch of the UPS module are off before powering on the system.
- Do not pull out or plug in disk modules, controllers, fibers, network cables, or serial cables when powering-on the disk to avoid loss of data.
- Do not disconnect or connect to the power supply while the disk is saving data. This is to prevent the disk from being damaged losing data. Wait for at least 1 minute before reconnecting the power supply once it has been disconnected.

1. Connect the power supply to the disk array.
2. Switch the two power buttons on the back to the ON position.

6 Installing a Solaris 10 OS Using a Quick Installation DVD

This topic describes how to install a Solaris 10 OS for the primary and secondary sites using a quick installation DVD.

Prerequisite

- The quick installation DVD U2000***version***_server_os_solaris_SPARC_sun4v_dvd2 or U2000***version***_server_os_solaris_SPARC_sun4u_dvd1 is available.

  NOTE

  - Ensure that the quick installation DVD U2000***version***_server_os_solaris_SPARC_sun4v_dvd2 is available if the hardware type of the selected server is sun4v (the T5220 server for example).
  - Ensure that the quick installation DVD U2000***version***_server_os_solaris_SPARC_sun4u_dvd1 is available if the hardware of the selected server is sun4u (the M4000 server for example).

  Installation engineers can run the **uname -m** command to view the hardware type of a server after logging in to the server OS as user **root**.
- Obtain the following information:
  - Host name
  - Network interface
  - System IP address
  - Subnet mask
  - Default Route IP address
- The IP address of the system controller is configured. For details about how to configure the IP address, see **4.1 Configuring Controller IP Addresses for Workstation**.

Context

CAUTION

The operations mentioned in this topic must be performed on all the servers of the primary and secondary sites.

If no quick installation DVD is available on site, manually install an OS using the Solaris installation DVD delivered along with equipment. For details about how to manually install an OS, see **F Manually Installing the Solaris OS and Its Patches**.

Procedure

1. **Optional:** If the quick installation DVD is used to install two or more servers, remove network cables from the system network interfaces of the servers and only keep network cables connected to network interfaces corresponding to system controllers for the purpose of installing Solaris OS.
2. **Optional:** If the T5220 server is used, perform the following operations to display the **OK** prompt:
   1. Log in to the system controller in SSH mode.

      NOTE

      The T5220 server does not support login through Telnet. Log in to the system controller performing the following:

      - Install the tool software of the SSH client on the Windows terminal to log in to the system controller, for example: **Putty**.
      - Run the **ssh** *SC_IP_Address* command on the terminals of other Sun servers. If the following message is displayed, enter **yes**:
        ```
        The authenticity of host '129.9.1.20 (129.9.1.20)' can't be
        established.
        RSA key fingerprint is 0b:23:07:0c:27:72:44:3f:d1:aa:12:99:ed:dd:c0:5a.
        Are you sure you want to continue connecting (yes/no)?
        ```
   2. In the CLI, enter the user name and password of the system controller. The default user name and password are **root** and **changeme**.
   3. Enter **set /HOST/bootmode state=reset_nvram script="setenv auto-boot? false"**.

      NOTE

      There must be a space between **?** and **false**.

      The following message will be displayed:

      ```
      Set 'state' to 'reset_nvram'
      Set 'script' to 'setenv auto-boot? false'
      ```
   4. Enter **start /SYS**.

      The following message will be displayed:

      ```
      Are you sure you want to start /SYS (y/n)?
      ```
   5. Enter **y** to start the T5220.

      The system is running if the following message is displayed:
      ```
      start: Target already started
      ```
      Perform the following operations:

      a. Enter **stop /SYS**.

         The following message will be displayed:

         ```
         Are you sure you want to stop /SYS (y/n)?
         ```

      b. Enter **y**.

         The following message will be displayed:

         ```
         Stopping /SYS
         ```

      c. Enter **show /HOST status** repeatedly to check the system status.

Proceed with the subsequent operations until the following message is displayed:

```
status = Powered off
```

d. Enter **start /SYS**.

The following message will be displayed:

```
Are you sure you want to start /SYS (y/n)?
```

e. Enter **y** to start the T5220.

6. Enter **start /SP/console -f**.

The following message will be displayed:

```
Are you sure you want to start /SP/console (y/n)?
```

7. Enter **y** and press **Enter**.

NOTE

If a prompt is displayed, enter **y** and press **Enter**.

The following message will be displayed:

```
Serial console started.  To stop, type #.
...
Setting NVRAM parameters to default values.


SPARC Enterprise T5220, No Keyboard
Copyright 2008 Sun Microsystems, Inc.  All rights reserved.
OpenBoot 4.28.0, 8064 MB memory available, Serial #85369820.
Ethernet address 0:21:28:16:a3:dc, Host ID: 8516a3dc.


auto-boot? =            false
{0} ok
```

3 Optional: If the M4000 server is used, perform the following to display the **OK** prompt:

1. Log in to the system controller through Telnet. Run the **telnet *Controller IP Address*** command on the controller.

The following message will be displayed:

```
Login:
```

2. Enter **eis-installer** as the user name.

The following message will be displayed:

```
Password:
```

3. Enter the password of user **eis-installer**.

The following message will be displayed:

```
XSCF>
```

4. Enter **showdomainmode -d 0**.

The following message will be displayed:

```
Host-ID             : 8501c2de
Diagnostic Level    : min
Secure Mode         : off (host watchdog: unavailable Break-signal: receive)
Autoboot            : on
CPU Mode            : auto
```

NOTE

If the **Secure Mode** item is in the **on** state, perform the following:

a. Enter **setdomainmode -d 0 -m secure=off**.

The following message will be displayed:

```
Diagnostic Level    :min        -> -
Secure Mode         : on         -> off
Autoboot            : on         -> -
CPU Mode            : auto
The specified modes will be changed.
Continue? [y|n]
```

b. Enter **y**.

The following message will be displayed:

```
configured.
Diagnostic Level    : min
Secure Mode         : off (host watchdog: unavailable Break-signal:
receive)
Autoboot            : on (autoboot:on)
CPU Mode            : auto
```

5. Enter **showdomainstatus -a**.

The following message will be displayed:

```
DID         Domain Status
00          Running
01          -
```

NOTE

If the following message is displayed, run the **poweron -d 0** command:

```
DID         Domain Status
00          Powered Off
01          -
```

Run the **showdomainstatus -a** command repeatedly to check the system status. Proceed with the next step only after the status is displayed as **running**.

6. Enter **sendbreak -d 0**.

The following message will be displayed:

```
Send break signal to DomainID 0? [y|n]
```

7. Enter **y**.
8. Enter **console -d 0 -f**.

The following message will be displayed:

```
Connect to DomainID 0? [y|n]
```

9. Enter **y** and press **Enter**.

```
OK
```

4 Insert the quick installation DVD of the server into the DVD drive of the server.

5 Run the following command at the **OK** prompt to set the OS automatic startup and press **Enter**:

```
ok setenv auto-boot? true
```

NOTE

There must be a space between **?** and **true**.

If the following message is displayed, the configuration is complete:

```
auto-boot? =           true
```

6 Run the following command to configure all network interfaces on the workstation to use different MAC addresses and press **Enter**:

```
ok setenv local-mac-address? true
```

NOTE

There must be a space between **?** and **true**.

If the following message is displayed, the configuration is complete:

```
local-mac-address? =           true
```

7 Run the following command to enable the system to boot from the DVD-ROM and open the single-user installation window. Press **Enter**.

```
ok boot cdrom - install
```

NOTE

There must be a space between **-** and **install**.

Wait about five minutes. The single-user installation window will be displayed.

```
Please select the server mode:
------------------------------------------------------------
 1    Single Server System
 2    High Availability System (Veritas Hot Standby)
------------------------------------------------------------
Please enter [1,2]:
>
```

8 Enter **2** to select the Veritas high availability system. Then, press **Enter**.

```
Please confirm the configuration...
The server mode is as follows:
------------------------------------------------------------
2 High Availability System (Veritas Hot Standby)
------------------------------------------------------------
Enter 'y' to apply the configuration and proceed to the next stage of the
restoration, or 'n' to return and make changes (y/n):
>
```

9 Confirm the configurations. Enter **y** and press **Enter**.

```
All the selections are confirmed.
If the server will use a disk array:
------------------------------------------------------------
 1    Yes
 2    No
------------------------------------------------------------
Please enter [1,2]:
>
```

10 Enter **1** or **2** according to conditions at your site. For example, if a disk array is not connected, select **2**.

```
The choice is as follows:
------------------------------------------------------------
 2    No
------------------------------------------------------------
Enter 'y' to apply the configuration and continue the
restoration, or enter 'n' to return and make changes (y/n):
>
```

11 Ensure that the configurations are correct. Enter **y** and press **Enter**.

```
Please select a language for the server:
------------------------------------------------------------
 1    English (C)
 2    Chinese (zh_CN.GB18030)
------------------------------------------------------------
Please enter [1,2]:
>
```

NOTE

- If **1** is entered, the English version is automatically selected during installation.
- If **2** is entered, the Chinese version is automatically selected during installation.
- In a high availability (HA) system, select the same language for the primary and secondary sites when restoring system data.

12 Enter **1** and press **Enter**.

```
The language is as follows:
-----------------------------------------------------------------
 1    English (C)
-----------------------------------------------------------------
Enter 'y' to apply the configuration and continue the
restoration, or enter 'n' to return and make changes (y/n):
```

13 Enter **y** after you confirm that the configuration is correct and press **Enter**.

```
Please configure the network information on the server.
Please enter a new hostname for the server:
>
```

14 Enter the planned host name of the server and press **Enter**.

NOTE

If the OS is installed at the primary site, enter the host name planned for the primary site, such as **primaster**; if the OS is installed at the secondary site, enter the host name planned for the secondary site, such as **secmaster**.

```
Please enter a new IP address for the server:
>
```

15 Enter the system IP address of the server and press **Enter**.

NOTE

If the OS is installed at the primary site, enter the system IP address of the primary site; if the OS is installed at the secondary site, enter the system IP address of the secondary site.

```
Please enter a new subnet mask for the server:
>
```

16 Enter the system IP address mask of the server and press **Enter**.

NOTE

If the OS is installed at the primary site, enter the system IP address mask of the primary site; if the OS is installed at the secondary site, enter the system IP address mask of the secondary site.

```
Please enter the default route of the server, or keep the default route blank:
>
```

17 Enter the default gateway of the server and press **Enter**.

NOTE

If the OS is installed at the primary site, enter the default gateway address of the primary site; if the OS is installed at the secondary site, enter the default gateway address of the secondary site.

```
Confirm the configuration of the server.
The configuration of the server is as follows:
-----------------------------------------------------------------
          Hostname             Primaster
          IP address            129.9.1.1
          Netmask               255.255.255.0
          Default route         129.1.1.254
-----------------------------------------------------------------
Enter 'y' to apply the configuration and continue the
restoration, or enter 'n' to return and make changes [y/n]:
>
```

18 Enter **y** after you confirm that the configuration is correct and press **Enter**.

```
The configuration of the local server is confirmed.
--------------------------------------------------------------------------------
The NICs available in the local server are as follows:
----------------------------------------
             1            e1000g0
             2            e1000g1
             3            e1000g2
             4            e1000g3
             5            nxge0
             6            nxge1
             7            nxge2
             8            nxge3
----------------------------------------
Please enter a number to select the system NIC[1-8]:
>
```

19 Enter **1** or another number to select the correct network interface of the system IP address and press **Enter**.

```
NIC e1000g0 is selected!
Enter 'y' to confirm the selection of NIC e1000g0 and continue,
or enter 'n' to return and make changes [y/n]:
>
```

20 Enter **y** after you confirm that the configuration is correct and press **Enter**. The system automatically starts to import data.

NOTE

- The workstation automatically restarts after the system data is imported.
- If **#** appears after the message "Solaris installation program completed" is displayed, enter **reboot** and press **Enter** to restart the OS.
- It takes about 60 minutes to import the system data from the DVD to the workstation. The time required depends on the workstation model.
- If the **Configure Keyboard Layout** window is displayed, press **F2** to continue.

21 Log in to the Solaris OS as user **root**.

NOTE

- The default login password is **root**.
- By default, the system enables the **root** user to perform remote login and use the FTP tool.

If login to Solaris OS as user **root** is possible, Solaris OS is successfully installed. Otherwise, install the OS again.

22 Run the following command to eject the DVD:

```
# eject
```

----End

Follow-up Procedure

- Run the following command to view the version of the system:

  ```
  # uname -rv
  ```

  Information similar to **5.10 Generic_141414-07** is displayed. Here, **5.10 Generic_141414-07** indicates the patch version of the Solaris 10(10/08) OS.

  If the patch version is **5.10 Generic_141414-07**, the OS and patches are successfully installed. Otherwise, refer to this topic to reinstall the OS and its patches.

- After the OS installation is completed by using the quick installation CD-ROM, the default time zone is **PRC**. The local time and time zone can be changed as required. For details, see **B.1.4.2 How to Change the System Time and Time Zone of Solaris OS**.

7 Installing the U2000 Software

About This Chapter

This topic describes how to install the U2000 software on the primary and secondary sites. You must start the U2000 installation program after the U2000 is preconfigured using a DVD or software package.

7.1 Preparing Software Packages

This topic describes how to upload and decompress software packages. Software packages must be uploaded to the server and then decompressed if the software packages are used to install the U2000. If the U2000 is installed by using DVD-ROMs, skip this operation.

Context

The U2000 can be installed by using software packages or installation DVDs. To install the U2000 by using software packages, perform the following operations to upload software packages to the server and then decompress them.

CAUTION

- Do not download the U2000***version***_client_solaris_SPARC.tar software package. Decompressing the U2000***version***_client_solaris_SPARC.tar and the following software packages into the same directory will cause the U2000 installation to fail.
- All software packages must be uploaded to the specified directories at the primary and secondary sties.

Procedure

1 Upload all software packages except the Veritas software to the **/opt/install** path on the server and then decompress them.

1. Log in to the Solaris OS as the **root** user.
2. Run the following command to create the **/opt/install** directory:

   ```
   # mkdir /opt/install
   ```

3. Do as follows to upload the software packages using FTP in bin mode to the **/opt/install** directory on the server:

   NOTE

   The software packages to be uploaded are as follows:

   - Veritas patch: U2000***version***_server_veritas5-1_patch_solaris_SPARC.tar or U2000*Version*_server_veritas5-0_patch_solaris_SPARC.tar
   - Database software: U2000***version***_server_db_solaris_SPARC.tar
   - Basic components: U2000***version***_server_nmsbase_solaris_SPARC.tar
   - Core components: U2000***version***_server_nmscore_solaris_SPARC.tar
   - Components of the transport domain (Select it if you want to manage transport or PTN equipment): U2000***version***_server_nmstrans_solaris_SPARC.tar
   - Components of the IP domain (Select it if you want to manage routers, switches, or security equipment): U2000***version***_server_nmsip_solaris_SPARC.tar
   - Components of the access domain (Select it if you want to manage access equipment): U2000***version***_server_nmsaccess_solaris_SPARC.tar
   - StorageTek 2540 disk array manager CAM (Select it when you configure the StorageTek 2540 disk array): U2000***version***_server_ospatch_solaris_SPARC.tar

   a. Log in to the PC where the software packages reside.

b. Choose **Start** > **Run**. Then, enter **ftp *the_system_IP_address_of_server*** and click **OK**. The FTP connection is set up and the CLI is displayed.

c. Enter **root** as the user name of the server.
```
User (IP Address:(none)):root
```

d. Enter the password of the **root** user.
```
Password:
```

e. Set the FTP transmission mode to **bin**.
```
ftp> bin
```

f. Enter the path where the software packages are stored on the PC.
```
ftp> lcd the_path_of_PC
```

g. Enter the **/opt/install** directory.
```
ftp> cd /opt/install
```

h. Run the **put** command to upload all required software packages to the server:
```
ftp> put Name_of_software_package
```
For example, put U2000***version***_server_nmscore_solaris_SPARC.tar.

Wait for a moment. When the software packages are uploaded, the system prompts **Transfer complete**.

CAUTION

Upload all of the needed software packages to the server.

i. Run the following command to exit from FTP:
```
ftp> quit
```

4. Run the following commands to switch to the directory where the software packages reside, and then run the **tar** command to decompress the uploaded software packages on the server.

CAUTION

Decompression of the Veritas patch package must comply with the following rules:

- If the used Veritas software is Veritas 5.1, decompressing the Veritas patch package is optional. It is recommended that the Veritas patch package not be decompressed.
- If the used Veritas software is Veritas 5.0, decompressing the Veritas patch package is prohibited.

The other software packages must be decompressed one by one. There is no specific decompression sequence.

```
# cd /opt/install
# tar xvf Name_of_software_package
```

For example, tar xvf U2000***version***_server_nmscore_solaris_SPARC.tar.

5. Run the following command to delete the software packages and release the space used by the software packaged:

CAUTION

The Veritas patch package U2000***version***_server_veritas5-1_patch_solaris_SPARC.tar or U2000V100R002C01_server_veritas5-0_patch_solaris_SPARC.tar cannot be deleted.

```
# rm Name_of_software_package
```

For example, rm U2000***version***_server_nmscore_solaris_SPARC.tar.

2 Do as follows to upload the Veritas software package veritas5.1_solaris.tar.gz to the **/opt/vrtstmp** path on the workstation and then decompress it:

NOTE

If Veritas 5.0 is downloaded, the software package is veritas5.0MP3_solaris.tar.gz.

1. Run the following command to create the **/opt/vrtstmp** directory:
   ```
   # mkdir /opt/vrtstmp
   ```
2. Upload the veritas5.1_solaris.tar.gz file to the **/opt/vrtstmp** directory using FTP in binary mode. For details, see Step 1.
3. Run the following commands to switch to the directory where the software packages reside, and then run the following commands to decompress all of the uploaded software packages:
   ```
   # cd /opt/vrtstmp
   # gzcat veritas5.1_solaris.tar.gz | tar -xvBpf -
   # chmod -R +x *
   ```
4. Run the following command to delete the software packages and release the space used by the software packaged:
   ```
   # rm Name_of_software_package
   ```
   For example, rm veritas5.1_solaris.tar.gz.

----End

7.2 Pre-configuring the U2000

Before starting the U2000 installation program, you must configure the OSs of the primary and secondary sites. Preconfigure the system by using a DVD or software package. The preconfiguration process involves copying installation files from the DVD or decompressed software package, generating the HWICMR script, modifying system parameters by using the HWICMR script, installing Veritas-related software and patches, encapsulating disks, creating disk volumes, configuring disk arrays, and configuring disk mirroring.

Prerequisite

- The installation software has been prepared. For more information, see **7.1 Preparing Software Packages**.
- The hardware is properly connected. For more information, see .
- Installation engineers are familiar with the IP address planning scheme of the U2000. For more information, see **3.4 Collecting Installation Information**.
- The primary and secondary power supplies of the disk array have been powered on. For more information, see **5 Powering On a Server**.
- IP addresses have been assigned to disk array controllers if automatic disk array configuration by means of the HWICMR is required.

- For information about how to configure the SC IP of OceanStor S2600 disk array, see **4.2.1 Configuring the SC IP Address of the OceanStor S2600 Disk Array**.
- For information about how to configure the SC IP of OceanStor S3100 disk array, see **H.3.1 Configuring the SC IP Address of the OceanStor S3100 Disk Array**.
- For information about how to configure the SC IP of StorageTek 2540 disk array, see **4.2.2 Configuring the SC IP Address of the StorageTek 2540 Disk Array**.

Context

CAUTION

- Configure the OSs on the servers of the primary and secondary sites.
- Do not adjust the size of the CLI when performing the operations described in this topic.

The topic mainly describes the following configurations:

- Modify service network settings, including the server IP address, server host name, and IPMP feature.
- Install the Veritas software and patches.
- Configure disk mirroring.
- Configure disk arrays. Check whether disk arrays are automatically connected to the server. If no, connect the disk arrays with the server.

A scenario where the disk array is mounted is mainly described in this section, while a scenario where a disk array is not mounted is also addressed.

Procedure

1. Log in to the OS as user **root**.
2. Start copying software.
   - **Mode one**: If installation is performed using a DVD, do as follows:
     1. Insert the installation DVD of the U2000 server software into the server DVD-ROM.
     2. Run the following commands to switch to the directory where the **pre_install.sh** file is stored and run the **pre_install.sh** file to start copying software:

        ```
        # cd /cdrom/cdrom0/engineering/HWICMR
        # . ./pre_install.sh
        ```

        NOTE

        There must be a space between the dot (.) and the command **./pre_install.sh**.

        It takes approximately five minutes to complete system pre-configuration. The pre-configuration includes copying the HWICMR, Network Management System Maintenance Suite, and Java environment.

        - Path for the Java environment variable: /opt/HWNMSJRE
        - Path for the NMS maintenance suite: /opt/HWENGR
        - HWICMR path: /opt/HWICMR

        A message similar to the following will be displayed:

```
==========================================
 System pre-configuration
==========================================
...
...
==========================================
Cannot find database installation package.
Please insert the installation CD #3, or extract database compress package
to /opt/install, or input another path that contains a database installation
package, then press Enter key to continue
```

3. The DVD-ROM will eject the installation DVD for the U2000 server software after configuration is complete. Insert the installation DVD for the database software into the server DVD-ROM.

   The system will automatically copy the database installation software to the server.

   A message similar to the following will be displayed:

   ```
   Deal with Database installation file to /opt/install...
   > Finish
   If install High Availability NMS System (Veritas Hot Standby), input "1" to
   start deal with Veritas installation software.
   If no need, input "2" to skip
   ```

4. Enter **1** to copy the Veritas software.

   A message similar to the following will be displayed:

   ```
   Start deal with Veritas software  ...
   Can not find Veritas installation file.
   Please insert the Veritas CD, or extract veritas compress package to /opt/
   vrtstmp, or input another path that contains veritas installation file, then
   press Enter key to continue
   ```

5. The DVD-ROM automatically ejects the installation DVD of the database software. Insert the installation DVD of the Veritas software into the DVD-ROM of the server, and then press **Enter**. The process takes about five minutes. Wait patiently.

   A message similar to the following will be displayed:

   ```
   Deal with Veritas installation file to /opt/vrtstmp  ...  > Finish

   Can not find Veritas patch package file.
   Please insert the Veritas patch DVD or extract Veritas patch compress
   package to /opt/vrtstmp, or input another path that contains Veritas patch
   file , then press Enter to continue
   ```

6. The DVD-ROM automatically ejects the installation DVD of the Veritas software. Insert the installation DVD of system patches into the DVD-ROM of the server, and then press **Enter**.

   A message similar to the following will be displayed:

   ```
   Configure OS successful...
   Finish...
   ```

7. Run the following commands to eject the DVD.

   ```
   # cd /
   # eject
   ```

- **Mode two**: If installation is performed using a software package, do as follows:

  1. Run the following commands to switch to the directory where the **pre_install.sh** file is stored and run the **pre_install.sh** file to start copying software:

     ```
     # cd /opt/install/engineering/HWICMR
     # ./pre_install.sh
     ```

  2. It takes approximately five minutes to complete system pre-configuration. The pre-configuration includes copying the HWICMR, Network Management System Maintenance Suite, and Java environment.

- Path for the Java environment variable: /opt/HWNMSJRE
- Path for the NMS maintenance suite: /opt/HWENGR
- HWICMR path: /opt/HWICMR

A message similar to the following will be displayed:

```
==========================================
 System pre-configuration
==========================================
...
...
==========================================
Skip copy Database software  ...
If install High Availability NMS System (Veritas Hot Standby), Input "1" to
start copy Veritas installation software.
If no need, input "2" to skip
```

3. Enter **1** to copy the Veritas software.

   A message similar to the following will be displayed:

CAUTION

In the scenario where installation is performed using a software package, obtain the software package from the **/opt/install** directory of the server. If the following information is displayed, it indicates that the OS has been configured successfully.

```
Start deal with Veritas software  ...
Find exist Veritas in "/opt/vrtstmp". Skip deal with Veritas installation
package.
Start deal with Veritas software's patches  ...
Deal with Veritas software's patches finished
> Finish

==========================================
Solaris patch 9.0.1 is already installed. Skip patch install.

==========================================
 * NMS Engineering Directory  : /opt/HWENGR
 * NMS Software Lib Directory : /opt/install/
 * NMS Java Runtime Environment : /opt/HWNMSJRE/jre_sol


Configure OS successful...
Finish...
```

3 Ensure that the language environment variable of the system is **C**.

Run the following command to check the language environment variable of the system:

```
# echo $LANG
```

If **C** is not displayed, change the language environment variable description in the **/etc/TIMEZONE** file to **LANG=C**, and then restart the system. Perform the following steps:

NOTE

The language environment variable **C** of the OS indicates that the system language is English.

1. Run the following commands to change the language environment variable description in the **/etc/TIMEZONE** file.

```
# cd /opt/HWICMR/tools
```

```
# ./ChangeLanEnv.sh
```

A message similar to the following will be displayed:

```
Getting the current working directory...
Working directory: /opt/HWICMR/tools
The current language is "zh_CN.GB18030", Do you really want to change? [y or n]
```

2. Enter **y** and press **Enter**.

   A message similar to the following will be displayed:

   ```
   Please enter the language you want to change!
   ```

3. Enter **C** and press **Enter**.

   A message similar to the following will be displayed:

   ```
   You input is C. Press Y to confirm!
   ```

4. Enter **Y** and press **Enter**.

   A message similar to the following will be displayed:

   ```
   Success to update, please restart the system to take effect!
   ```

5. Run the following commands to restart the OS:

   ```
   # sync;sync;sync;sync
   # shutdown -y -g0 -i6
   ```

4 **Optional:** If disk arrays are installed, perform this step. Otherwise, skip this step.

NOTE

- The OceanStor S2600 disk array (6 x 300 GB) and the StorageTek 2540 disk array (6 x 300 GB) support automatic configuration by means of the **HWICMR**. To use disk arrays that do not support automatic configuration, contact Huawei engineers.
- The OceanStor S3100 disk array does not support automatic script configuration. For details about how to configure the OceanStor S3100 disk array, see **H.3.2 Using the Manager Suite to Configure the OceanStor S3100 Disk Array**.

To configure the OceanStor S2600 disk array by using an automatic configuration script, perform the following operations:

1. Run the following commands to switch to the directory where the script for configuring the OceanStor S2600 disk array is stored, and run the **AutoSetupS2600.sh** script to start configuring the OceanStor S2600 disk array:

   ```
   # cd /opt/HWICMR/bin/array
   # ./AutoSetupS2600.sh
   ```

   A message similar to the following will be displayed:

   ```
   Please enter the username of the array.
   ```

2. Enter the user name of the disk array and press **Enter**. The default user name is **admin**.

   A message similar to the following will be displayed:

   ```
   Please enter the password of the disk array.
   ```

3. Enter the user password of the disk array and press **Enter**. The default password is **123456**.

   A message similar to the following will be displayed:

   ```
   Please enter the IP address of array controller A.
   ```

4. Enter the IP address of the primary controller of the disk array, such as *129.9.1.10* and press **Enter**.

   A message similar to the following will be displayed:

   ```
   Are you sure to continue? [y/n]
   ```

5. Enter **y** and press **Enter**. The script clears the configurations of the disk array.

   ```
   Configured the disk array successfully.
   ```

NOTE

Wait about five minutes. The configuration result will be displayed. If the configuration fails, run the **AutoSetupS2600.sh** script again. If the configuration fails again, use the ISM to configure the OceanStor S2600 disk array. For more information, see **H.1 Configuring the OceanStor S2600 Disk Array by Using the ISM**.

6. Run the following commands to restart the OS:
```
# sync;sync;sync;sync
# shutdown -y -g0 -i6
```

To configure the StorageTek 2540 disk array using the automatic configuration script, perform the following operations:

1. Install the CAM. For details, see Step 1 in **H.2 Configuring the StorageTek 2540 Disk Array Through the Web Browser**.
2. Run the following commands to navigate to the directory where the script for configuring the StorageTek 2540 disk array is stored. Run the **AutoSetup2540.sh** file to start configuring the StorageTek 2540 disk array:
```
# cd /opt/HWICMR/bin/array
# ./AutoSetup2540.sh dmp
```
   A message similar to the following will be displayed:
```
Please input "y" to go on or "n" to quit:
```
3. Enter **y** and press **Enter**.
   A message similar to the following will be displayed:
```
Please input the IP address of the array:
```
4. Enter the IP address of a disk array controller, such as the IP address of the primary controller *129.9.1.10*, and press **Enter**.
   A message similar to the following will be displayed:
```
Please input the password of user root...
Type your password:
```
5. Enter the password of user **root** of the OS and press **Enter**. The default password is **root**.
   Wait about 10 minutes. The result of the configuration will be displayed. If the configuration fails, run the **AutoSetup2540.sh** script and configure the StorageTek 2540 disk array again. If the configuration fails again, configure the StorageTek 2540 disk array through the Web browser. For more information, see **H.2 Configuring the StorageTek 2540 Disk Array Through the Web Browser**.
   A message similar to the following will be displayed:
```
...
Succeeded to configure disk array!
...
```
6. Run the following commands to restart the OS:
```
# sync;sync;sync;sync
# shutdown -y -g0 -i6
```

5 If Veritas 5.0 is installed, run the following command to change the OS system time to be within the demo license validity period. If Veritas 5.1 is installed, skip this step.
```
# date 092701012006
```

NOTE

The demo license validity period for Veritas must be in the range of 2006–09–25 to 2006–11–25.

Run the following commands to restart the OS:
```
# sync;sync;sync;sync
# shutdown -y -g0 -i6
```

6 Run the following commands to switch to the directory where the HWICMR is stored, and run the **install.sh** script to start the HWICMR for system pre-configuration:

```
# cd /opt/HWICMR/bin
# ./install.sh -r
```

NOTE

If the IPMP has been configured for the network or an incorrect host name or IP address is entered during OS configuration and the network need to be reconfigured, perform the following operations to reconfigure the OS:

1. Press **Ctrl+C** to stop the program for configuring the OS.
2. Run the following commands to restart the OS and clear the network configuration environment:
   ```
   # sync;sync;sync;sync
   # shutdown -y -g0 -i6
   ```
3. Run the following commands to reconfigure the OS:
   ```
   # cd /opt/HWICMR/bin
   # ./install.sh -r
   ```
   The information displayed is different from that displayed after the **install.sh** script is run for the first time. Perform operations by following the prompts and pay attention to the configuration items whose configuration results are **Failed**.

A message similar to the following will be displayed:

```
 ======= Installation Type =======
Select the installation type. The installation wizard will guide
you through the rest of the installation process according
to the installation type you selected.
       1.      Single-Server System (Solaris)
       2.      High Availability System (Solaris)
                     Select[1]:
```

7 Enter **2** to select the high availability system (Veritas hot standby). Then, press **Enter**.

A message similar to the following will be displayed:

```
======= The path of database =======

               Please input the database path, which is a directory used to install
the database software.

                        Please input path or press the Enter key that used the
default directory[/opt/sybase]:
```

8 Enter a database installation directory. Using the default directory is recommended. Then, press **Enter**.

CAUTION

The database installation path may vary according to disk partitions. By default, the database is installed in the **/opt/sybase** path. Do not change the database installation path.

A message similar to the following will be displayed:

```
 ======= The path of NMS =======

                Please input the NMS path which is a directory used to install the
NMS software.

                        Please input path or press Enter key that used the default
directory [/opt/U2000]:
```

9 Enter a U2000 installation directory. Using the default directory is recommended. Then, press **Enter**.

CAUTION

The NMS installation path may vary according to disk partitions. By default, the NMS is installed in the **/opt/U2000** path. Do not change the NMS installation path.

A message similar to the following will be displayed:

```
Trying to backup the current network configurations...

Please input the system ip[129.9.1.1]:
>
```

10 Set IP addresses according to different NIC schemes.

NIC Scheme	Operation
Single scheme	See **Single-NIC Scheme (Recommended)**. 1. Enter a planned system IP address, for example, 129.9.1.1. `Please input the system hostname[primaster]:` 2. Enter a planned host name. For example, enter Primaster when configuring the OS of the primary site or Secmaster when configuring the OS of the secondary site. Here, configuration of the primary site is taken as an example. **CAUTION** To ensure that the NMS can run properly, host name planning must comply with the following rules and restrictions: ● The host name of the U2000 server must be unique on the network. ● The host name must be a string consisting of no more than 24 characters that can only be letters (A to Z), digits (0 to 9) and hyphen (-). ● The first character must be a letter and the last character cannot be a hyphen. ● The host name must be case-sensitive. ● The host name cannot contain any space. ● The host name cannot contain only one character. ● The host name cannot contain **--**. ● The host name cannot be any of the following keywords in the high availability system. `action false keylist static after firm local stop requires remotecluster system group resource global Start str temp set heartbeat ArgListValues System Group boolean hard Name soft before online condition MonitorOnly remote start cluster event VCShm type Path offline Signaled HostMonitor Probed state Cluster IState int Type State VCShmg NameRule ConfidenceLevel` `Please input the system netmask[255.255.254.0]:` 3. Enter a planned subnet mask. `Please input the system default router[129.9.1.254]:` 4. Enter a planned route. `Please confirm the following configurations` 5. Enter **y** to confirm configurations. To modify a configuration, enter **n**. `Will the heart beat network reuse the system network[y/n]?` 6. Enter **y** to set the system network IP address as the heartbeat network IP address. `Do you want to configure the heart beat network service as IPMP [y/n]?` 7. Enter **n** to choose not to configure IPMP. `Will the replicater network reuse the heart beat network[y/n]?` 8. Enter **y** to reuse the heartbeat network as the replication network. `Will the NMS application network reuse the network[y/n]?` 9. Enter **y** to reuse the network as the NMS application network. `======= Select the network type =======` `Please choose one network type to reuse` `1. Reuse the System network` `2. Reuse the Heatbeat network` `Select[1]:`

NIC Scheme	Operation
	10. Select the configurations of any network for reuse. For example, enter **1** to reuse network configurations of the system. Then, press **Enter**.

NIC Scheme	Operation
Double-NIC scheme	See **Double-NIC Scheme (Without IPMP)**. 1. Enter a planned system IP address, for example, 129.9.1.1. `Please input the system hostname[primaster]:` 2. Enter a planned host name. For example, enter Primaster when configuring the OS of the primary site or Secmaster when configuring the OS of the secondary site. Here, configuration of the primary site is taken as an example. **CAUTION** To ensure that the NMS can run properly, host name planning must comply with the following rules and restrictions: ● The host name of the U2000 server must be unique on the network. ● The host name must be a string consisting of no more than 24 characters that can only be letters (A to Z), digits (0 to 9) and hyphen (-). ● The first character must be a letter and the last character cannot be a hyphen. ● The host name must be case-sensitive. ● The host name cannot contain any space. ● The host name cannot contain only one character. ● The host name cannot contain **--**. ● The host name cannot be any of the following keywords in the high availability system. `action false keylist static after firm local stop requires remotecluster system group resource global Start str temp set heartbeat ArgListValues System Group boolean hard Name soft before online condition MonitorOnly remote start cluster event VCShm type Path offline Signaled HostMonitor Probed state Cluster IState int Type State VCShmg NameRule ConfidenceLevel` `Please input the system netmask[255.255.254.0]:` 3. Enter a planned subnet mask. `Please input the system default router[129.9.1.254]:` 4. Enter a planned route. `Please confirm the following configurations` 5. Enter **y** to confirm configurations. To modify a configuration, enter **n**. `Will the heart beat network reuse the system network[y/n]?` 6. Enter **n** to choose not to reuse the system network as the heartbeat network. `Please select a NIC to be used for the master NIC for the heart beat network service ip [1,2,...]:` 7. Enter the serial number of an idle NIC. For example, **2**. `Please input the heart beat network service ip[]:` 8. Enter a planned service IP address of the heartbeat network. `Please input the hostname for the heart beat network service ip [HBService]:` 9. Press **Enter**. `Please input the netmask for the heart beat network service ip [255.255.255.0]:` 10. Enter a planned subnet mask. `Please confirm the following configurations`

NIC Scheme	Operation

(without IPMP)	11. Enter **y** to confirm configurations. To modify a configuration, enter **n**.
	`Do you want to configure the heart beat network service as IPMP [y/n]?`
	12. Enter **n** to choose not to configure IPMP.
	`Will the replicater network reuse the heart beat network[y/n]?`
	13. Enter **y** to reuse the heartbeat network as the replication network.
	`Will the NMS application network reuse the network[y/n]?`
	14. Enter **y** to reuse the network as the NMS application network.
	`======= Select the network type =======`
	`Please choose one network type to reuse`
	`1. Reuse the System network`
	`2. Reuse the Heatbeat network`
	`Select[1]:`
	15. Select the configurations of any network for reuse. For example, enter **1** to reuse network configurations of the system. Then, press **Enter**.

NIC Scheme	Operation
Double-NIC scheme (with IPMP)	See **Double-NIC Scheme (with IPMP)**. 1. Enter a planned system IP address, for example, 129.9.1.1. `Please input the system hostname[primaster]:` 2. Enter a planned host name. For example, enter Primaster when configuring the OS of the primary site or Secmaster when configuring the OS of the secondary site. Here, configuration of the primary site is taken as an example. **CAUTION** To ensure that the NMS can run properly, host name planning must comply with the following rules and restrictions: ● The host name of the U2000 server must be unique on the network. ● The host name must be a string consisting of no more than 24 characters that can only be letters (A to Z), digits (0 to 9) and hyphen (-). ● The first character must be a letter and the last character cannot be a hyphen. ● The host name must be case-sensitive. ● The host name cannot contain any space. ● The host name cannot contain only one character. ● The host name cannot contain **--**. ● The host name cannot be any of the following keywords in the high availability system. `action false keylist static after firm local stop requires remotecluster system group resource global Start str temp set heartbeat ArgListValues System Group boolean hard Name soft before online condition MonitorOnly remote start cluster event VCShm type Path offline Signaled HostMonitor Probed state Cluster IState int Type State VCShmg NameRule ConfidenceLevel` `Please input the system netmask[255.255.254.0]:` 3. Enter a planned subnet mask. `Please input the system default router[129.9.1.254]:` 4. Enter a planned route. `Please confirm the following configurations` 5. Enter **y** to confirm configurations. To modify a configuration, enter **n**. `Will the heart beat network reuse the system network[y/n]?` 6. Enter **y** to set the system network IP address as the heartbeat network IP address. `Do you want to configure the heart beat network service as IPMP [y/n]?` 7. Enter **y** to configure IPMP for the heartbeat network. `Please input the base ip for the heart beat master NIC[]:` 8. Enter a planned IP address for the active NIC of the heartbeat network. `Please input the hostname for the heart beat master base ip [HBMaster]:` 9. Press **Enter**. `Please input the netmask for the heart beat master base ip [255.255.255.0]:` 10. Enter a planned subnet mask. `Please confirm the following configurations`

NIC Scheme	Operation

	11. Enter **y**. To modify a configuration, enter **n**.
	`Please select a NIC to be used for the standby NIC for the heart beat network service ip [1,2,...]:`
	12. Enter a serial number for an idle NIC. For example, **2**.
	`Please input the base ip for the heart beat standby NIC[]:`
	13. Enter a planned IP address for the standby NIC of the heartbeat network.
	`Please input the hostname for the heart beat standby base ip [HBSlave]:`
	14. Press **Enter**.
	`Please input the netmask for the heart beat standby base ip [255.255.255.0]:`
	15. Enter a planned subnet mask.
	`Please confirm the following configurations`
	16. Enter **y** to reuse the heartbeat network as the replication network.
	`Will the NMS application network reuse the network[y/n]?`
	17. Enter **y** to reuse the network as the NMS application network.
	`======= Select the network type =======`
	`Please choose one network type to reuse`
	`1. Reuse the System network`
	`2. Reuse the Heatbeat network`
	`Select[1]:`
	18. Select the configurations of any network for reuse. For example, enter **1** to reuse network configurations of the system. Then, press **Enter**.

Other schemes	Contact Huawei engineers for scheme design.

After the network configuration is compete, information similar to the following is displayed. It takes about 30 minutes to complete the process. Please wait patiently.

```
        Modifying the system
parameters.....................................................................
........
        Installing veritas volume manager
.....................................................................
        Installing veritas extra patches.............................
.....................................................................

Press Enter to restart the computer...
```

The displayed configuration result depends on the configurations of the system network. Watch out for failed configurations.

If **Failed** is returned, the configuration fails. In this case, save the operation log and contact Huawei engineers for fault locating.

11 Press **Enter** to restart the server.

12 After the server is restarted, log in to the OS as the **root** user. Run the following commands in the CLI to navigate to the path where the HWICMR is located and then run the **install.sh** file. It takes about 10 minutes to complete the process. Please wait patiently.

```
# cd /opt/HWICMR/bin
# ./install.sh
```

A message similar to the following will be displayed:

```
        Modifying the system
parameters.....................................................................
........
        Installing veritas volume manager
.....................................................................
        Installing veritas extra patches.............................
.....................................................................
        Encapsuling
diskgroup.....................................................

Press Enter to restart the computer...
```

13 Press **Enter** to restart the server.

14 After the server is restarted, log in to the OS as the **root** user. Then, run the following commands in the CLI to navigate to the path where the HWICMR is located and run the **install.sh** file. It takes about 90 minutes to complete the process. Please wait patiently.

```
# cd /opt/HWICMR/bin
# ./install.sh
```

A message similar to the following will be displayed:

```
    Modifying the system parameters.....................................
    Installing veritas volume
manager.....................................................
    Installing veritas extra
patches.....................................................
    Encapsuling
diskgroup.....................................................
    Create volumes
        It will take 3-5 minute(s) to execute this task. Please wait....
.....................................................................
......
    Mirroring disks
        It will take 30-60 minute(s) to execute this task. Please wait....
.....................................................................
......
    Adding hotspare disk
        It will take 1-2 minute(s) to execute this task. Please wait....
.....................................................................
......
    Configuring the vcs
        It will take 3-5 minute(s) to execute this task. Please wait....
.....................................................................
......

All operations defined in the task flow have been completed.
1 operation logs are saved in:
             /var/ICMR/ICMR_20060925024631.log
```

If **Failed** is returned, the configuration fails. In this case, save the operation log and contact Huawei engineers for fault locating.

After configuring the OS, apply for the formal Veritas license for the related Veritas version as soon as possible.

----End

Follow-up Procedure

If the IPMP has been configured for the network or an incorrect host name or IP address is entered during OS configuration and the network need to be reconfigured, perform the following operations to reconfigure the OS:

1. Press **Ctrl+C** to stop the program for configuring the OS.

2. Run the following commands to restart the OS and clear the network configuration environment:
```
# sync;sync;sync;sync
# shutdown -y -g0 -i6
```
3. Run the following commands to reconfigure the OS:
```
# cd /opt/HWICMR/bin
# ./install.sh -r
```
The information displayed is different from that displayed after the **install.sh** script is run for the first time. Perform operations by following the prompts and pay attention to the configuration items whose configuration results are **Failed**.

7.3 Starting the U2000 Installation Program

This topic describes how to start the U2000 installation program. Install the U2000 software through the GUI (recommended) or CLI. If the GUI cannot be logged in to, install the U2000 software through the CLI.

7.3.1 Installing the U2000 Through the GUI
This topic describes how to install the U2000 software through the GUI. It is recommended that you install the U2000 through the GUI if you are not familiar with the common commands of the Solaris OS.

7.3.2 Installing the U2000 Through the CLI
This topic describes how to install the U2000 software through the CLI. Installation engineers are recommended to install the U2000 through the CLI if they cannot log in to the GUI.

7.3.1 Installing the U2000 Through the GUI

This topic describes how to install the U2000 software through the GUI. It is recommended that you install the U2000 through the GUI if you are not familiar with the common commands of the Solaris OS.

Prerequisite

- If the U2000 is not pre-configured, see **7.2 Pre-configuring the U2000**. The U2000 will fail to install if it is not pre-configured.
- The operation procedure varies according to whether a database is installed on site.

  1. The Sybase database is not reused.

     If the Sybase database is not installed on site or the version of the installed database does not meet requirements, it is recommended that the Sybase database be not reused. The database software is pre-installed on the U2000.

  2. The Sybase database is reused.

     If the database is installed on the server and installation engineers want to use the original database software, ensure that the database is running. For details, see **B.3.1.3 How to Verify That the Sybase Process Is Running** and **B.3.1.2 How to Start the Sybase Database Service**.

     - If the Sybase 12.5 is installed, do not use the original database software.
     - If the Sybase 15.0 is installed, do not use the original database software. In the event that the original Sybase 15.0 software must be used, ensure that the following criteria are met:

(1) The server name of the Sybase database is **DBSVR**. For details, see **B.3.2.7 How to Change the Server Name of the Sybase Database to DBSVR**.

(2) There are not any redundant database items. For details, see **B.3.2.8 How to Delete Redundant Database Items**.

(3) The character set **UTF-8** is configured for the database. For details, see **B.3.2.9 How to Change the Character Set of the Database to UTF-8**.

- Ensure that the size of the installation directory of the server meets the requirement. For example, if all components need to be installed, the remaining space of the installation directory must be larger than 30 GB. It is advisable to install the components of only one product domain if the server is configured with only two 73 GB hard disks.

  TIP

  Run the **df -hk /opt** command to view the remaining space of the **/opt** directory.

- The remote desktop control software is ready.

Context

CAUTION

If the server on which the steps described in this topic must be performed is not specified, perform the steps on the primary and secondary sites.

Any of the following methods can be used to install the U2000:

- **Installation by typical network**: Choose the desired scenario according to the type of the equipment to be managed. The U2000 software provides common scenarios. This method is recommended in situations where the license file is not on-hand.
- **Installation by license**: This method is recommended if the license is on-hand.
- **Custom installation**: This method is applicable to advanced users familiar with managing the network and U2000. This method is also recommended in the event that the license file is on-hand and the common scenarios provided by the U2000 software are insufficient.

Procedure

1. Log in to the **Java Desktop System, Release 3** session of the server OS as user **root** using the remote desktop control software.

   TIP

   - To log in to the **Java Desktop System, Release 3**, perform the following operations: In the login dialog box of the remote desktop control software, choose **Options** > **Session** > **Java Desktop System, Release 3**. Then, set the session to **Java Desktop System, Release 3**.
   - After you log in to the **Java Desktop System, Release 3**, if the **Solaris Registration Wizard** dialog box is displayed, click the **Run the Solaris software without registering** option button and then click **Next**. In the dialog box that is displayed, click **Never Register**.

2. On the desktop, right-click and choose **Open Terminal** from the shortcut menu to display a CLI.

3. Run the following command to check whether the system character set is correct:

   ```
   # locale -a
   ```

   If the following message is displayed, the character set of Solaris OS is correct. Otherwise, reinstall the OS.

```
C
en_US.UTF-8
```

4 Run the following commands to go to the path where the **install.sh** file is stored and run the **install.sh** file:

```
# cd /opt/HWENGR
# ./install.sh
```

Wait about one minute. The **Copyright** dialog box will be displayed.

NOTE

If the U2000 is not pre-configured, the **/opt/HWENGR** directory and the **install.sh** will not be generated and the U2000 cannot be installed.

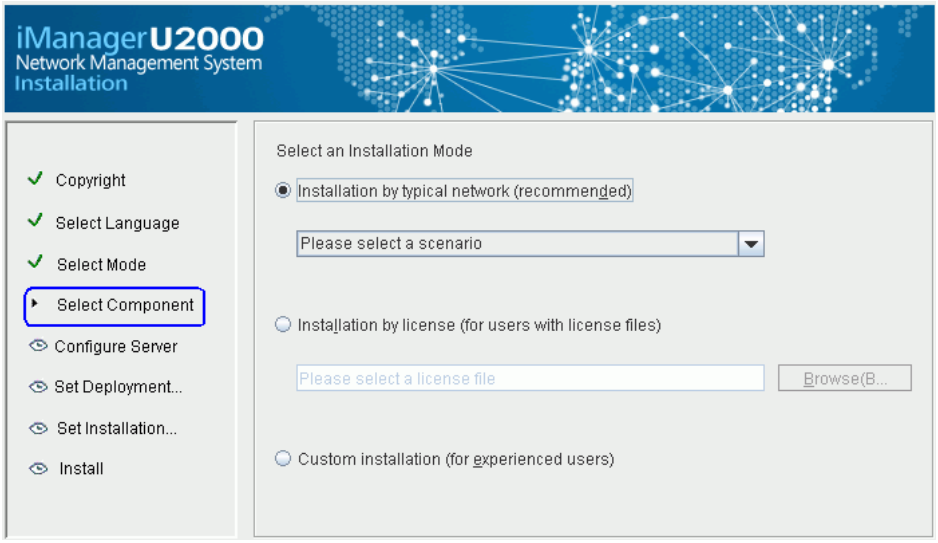
Read the terms of the software license agreement carefully.

5 Click **Accept these terms**, and click **Next** to continue. The **Select Language** dialog box will be displayed.

NOTE

If a dialog box is displayed prompting you to select the directory of the installation package, enter the directory where the installation files were uploaded to the server. For example, **/opt/install**.

6 Select the language according to the conditions at your site, such as **English**. Then, click **Next**. The **Installation Mode** dialog box will be displayed.



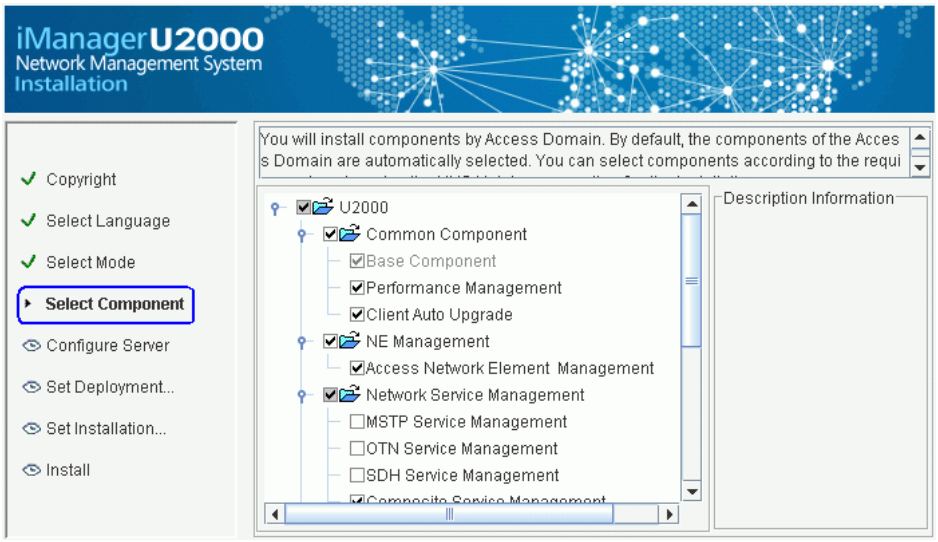
- Select **Installation by typical network**. Then, select a scenario from the drop-down list according to the type of the equipment to be managed.
- Select **Installation by license**. Then, click **Browse** to select the license file that has already been applied for and issued.
- Select **Custom installation**.

NOTE

Any of the following methods can be used to install the U2000:

- **Installation by typical network**: Choose the desired scenario according to the type of the equipment to be managed. The U2000 software provides common scenarios. This method is recommended in situations where the license file is not on-hand.
- **Installation by license**: This method is recommended if the license is on-hand.
- **Custom installation**: This method is applicable to advanced users familiar with managing the network and U2000. This method is also recommended in the event that the license file is on-hand and the common scenarios provided by the U2000 software are insufficient.

7 Click **Next**. The **Component** dialog box will be displayed.



- If you select **Installation by typical network**, the software selects the components to be installed according to the conditions at your site.
- If you select **Installation by license**, the software selects the components to be installed according to the license file.
- If you select **Custom installation**, the software selects the components to be installed according to the type of the equipment to be managed.

CAUTION

Components and instances installed on the primary and secondary sites must be the same.

8 Click **Next**. The **Server** dialog box is displayed.

NOTE

To modify the server parameters, select the server and click **Modify**. Then, modify the server parameters in the dialog box that is displayed.

9 Click **Next**. The **Deployment Parameters** dialog box will be displayed.

NOTE

If the **/opt/U2000** path does not exist, the **Confirm** dialog box will be displayed. Click **Yes** to create the **/opt/U2000** path.

- You can modify the number of instances only for components with **single-server multi-instance**.
- Limited by the port quantity, a maximum number of 25 instances can be deployed for the transport domain in the single-server multi-instance deployment mode.
- To use the CORBA northbound interface (NBI), XML NBI, SNMP NBI, and text NBI, instances must be added by using the Network Management System Maintenance Suite after installing the desired NBIs.

10 Click **Next**. The **Version Style** dialog box will be displayed.

NOTE

The following is an example of the differences between the two styles:

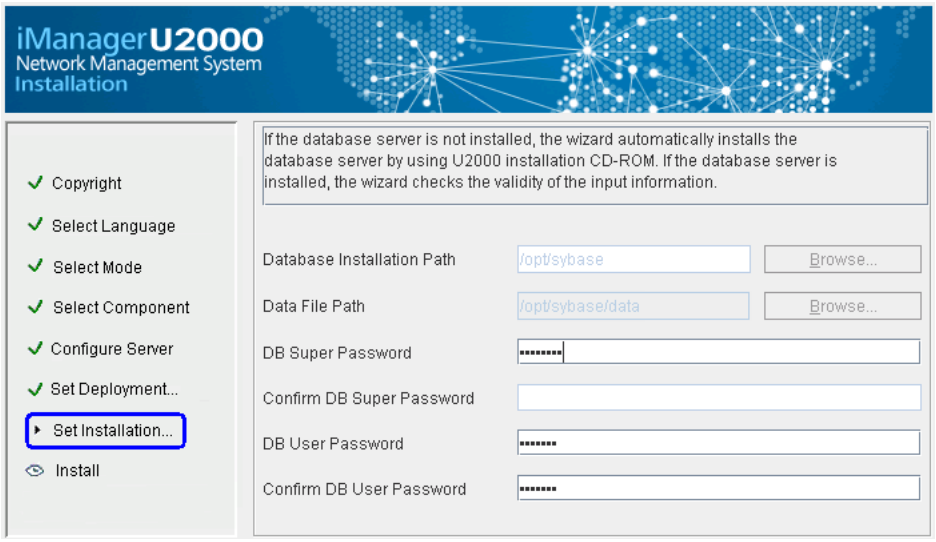
- For the default style, alarms are displayed in the following descending order of severity: **Critical**, **Major**, **Minor** and **Warning**.
- For the North America style, alarms are displayed in the following five levels in descending order of severity: **Critical**, **Major**, **Minor**, **Not Alarmed** and **Not Reported**.

11 Select the style according to the conditions at your site, such as **Default style**. Click **Next**. The **Installation Parameters** dialog box will be displayed.

NOTE

If the components include **SDH Network Element Management** or **SDH Service Management**, the **Version Timeslot Mode** dialog box will be displayed. Select the slot mode according to the conditions at your site, such as **Sequence mode**. Click **Next**.

The **Sequence mode** is the international standard mode and is recommended.



The following table shows the basic settings of the database server and NMS database user.

Parameter	Description
Database Installation Path	Specifies the installation directory of the Sybase database. The default value is **/opt/sybase**. This parameter does not need to be set.
Data File Path	Specifies the path of the data file. The default value is **/opt/sybase/data**. This parameter does not need to be set.

Parameter	Description
Database Superuser Password	Specifies the superuser password of the database. This password can be left blank (not recommended). The password must be 6-30 characters long and consists of letters or digits. Special characters are not allowed. For example, it can be **changeme**. **CAUTION** ● The password of the database superuser at the primary site must be consistent with that at the secondary site. ● If the database is installed, enter the password of the database superuser (this password was set when the database was installed).
Reenter Database Superuser Password	Confirms the password of the database superuser. **NOTE** If the database is installed, you do not need to enter the password of the database superuser.
Database User Password	Specifies the password of the database user. This parameter contains a minimum of six characters. The default value is **NMSuser**. **CAUTION** ● The password of the database user at the primary site must be consistent with that at the secondary site. ● If the database is installed, set the password of the database user (this password was set when the database was installed).
Reenter Database User Password	Confirms the password of the database user.

12 Set the installation parameters and click **Next**. The installation information will be displayed.

NOTE

- If the system prompts you to use the original database software, a database has been installed on the server. If you reuse the database, the installation program will skip database installation. If you do not reuse the database, the installation program will uninstall the existing database and reinstall the database. It is recommended that installation engineers not to reuse the database.
- If the message "Select Installation Package Patch" is displayed, no database installation package is stored in the **/opt/install** directory. In this case, upload database software U2000***version***_server_db_solaris_SPARC.tar to the **/opt/install** directory on the server and decompress it. Set the directory of the installation package to **/opt/install**.

13 Verify that the installation information is correct and click **Next**. A progress bar will be displayed. The time required for the installation depends on the number of components to be installed and the server configuration. The entire process takes about 120 minutes. Wait patiently.

NOTE

- The NMS can automatically expand the capacity of a database according to the growth parameters defined when the database is created. The disk space for installing the database must be greater than the maximum size to which the file is permitted to grow. If the disk space is insufficient, the system will display a prompt message in red. The U2000 can manage up to the maximum of NEs as supported by the server model.
- When the progress bar reaches 99%, the system may wait about half an hour until U2000 installation is complete. This is normal.
- If a message indicating an installation failure or interruption is displayed during installation, perform the following operations to clear the installation environment, and then install the U2000.
  1. Run the following commands to use the environment clean-up tool to clear the installation environment:
     ```
     # cd /opt/HWENGR/engineering/tool
     # ./FailedNMSInstallationClear.sh
     ```
  2. Perform 4 to install the U2000.

14 The system will display a prompt indicating that installation was successfully completed.

15 Click **Finish** to complete the U2000 installation.

16 Run the following commands to stop the VCS service:

```
# cd /opt/VRTSvcs/bin
# hastop -local -force
```

17 Run the following command to verify that the VCS service is stopped:

```
# ps -ef|grep had
```

A message similar to the following will be displayed:

```
root 27663 17299   0 00:31:00 pts/2  0:00 grep had
```

NOTE

If the **had** and **hadshadow** processes are not displayed, the VCS service is successfully stopped; otherwise, run the **kill -9 process ID** command to stop the related processes.

18 Run the following commands to restart the OS:

```
# sync;sync;sync;sync
# shutdown -y -g0 -i6
```

19 Do as follows to set **Disable alarm generation** for **/opt/sybase/data**:

CAUTION

This step needs to be performed only on the primary site.

NOTE

The **/opt/sybase/data** path is used to store database data. In the high availability system, data in this path must be replicated to the secondary site in real time. The database data size is used by default according to the data replication rate and traffic. Therefore, the remaining hard disk space is small, and an alarm is reported on **Hard Disk Monitor** of the System Monitor. This alarm is a normal one and you need to set the monitoring status on **Hard Disk Monitor** to **Disable alarm generation**.

1. Start the U2000 server. For details, see **B.2.2.8 How to Start/Stop the NMS Before Synchronizing the Primary and Secondary Sites**.
2. Log in to the GUI of the OS as the **nmsuser** user.
3. On the desktop, double-click **U2000 System Monitor**.

4. In the dialog box that is displayed, enter the U2000 user name and password to log in to the System Monitor. The initial password for the **admin** user is empty and you must change the password at the first login.
5. Choose **Administration** > **Settings** from the main menu. The **System Monitor Settings** dialog box is displayed.
6. Click the **Hard Disk Monitor** tab. In the **Disk Monitor Threshold Settings** area, click **Advanced setting**.
7. Click + to the left of the server name, and select the volume name that contains **/opt/sybase/data**.
8. Click **Default value** and choose **Disable alarm generation** from the drop-down list.
9. Click **OK**.

----End

Follow-up Procedure

Before synchronizing the primary and secondary sites, start the NMS to manage NEs. For details about how to start the NMS, see **B.2.2.8 How to Start/Stop the NMS Before Synchronizing the Primary and Secondary Sites**.

7.3.2 Installing the U2000 Through the CLI

This topic describes how to install the U2000 software through the CLI. Installation engineers are recommended to install the U2000 through the CLI if they cannot log in to the GUI.

Prerequisite

- If the U2000 is not pre-configured, see **7.2 Pre-configuring the U2000**. The U2000 will fail to install if it is not pre-configured.
- The operation procedure varies according to whether a database is installed on site.

  1. The Sybase database is not reused.

     If the Sybase database is not installed on site or the version of the installed database does not meet requirements, it is recommended that the Sybase database be not reused. The database software is pre-installed on the U2000.

  2. The Sybase database is reused.

     If the database is installed on the server and installation engineers want to use the original database software, ensure that the database is running. For details, see **B.3.1.3 How to Verify That the Sybase Process Is Running** and **B.3.1.2 How to Start the Sybase Database Service**.

     - If the Sybase 12.5 is installed, do not use the original database software.
     - If the Sybase 15.0 is installed, do not use the original database software. In the event that the original Sybase 15.0 software must be used, ensure that the following criteria are met:

     (1) The server name of the Sybase database is **DBSVR**. For details, see **B.3.2.7 How to Change the Server Name of the Sybase Database to DBSVR**.

     (2) There are not any redundant database items. For details, see **B.3.2.8 How to Delete Redundant Database Items**.

(3) The character set **UTF-8** is configured for the database. For details, see **B.3.2.9 How to Change the Character Set of the Database to UTF-8**.

- Ensure that the size of the installation directory of the server meets the requirement. For example, if all components need to be installed, the remaining space of the installation directory must be larger than 30 GB. It is advisable to install the components of only one product domain if the server is configured with only two 73 GB hard disks.

  TIP

  Run the **df -hk /opt** command to view the remaining space of the **/opt** directory.

Context

CAUTION

If the server on which the steps described in this topic must be performed is not specified, perform the steps on the primary and secondary sites.

- A large amount of information is displayed in the CLI when installation is performed in CLI mode. Adjust the CLI parameters before installing the U2000 to have the information neatly and quickly displayed. Details are as follows:
  1. Right-click the title bar of the CLI and choose **Properties** from the shortcut menu. The **Properties** dialog box will be displayed.
  2. On the **Option** tab page, set **Buffer Size** to **100** in the **Command History** area.
  3. On the **Layout** tab page, set **Width** to **120** in the **Screen Buffer Size** area.
- Any of the following methods can be used to install the U2000:
  - **Installation by typical network**: Choose the desired scenario according to the type of the equipment to be managed. The U2000 software provides common scenarios. This method is recommended in situations where the license file is not on-hand.
  - **Installation by license**: This method is recommended if the license is on-hand.
  - **Custom installation**: This method is applicable to advanced users familiar with managing the network and U2000. This method is also recommended in the event that the license file is on-hand and the common scenarios provided by the U2000 software are insufficient.

Procedure

1 Log in to the OS of the server as user **root**.

2 Run the following command to verify that the character set of the system is correct:

```
# locale -a
```

If the following message is displayed, the character set of Solaris OS is correct. Otherwise, reinstall the OS.

```
C
en_US.UTF-8
```

3 Run the following commands to switch to the path where the **install.sh** file is stored and run the **install.sh** script:

```
# cd /opt/HWENGR
```

```
# ./install.sh -cmd
```

NOTE

After the message `Starting NMS Engineering CMD Install Server...` is displayed, wait about two minutes.

A message similar to the following will be displayed:

```
===============< Copyright Notice >===============
Copyright Notice
...
I accept these terms [y:Yes, n:No, n]:
```

NOTE

If the U2000 is not pre-configured, the **/opt/HWENGR** directory and the **install.sh** will not be generated and the U2000 cannot be installed.

Read the terms of the software license agreement carefully. Enter **y** if the terms are accepted.

4 Enter **y** and press **Enter**.

NOTE

If a dialog box is displayed prompting you to select the directory of the installation package, enter the directory where the installation files were uploaded to the server. For example, **/opt/install**.

A message similar to the following will be displayed:

```
Install [c:Cancel, <p:< Previous, n:Next>, n]:
```

5 Enter **n** and press **Enter**.

A message similar to the following will be displayed:

```
===============< Select NMS Language >===============

NMS Version Language [1:Chinese, 2:English, 2]:
```

6 Enter **2** and then press **Enter** to select the English version.

A message similar to the following will be displayed:

```
Install [c:Cancel, <p:< Previous, n:Next>, n]:
```

7 Enter **n** and press **Enter**.

A message similar to the following will be displayed:

```
===============< Select an Installation Mode >===============

[1: Installation by typical network (recommended), 2: Installation by license (for
users with license files), 3: Custom installation (for experienced users), 1]:
```

The following uses **Installation by typical network** as an example.

Any of the following methods can be used to install the U2000:

- **Installation by typical network**: Choose the desired scenario according to the type of the equipment to be managed. The U2000 software provides common scenarios. This method is recommended in situations where the license file is not on-hand.
- **Installation by license**: This method is recommended if the license is on-hand.
- **Custom installation**: This method is applicable to advanced users familiar with managing the network and U2000. This method is also recommended in the event that the license file is on-hand and the common scenarios provided by the U2000 software are insufficient.

NOTE

- Enter **2** and press **Enter** to install with a license. Enter the path where the license file is stored and press **Enter**. Then, follow the prompts to install the U2000.
- Enter **3** and press **Enter** to install with a customized installation. Then, follow the prompts to install the U2000.

8 Enter **1** to select **Installation by typical network** and press **Enter**.

NOTE

The following uses the installation by typical network as an example.

A message similar to the following will be displayed:

```
Select a scenario: [1: Transport domain, 2: Access domain, 3: IP domain, 4: All
domains,  1 ][]:
```

9 Select the desired scenario according to the conditions at your site. For example, enter **1** to select the transport network domain scenarios, and press **Enter**.

A message similar to the following will be displayed:

```
Install [c:Cancel, <p:< Previous, n:Next>, n]:
```

10 Enter **n** and press **Enter**.

A message similar to the following will be displayed:

```
===============< Select Components >===============

[1: Select Component, 2: Finished select, 1]:
```

CAUTION

Components and instances installed on the primary and secondary sites must be the same.

11 Enter **2** to finish selecting the components.

NOTE

- Components marked with the asterisk (*****) in the **component** column are mandatory.
- Selected components are indicated with **Y** in the **Option** column.

Enter **1** to reselect the components to be installed if modification is still required.

A message similar to the following will be displayed:

```
Install [c:Cancel, <p:< Previous, n:Next>, n]:
```

12 Enter **n** and press **Enter**.

A message similar to the following will be displayed:

```
===============< Deployment Server >===============
+---------+-------------+-------------+----------------------+-----------------+
|Server Name |IP Address|Server Type|Administrator Password|Installation Path|
+---------+-------------+-------------+----------------------+-----------------+
|Primaster|129.9.1.1|Master Server|****                  |/opt/U2000         |
+---------+-------------+-------------+----------------------+-----------------+

[1: Modify , 2: Complete, 2]:
```

To modify the server, enter **1** and press **Enter**. Follow the prompts to modify the server parameters.

13 Confirm that the information about the server is correct. Enter **2** and press **Enter** to complete the installation.

A message similar to the following will be displayed:

```
Install [c:Cancel, <p:< Previous, n:Next>, n]:
```

14 Enter **n** and press **Enter**.

A message similar to the following will be displayed:

```
===============< An instance is configured for each deployment package for the
master server.
By default, no instance is configured for a slave server.
Specify the number of instances for deployment packages for each server according
to the installation plan. >===============

[1: Configure instances, 2: Configuration is complete., 1]:
```

15 Enter **2** to finish the deployment of instances.

NOTE

- Enter **1** to configure the number of the instances if this parameter needs to be modified.
- You can modify the number of instances only for components with **single-server multi-instance**.
- Limited by the port quantity, a maximum number of 25 instances can be deployed for the transport domain in the single-server multi-instance deployment mode.
- To use the CORBA northbound interface (NBI), XML NBI, SNMP NBI, and text NBI, instances must be added by using the Network Management System Maintenance Suite after installing the desired NBIs.

A message similar to the following will be displayed:

```
Install [c: Cancel, <p: < Previous, n:Next>, n]:
```

16 Enter **n** and press **Enter**.

A message similar to the following will be displayed:

```
===============< Select Style >===============

Version Style [1: Default style, 2: North America style, 1]:
```

NOTE

The following is an example of the differences between the two styles:

- For the default style, alarms are displayed in the following descending order of severity: **Critical**, **Major**, **Minor** and **Warning**.
- For the North America style, alarms are displayed in the following five levels in descending order of severity: **Critical**, **Major**, **Minor**, **Not Alarmed** and **Not Reported**.

17 Select the style according to the conditions at your site. For example, enter **1** to select **Default style** and press **Enter**.

A message similar to the following will be displayed:

```
Install [c: Cancel, <p: < Previous, n:Next>, n]:
```

18 Enter **n** and press **Enter**.

NOTE

If the components include **SDH Network Element Management** or **SDH Service Management**, the **Select timeslot mode** information will be displayed. Select the slot mode according to the conditions at your site. For example, enter **1** to select **Sequence mode** and press **Enter**. Enter **n** and press **Enter** to proceed with the next step.

The **Sequence mode** is the international standard mode and is recommended.

A message similar to the following will be displayed:

```
...
Database Installation Path [/opt/sybase]
Data File Path []: /opt/sybase/data
DB Super Password []:
```

19 Configure the information about the database service as follows:

1. Enter the password of user **DB Super** and press **Enter**.

   NOTE

   - Specifies the superuser password of the database. This password can be left blank (not recommended). The password must be 6-30 characters long and consists of letters or digits. Special characters are not allowed. For example, it can be **changeme**.
   - The password of the database superuser at the primary site must be consistent with that at the secondary site.
   - If the database is installed, and you do not need not to perform the next operations (Enter the password of the **DB Super** user again).

   A message similar to the following will be displayed:

   ```
   Confirm DB Super Password[]:
   ```

2. Enter the password of user **DB Super** again and press **Enter**.

   A message similar to the following will be displayed:

   ```
   DB User Password [******]:
   ```

3. Enter the password of the DB user and press **Enter**.

   NOTE

   - This parameter contains a minimum of six characters and specifies the password of the DB NMS user. The default value is **NMSuser**.
   - The password of the database user at the primary site must be consistent with that at the secondary site.

   A message similar to the following will be displayed:

   ```
   Confirm DB User Password [******]:
   ```

4. Enter the password of the DB user and press **Enter**.

   A message similar to the following will be displayed:

   ```
   Install [c: Cancel, <p: < Previous, n:Next>, n]:
   ```

5. Enter **n** and press **Enter**.

NOTE

- If the system prompts you to use the original database software, a database has been installed on the server. If you reuse the database, the installation program will skip database installation. If you do not reuse the database, the installation program will uninstall the existing database and reinstall the database. It is recommended that installation engineers not to reuse the database.
- If the message "Select Installation Package Patch" is displayed, no database installation package is stored in the **/opt/install** directory. In this case, upload database software U2000***version***_server_db_solaris_SPARC.tar to the **/opt/install** directory on the server and decompress it. Set the directory of the installation package to **/opt/install**.

A message similar to the following will be displayed:

```
===============< Please check the following overall information about the
U2000 installation>===============
[Basic Information]
...
Install[c:Cancel, <p:< Previous, n:Next>, n]:
```

20 Confirm that the installation information is correct, enter **n** and press **Enter**.

A message similar to the following will be displayed:

```
===============< Progress information >===============


Initializing the data model. Please wait...: 0%
```

NOTE

- The NMS can automatically expand the capacity of a database according to the growth parameters defined when the database is created. The disk space for installing the database must be greater than the maximum size to which the file is permitted to grow. If the disk space is insufficient, the system displays a prompt message in red. The management capability of the U2000 after the installation cannot reach the associated maximum value of this model.
- When the progress bar reaches 99%, the system may wait about half an hour until U2000 installation is complete. This is normal.
- If a message indicating installation failure or abnormal interruption is displayed during installation, perform the following operations to clean up the installation environment, and then install the U2000.
  1. Run the following commands to use the environment clean-up tool to clear the installation environment:
     ```
     # cd /opt/HWENGR/engineering/tool
     # ./FailedNMSInstallationClear.sh
     ```
  2. Run Step 3 to install the U2000.

21 After the installation, the message similar to the following will be displayed:

```
...
Install [c: Cancel, p: < Previous, n:Next>, n]:
```

22 Enter **n** and press **Enter** to complete the installation.

A message similar to the following will be displayed:

```
===============< Installation Completed >===============

The iManager U2000 is installed successfully.
...
```

23 Run the following commands to stop the VCS service:

```
# cd /opt/VRTSvcs/bin
# hastop -local -force
```

24 Run the following command to verify that the VCS service is stopped:

```
# ps -ef|grep had
```

A message similar to the following will be displayed:

```
root 27663 17299   0 00:31:00 pts/2  0:00 grep had
```

NOTE

If the **had** and **hadshadow** processes are not displayed, the VCS service is successfully stopped; otherwise, run the **kill -9 process ID** command to stop the related processes.

25 Run the following commands to restart the OS:

```
# sync;sync;sync;sync
# shutdown -y -g0 -i6
```

26 Do as follows to set **Disable alarm generation** for **/opt/sybase/data**:

CAUTION

This step needs to be performed only on the primary site.

NOTE

The **/opt/sybase/data** path is used to store database data. In the high availability system, data in this path must be replicated to the secondary site in real time. The database data size is used by default according to the data replication rate and traffic. Therefore, the remaining hard disk space is small, and an alarm is reported on **Hard Disk Monitor** of the System Monitor. This alarm is a normal one and you need to set the monitoring status on **Hard Disk Monitor** to **Disable alarm generation**.

1. Start the U2000 server. For details, see **B.2.2.8 How to Start/Stop the NMS Before Synchronizing the Primary and Secondary Sites**.
2. Log in to the OS where the remote System Monitor is installed.
   - In Windows, log in to the OS as the **administrator** user.
   - In Solaris, log in to the GUI of the OS as the **nmsuser** user.
3. On the desktop, double-click **U2000 System Monitor**.
4. In the dialog box that is displayed, enter the U2000 user name and password to log in to the System Monitor. The initial password for the **admin** user is empty and you must change the password at the first login.
5. Choose **Administration** > **Settings** from the main menu. The **System Monitor Settings** dialog box is displayed.
6. Click the **Hard Disk Monitor** tab. In the **Disk Monitor Threshold Settings** area, click **Advanced setting**.
7. Click + to the left of the server name, and select the volume name that contains **/opt/sybase/data**.
8. Click **Default value** and choose **Disable alarm generation** from the drop-down list.
9. Click **OK**.

----End

Follow-up Procedure

Before synchronizing the primary and secondary sites, start the NMS to manage NEs. For details about how to start the NMS, see **B.2.2.8 How to Start/Stop the NMS Before Synchronizing the Primary and Secondary Sites**.

8 Connecting the Primary and Secondary Sites

This topic describes how to connect the primary and secondary sites using the MSuite. After the U2000 is installed on the primary and secondary sites, you must connect the primary and secondary sites to establish a high availability system.

Prerequisite

- The preceding steps for installing the primary and secondary sites must be complete.
- The instances deployed on the primary and secondary sites must be the same.
- **Ensure that VVR ports can be connected**.
- **Ensure that files can be properly transferred between primary and secondary sites**.

Context

Connect the primary and secondary sites in either of the following modes:

- **Mode 1 (recommended)**: GUI mode. If you are not familiar with common commands of the Solaris OS, connecting the primary and secondary sites in GUI mode is recommended.
- **Mode 2**: CLI mode. If you fail to log in to the OS in GUI mode, using primary and secondary sites the CLI mode is recommended.

Using the GUI mode is taken as an example here.

Procedure

- **Mode 1 (recommended)**: Connect the primary and secondary sites in GUI mode.
  1. Ensure that the MSuite servers on the primary and secondary sites have been started.

     Run the following command as the **root** user to check whether the MSuite servers are started:

     ```
     # ps -ef | grep java
     ```

     A message similar to the following will be displayed:

     ```
     ...
     root  5694     1   0 19:47:23 ?          61:16 /opt/HWNMSJRE/jre_sol/bin/
     java -server -Dlanguage=en -Xverify:none -Xmx256m -Xm
     ```

     NOTE

     If the displayed information contains **/opt/HWNMSJRE/jre_sol/bin/java -server**, it indicates that the MSuite servers have been started.

     If the MSuite server have not been started, run the following commands as the **root** user to start the MSuite servers:

```
# cd /opt/HWENGR/engineering
# ./startserver.sh
```

2. Log in to the **Java Desktop System, Release 3** session of the OS of the primary site as the nmsuser user.

   NOTE

   As the default password of the **nmsuser** user is not set, it can be blank or any character that can be used when the OS is first logged in to as the **nmsuser** user. The system will prompt you to change the password which must be a string of at least six characters and contain at least one digit or special character. The login window will close after the password is changed. Then, log in to the Java Desktop System, Release 3 session process of the server OS again as the **nmsuser** user.

3. On the primary site, start up the MSuite client running the following commands:

   ```
   $ cd /opt/U2000/engineering
   $ ./startclient.sh
   ```

   Wait for about one minute. A dialog box is displayed, as shown in the following figure.

   Then, set the related parameters according to the following table.

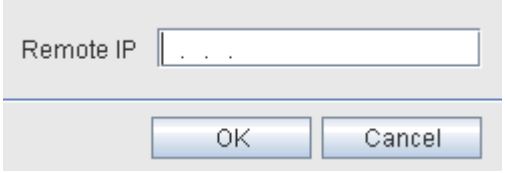
Parameter	Settings
IP Address	Specifies the system IP address on the primary site. ● If the Network Management System Maintenance Suite client and the Network Management System Maintenance Suite server are on the same computer, you must enter 127.0.0.1 or the system IP address on the primary site. ● If the Network Management System Maintenance Suite client and the Network Management System Maintenance Suite server are on different computers, enter only the system IP address on the primary site.
Port Number	Specifies the port number. The default value is **12212**.
User Name	Specifies the user name. The default value is **admin**.
Password	Specifies the password of the **admin** user. The default password is **admin**.

4. Click **Login** to access the **NMS Maintenance Suite** window.

   NOTE

   When you log in to the MSuite client, a progress bar showing the progress of querying subsystems and instances is displayed. Wait until the operation is complete.

5. Choose **Deploy** > **Synchronize Primary and Secondary Sites**. A dialog box is displayed, as shown in the following figure.



6. Enter the system IP address on the opposite site, and then click **OK**. A progress bar is displayed, indicating the progress of synchronizing the primary and secondary sites. It takes about 30 minutes to complete the process. Please wait patiently until a confirmation dialog box is displayed.
7. Click **OK**.
8. On the primary site, run the following command to switch from the **nmsuser** user to the **root** user:

```
$ su - root
```

9. On the primary site, repeatedly run the following command as the **root** user to check the data replication status:

```
# vradmin -g datadg repstatus datarvg
```

TIP

To save time, running the preceding command every half an hour is recommended to check the data replication status.

A message similar to the following will be displayed:

```
Replicated Data Set: datarvg
Primary:
  Host name:                    192.168.1.10
  RVG name:                     datarvg
  DG name:                      datadg
  RVG state:                    enabled for I/O
  Data volumes:                 1
  VSets:                        0
  SRL name:                     srl_vol
  SRL size:                     1.00 G
  Total secondaries:            1

Secondary:
  Host name:                    192.168.1.11
  RVG name:                     datarvg
  DG name:                      datadg
  Data status:                  consistent, up-to-date
  Replication status:           replicating (connected)
  Current mode:                 asynchronous
  Logging to:                   SRL
  Timestamp Information:        behind by 0h 0m 0s
```

NOTE

- If **Replication status** is displayed as **resync in progress (autosync)**, **Data status** is displayed as **in consistent**, and the value of **DCM** is becoming smaller, it indicates that data is being duplicated between primary and secondary sites.
- If **Replication status** is displayed as **replicating (connected)** and **Data status** is displayed as **consistent,** , it indicates that data duplication of the high availability system (Veritas hot standby) is complete.
- If **Replication status** is displayed as **logging to DCM (needs dcm resynchronization)**, you must run the **vradmin -g datadg resync datarvg** command on the primary site as the **root** user to perform manual synchronization.
- The duration of data replication depends on the stability of the network bandwidth and the volume of the data to be replicated.

- **Mode 2**: Connect the primary and secondary sites in CLI mode.
  1. Ensure that the primary and secondary sites of the on the MSuite server have been started. For details, see Step 1 in mode 1.
  2. Log in to the OS of the primary site as the **nmsuser** user and run the following commands:
     ```
     cd /opt/U2000/engineering
     ./startclient.sh deploy -ip 127.0.0.1 -port 12212 -username admin -
     password admin buildHA -secondaryip System IP address of the peer site
     ```
     Perform operations as prompted.
  3. On the primary site of the , check data replication status as the **root** user. For details, see Step 9 in mode 1.

----End

9 Loading or Updating a License File

About This Chapter

This topic describes how to load or update a license file. After a U2000 is installed, it is recommended that you update the Veritas license file and load the U2000 license file in time. You can update the Veritas license before loading the U2000 license file or vice versa.

9.1 Updating a Veritas License

This topic describes how to update a Veritas license. The Veritas license used in the NMS installation is a demo license. After the server is delivered to the installation site, the demo license must be replaced with the formal Veritas license in time.

Prerequisite

The formal Veritas license must be obtained.

Context

NOTE

You need to replace the demo licenses on the NMS servers of both the primary and secondary sites with formal Veritas licenses.

Procedure

1. Log in to the OS as the **root** user.
2. To back up all the license files in the **/etc/vx/licenses/lic** path, run the following commands:
   ```
   # mkdir /export/home/licenses
   # mv /etc/vx/licenses/lic/*.vxlic /export/home/licenses
   ```
3. To access the path where the script for updating licenses is stored, run the following command:
   ```
   # cd /opt/VRTS/bin
   ```
4. To update the VxVM license, run the following command:
   ```
   # ./vxlicinst
   ```
   The following information is displayed:
   ```
   Symantec License Manager vxlicinst utility version 3.02.33.0
   Copyright (C) 1996-2007 Symantec Corporation. All rights reserved.

   Enter your license key :
   ```
5. Enter the new license key of VRTS STORAGE FOUNDATION STANDARD. The new license key is in the format of XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-X. Then, press **Enter**.

   NOTE

   - X indicates the a letter or digit of a license key.
   - The information about the demo or formal license that is newly obtained is contained in the license file.
   - The new licenses include VRTS STORAGE FOUNDATION STANDARD, VRTS VOLUME REPLICATOR OPTION, and VRTS CLUSTER SERVER HA/DR.
6. Repeat step 4, and then enter the new license key of VRTS VOLUME REPLICATOR OPTION.
7. Repeat step 4, and then enter the new license key of VRTS CLUSTER SERVER HA/DR.
8. To check whether the updated license takes effect, run the following command:
   ```
   # /opt/VRTSvlic/bin/vxlicrep
   ```
   Check whether the license key of the associated component is updated and whether the authentication date of the component is correct.
9. To stop the VCS service, run the following commands:

```
# cd /opt/VRTSvcs/bin
# hastop -local -force
```

10 To check whether the VCS service is stopped, run the following command:

```
# ps -ef|grep had
```

A message similar to the following will be displayed:

```
root 27663 17299   0 00:31:00 pts/2  0:00 grep had
```

NOTE

If the **had** and **hadshadow** processes are not displayed, the VCS service is successfully stopped; otherwise, run the **kill -9 process ID** command to stop the related processes.

11 To restart the OS, run the following commands:

```
# sync;sync;sync;sync
# shutdown -y -g0 -i6
```

----End

9.2 (Optional) Loading a U2000 License

This topic describes how to load a U2000 license. If **Installation by license** is not selected during installation of the U2000 software, you must upload a U2000 license.

Prerequisite

The U2000 license file must be ready. The file name cannot contain any space. If a space is included in the file name, delete the space or change it to an underscore (_).

Context

The U2000 license must be installed on the primary and secondary sites separately.

Two methods are available for loading a U2000 license.

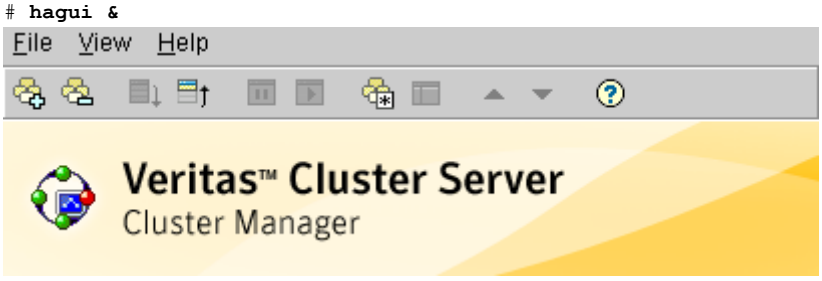
- **Method one**: Use commands to load the license. This method is applicable to users who cannot log in to GUI OSs.
- **Method two**: Load the license in the GUI. This method is applicable to users who are not familiar with common commands of the Solaris OS.

Procedure

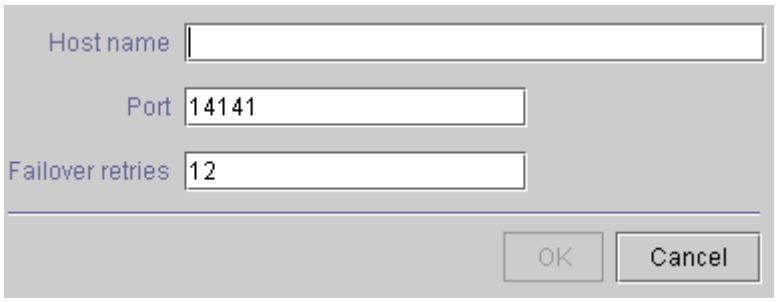
1 On the primary site, do as follows to start U2000 processes:

1. Run the following command as the **root** user to start the VCS client:

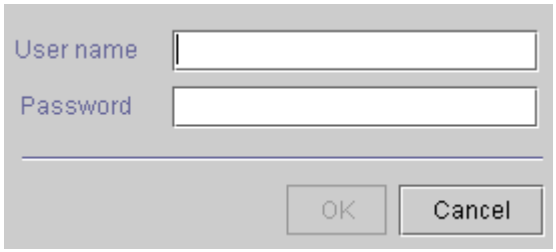
```
# hagui &
```



2. Choose **File** > **New Cluster**. A dialog box is displayed, as shown in the following figure.



3. Enter the IP address for the Heartbeat network service of the primary site. Then, click **OK**.



4. Enter the default user name **admin** and the initial password **password** for the VCS client. Then, click **OK**.
5. Right-click **AppService** in the navigation tree and choose **Online** > ***host_name*** from the shortcut menu.
6. In the dialog box that is displayed, click **Yes**.

If all resources, including NMSServer, BackupServer, DatabaseServer, DataFilesystem, RVGPrimary and appNIC, are in the **Online on Primaster** state, the U2000 server is started successfully.

2 On the primary and secondary sites, check whether a license file already exists in the license path. If a license file already exists, back it up.

```
# cd /opt/U2000/server/etc/conf/license
# ls
```

If the folder contains any other license file, run the following commands to back up the any other license file to the **/opt/U2000/server/etc/conf/license_backup** path.

```
# mkdir -p /opt/U2000/server/etc/conf/license_backup
# cd /opt/U2000/server/etc/conf/license
# cp license_file_name /opt/U2000/server/etc/conf/license_backup
```

3 Load the U2000 license.

Method one: Use commands to load the license.

1. Send the license file to the U2000 installation path **/export/home/nmsuser** of the primary site in ASCII mode by FTP as the **root** user. Details are as follows:
   a. Log in to the PC where the license file is stored.
   b. Choose **Start** > **Run**. In the **Run** dialog box, enter **ftp** ***system IP address of the server*** and click **OK**. An FTP connection is established and a CLI is displayed.
   c. In the CLI, enter **nmsuser** as the name of the OS user.
      ```
      User (IP_address:(none)):nmsuser
      ```
   d. Enter the password for the **nmsuser** user.
      ```
      Password:
      ```
   e. Set the format of the file to be transferred using FTP to ASCII.

```
ftp> ascii
```

f. Navigate to the path on the computer where the license file is stored.
```
ftp> lcd PC_directory
```

g. Navigate to the **/export/home/nmsuser** directory.
```
ftp> cd /export/home/nmsuser
```

h. Run the **put** command to upload the license file to the server.
```
ftp> put "License_file_name"
```

i. To exit the FTP program, run the following command:
```
ftp> quit
```

2. Do as follow to make the license take effect:

a. log in to the OS of the U2000 server as the **nmsuser** user on the primary site.

b. To update the U2000 license file, run the following commands:
```
$ cd /export/home/nmsuser
$ updateLicense -file License_file_name
```
Information similar to the following is displayed:
```
state            product        feature        item        name        old
value        new value
no change:    U2000        COMMON        LSW1CAPA01        Client
500        500
no change:    U2000        COMMON        LSW1CAPA01        Client
1        1
no change:    U2000       COMMON       LSW1FMCLT01       Alarm Export
1        1
no change:    U2000        COMMON        LSW1RENOTI01        Client
1        1

Are you sure to update the license?(Y/N)
```

c. Enter **Y**, and then press **Enter**.

3. Send the license file to the **/opt/U2000/server/etc/conf/license** path on the secondary site in ASCII mode by FTP as the **nmsuser** user. For details, **3.1**.

Method two: Load the license in the GUI.

Update the license on the primary site.

1. Log in to the OS where the U2000 client is installed.
   - In Windows, log in to the OS as the **administrator** user.
   - In Solaris, log in to the OS as the **nmsuser** user.
2. Save the license to be loaded to the server where the U2000 client is installed.
3. On the desktop, double-click **U2000 Client**. The **Login** dialog box is displayed.
4. In the **Server** drop-down list, select the server (server on the primary site) to be logged in to. Then, set **User Name** and **Password** to the valid values, and click **Login**. If you have logged in to the System Monitor before, enter the password for logging in to the System Monitor. If you have never logged in to the System Monitor before and this is the first time that you log in to the U2000 client, the password is empty and you must change the password.

   NOTE

   - If a message indicating that no license is available is displayed when you log in to the U2000 client, select the license to be updated as prompted.
   - If an access domain component is selected during installation, choose **Help** > **License Management** > **License Information** from the main menu of the U2000 client. In the **License Information** dialog box, click **Update License**. In the **Open** dialog box, select the new license file and click **Open**.

Update the license on the secondary site.

1. On the primary site, log in to the VCS client. For details, see **1.1**.
2. Right-click the AppService resource group and choose **Switch to** > **Remote switch** from the shortcut menu.
3. Select the clusters and systems to be switched.
4. Click **OK**.
5. In the **Confirm** dialog box, click **Yes** to switch U2000 services to the secondary site.
6. Use the U2000 client to reconnect to the system IP address of the secondary site.

   NOTE

   - If a message indicating that no license is available is displayed when you log in to the U2000 client, select the license to be updated as prompted.
   - If an access domain component is selected during installation, choose **Help** > **License Management** > **License Information** from the main menu of the U2000 client. In the **License Information** dialog box, click **Update License**. In the **Open** dialog box, select the new license file and click **Open**.

----End

10 Checking System Installation

This topic describes how to check the installation of a high availability system (Solaris).

Context

- During installation of the U2000 software, the OS user **nmsuser** is created automatically. The **nmsuser** user is used to regularly maintain a U2000.
- During installation of the U2000 software, only one default NMS user, that is, user **admin**, is provided. The **admin** user is the administrator of the U2000 and has the highest rights of the U2000. The default password of user **admin** is blank. You must change the default password during first-time login.

Procedure

1. Log in to the OSs of the servers of the primary and secondary sites as the **root** user.
2. To check the U2000 version, run the following commands:

   ```
   # cd /opt/U2000/server/etc/conf
   # cat imap.cfg
   ```

   Information similar to the following is displayed:

   ```
   ...
   VER = U2000V100R002C01
   ```

   The last line of the displayed information shows the U2000 version. If the version information does not meet the actual requirement, uninstall the U2000 and obtain the correct software version to install the U2000 again.
3. To check whether disk arrays are properly mounted, run the following command:

   NOTE

   If no disk array has been configured, skip this step.

   ```
   # df -h
   ```

   Information similar to the following is displayed:

   ```
   Filesystem             size   used  avail capacity  Mounted on
   /dev/vx/dsk/bootdg/rootvol
                          15G   4.6G    10G    32%    /
   /devices                0K     0K     0K     0%    /devices
   ctfs                    0K     0K     0K     0%    /system/contract
   proc                    0K     0K     0K     0%    /proc
   mnttab                  0K     0K     0K     0%    /etc/mnttab
   ```

```
swap                    42G   1.8M    42G     1%    /etc/svc/volatile
objfs                    0K     0K     0K     0%    /system/object
sharefs                  0K     0K     0K     0%    /etc/dfs/sharetab
fd                       0K     0K     0K     0%    /dev/fd
/dev/vx/dsk/bootdg/var
                        15G   1.4G    13G    10%    /var
swap                    42G    88K    42G     1%    /tmp
swap                    42G    40K    42G     1%    /var/run
swap                    42G     0K    42G     0%    /dev/vx/dmp
swap                    42G     0K    42G     0%    /dev/vx/rdmp
/dev/vx/dsk/bootdg/opt
                        21G   2.9G    18G    15%    /opt
/dev/odm                 0K     0K     0K     0%    /dev/odm
/dev/vx/dsk/datadg/lv_database
                        20G    20M    19G     1%    /opt/sybase
/dev/vx/dsk/datadg/lv_nms_data
                        89G    64M    88G     1%    /opt/sybase/data
/dev/vx/dsk/datadg/lv_nms
                       197G    64M   195G     1%    /opt/U2000
/dev/vx/dsk/datadg/lv_backup
                       197G    64M   195G     1%    /opt/backup
/dev/vx/dsk/datadg/lv_ftproot
                       295G    64M   292G     1%    /ftproot
```

Pay attention to the lines that contain **datadg**.

- If the values of **Mounted on** for the lines that contain **datadg** are the same as the preceding command output, disk arrays are properly mounted.
- If the values of **Mounted on** for the lines that contain **datadg** are different from the preceding command output, disk arrays are not properly mounted. Contact Huawei engineers to locate the fault.

4 Do as follows to check the Veritas version and patch information:

1. To check the VxVM version, run the following command:

   ```
   # pkginfo -l VRTSvxvm
   ```

   If the VxVM version is correct, information similar to the following is displayed:

   ```
      PKGINST:  VRTSvxvm
         NAME:  Binaries for VERITAS Volume Manager by Symantec
     CATEGORY:  system
         ARCH:  sparc
      VERSION:  5.1,REV=10.06.2009.22.05
      BASEDIR:  /
       VENDOR:  Symantec Corporation
         DESC:  Virtual Disk Subsystem
       PSTAMP:  5.1.002.000-5.1RP2-2010-08-27
    INSTDATE:  Nov 16 2010 02:09
     HOTLINE:  http://support.veritas.com/phonesup/phonesup_ddProduct_.htm
       EMAIL:  support@veritas.com
      STATUS:  completely installed
       FILES:      898 installed pathnames
                    37 shared pathnames
                   110 directories
                   384 executables
                364221 blocks used (approx)
   ```

   Pay attention to information to the right of **PSTAMP**. If the information to the right of **PSTAMP** is not **5.1.002.000-5.1RP2-2010-08-27**, you must reinstall Veritas 5.1 or contact Huawei engineers. For details, see **7.2 Pre-configuring the U2000**.

2. To check the VCS version, run the following command:

   ```
   # pkginfo -l VRTSvcs
   ```

   If the VCS version is correct, information similar to the following is displayed:

   ```
      PKGINST:  VRTSvcs
         NAME:  Veritas Cluster Server by Symantec
     CATEGORY:  system
         ARCH:  sparc
      VERSION:  5.1
   ```

```
   BASEDIR:  /
    VENDOR:  Symantec Corporation
      DESC:  Veritas Cluster Server by Symantec
    PSTAMP:  5.1.002.000-5.1RP2-2010-08-26_19.00.00
  INSTDATE:  Nov 16 2010 02:17
    STATUS:  completely installed
     FILES:      281 installed pathnames
                  27 shared pathnames
                   4 linked files
                  60 directories
                 102 executables
              234265 blocks used (approx)
```

Pay attention to information to the right of **PSTAMP**. If the information to the right of **PSTAMP** is not **5.1.002.000-5.1RP2-2010-08-26_19.00.00**, you must reinstall Veritas 5.1 or contact Huawei engineers. For details, see **7.2 Pre-configuring the U2000**.

5 To check disk group status, run the following command:

```
# vxdg list
```

Information similar to the following is displayed:

```
vxdg list

NAME         STATE           ID
rootdg       enabled              1281152223.12.primaster
datadg       enabled              1281151979.10.primaster
```

- If the value of **STATE** is **enabled**, the disk group status is correct.
- If the value of **STATE** is not **enabled**, the disk group does not function properly. Contact Huawei engineers to locate the fault.

6 To check disk status, run the following command:

```
# vxdisk list
```

Information similar to the following is displayed:

```
DEVICE       TYPE            DISK         GROUP        STATUS
c1t0d0s2     auto:sliced     disk01       rootdg       online
c1t1d0s2     auto:sliced     disk02       rootdg       online
c1t2d0s2     auto:sliced     disk03       datadg       online
c1t3d0s2     auto:sliced     disk04       rootdg       online
c1t4d0s2     auto:sliced     disk05       rootdg       online
c1t5d0s2     auto:sliced     disk06       datadg       online
```

NOTE

The equipment names in the **DEVICE** column may be different from those displayed on the terminal according to the actual situation of the workstation. Here, six hard disks are taken as an example.

- If the value of **STATUS** is **online**, the disk status is correct.
- If the value of **STATUS** is not **online**, the disk does not function properly. Contact Huawei engineers to locate the fault.

7 To check disk volume status, run the following command:

```
# vxprint -v
```

Information similar to the following is displayed:

```
Disk group: rootdg

TY NAME         ASSOC        KSTATE   LENGTH    PLOFFS   STATE    TUTIL0  PUTIL0
v  backup       fsgen        ENABLED  161493120 -        ACTIVE   -       -
v  home         fsgen        ENABLED  4212864   -        ACTIVE   -       -
v  opt          fsgen        ENABLED  283116672 -        ACTIVE   -       -
v  rootvol      root         ENABLED  41945472  -        ACTIVE   -       -
v  swapvol      swap         ENABLED  33560448  -        ACTIVE   -       -
v  var          fsgen        ENABLED  41945472  -        ACTIVE   -       -
```

```
Disk group: datadg

TY NAME         ASSOC        KSTATE   LENGTH   PLOFFS   STATE    TUTIL0  PUTIL0
v  lv_nms_data  datarvg       ENABLED  83886080 -        ACTIVE   -       -
v  srl_vol      datarvg       ENABLED  2097152  SRL      ACTIVE   -       -
```

NOTE

The displayed information varies with the data of the hard disks that are actually configured.

- If more than two hard disks are configured, the two disk groups (rootdg and datadg) are available.
- If only two disks are configured, only one disk group (datadg) is available.

Reference Standards

- All disk volumes used by the U2000 exist. Currently, the U2000 uses the following disk volumes: backup, home, opt, rootvol, swapvol, var, lv_nms_data, and srl_vol.
- The value of **KSTATE** must be **ENABLED** for all disk volumes.
- The value of **STATE** must be **ACTIVE** for all disk volumes.

If disk volume status does not meet the preceding requirements, run the following command to record details about all disk volumes, and contact Huawei local office or customer service center in time according to warranty information.

```
# vxprint -l disk volume name
```

8 To check whether the replication between the primary and secondary sites is normal, run the following command on the primary site:

```
# vradmin -g datadg repstatus datarvg
```

Information similar to the following is displayed:

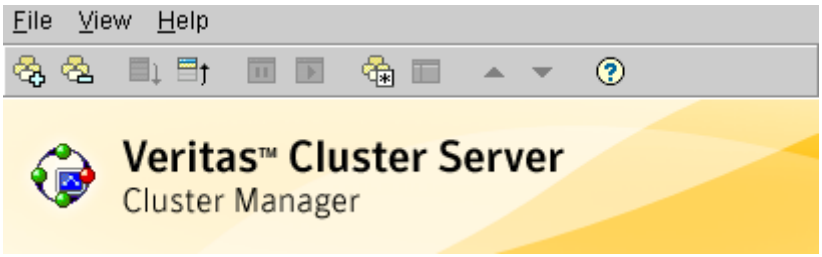
```
Replicated Data Set: datarvg
Primary:
  Host name:                    192.168.1.10
  RVG name:                     datarvg
  DG name:                      datadg
  RVG state:                    enabled for I/O
  Data volumes:                 1
  VSets:                        0
  SRL name:                     srl_vol
  SRL size:                     1.00 G
  Total secondaries:            1

Secondary:
  Host name:                    192.168.1.11
  RVG name:                     datarvg
  DG name:                      datadg
  Data status:                  consistent, up-to-date
  Replication status:           replicating (connected)
  Current mode:                 asynchronous
  Logging to:                   SRL
  Timestamp Information:        behind by 0h 0m 0s
```

If the value of **Replication status** is **replicating (connected)**, the replication is normal.

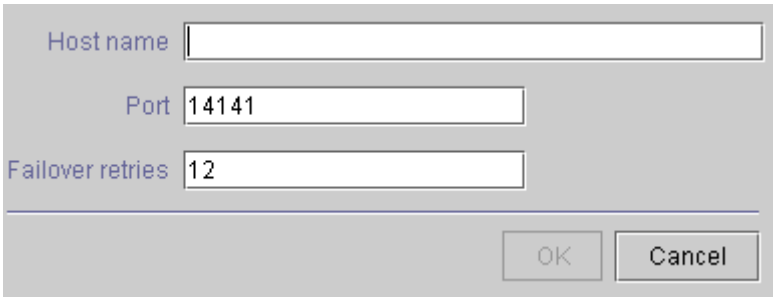
9 Do as follows on the primary site to start the U2000 server:

1. To start the VCS client, run the following command:

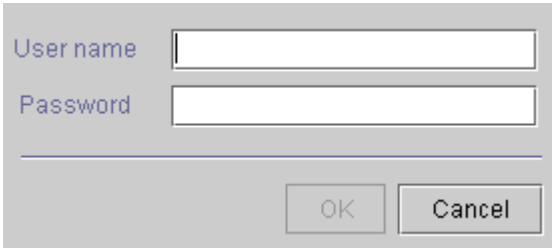
   ```
   # hagui &
   ```



2. Choose **File** > **New Cluster**. A dialog box is displayed, as shown in the following figure.



3. Enter the IP address of the Heartbeat network service of the primary site. Then, click **OK**.



4. Enter the default user name **admin** and the initial password **password** for the VCS client. Then, click **OK**.
5. Right-click **AppService** and choose **Online** > ***host_name*** from the shortcut menu.

   NOTE

   If a fault has occurred when the AppService process was started before, right-click **AppService** and choose **clear fault** from the shortcut menu. Then, choose **Online** > ***host_name*** to start the AppService process.
6. In the dialog box that is displayed, click **Yes**.

NOTE

If all resources, including NMSServer, BackupServer, DatabaseServer, DataFilesystem, RVGPrimary and appNIC, are in the Online on **Primaster** state, the U2000 server is started successfully.

10 Log in to the active site server GUI as the **nmsuser** user. Then, start the System Monitor to view the running status of each process.

CAUTION

If you cannot log in to the GUI of the server OS, do as follows to view the process status:

1. Run the **su - nmsuser** command to switch to the **nmsuser** user.
2. Run the **svc_adm -cmd status** command to view the process status.

1. On the desktop of the OS, double-click the **U2000 System Monitor** shortcut icon.

2. In the dialog box that is displayed, enter the U2000 user name and password (to open the System Monitor window). The default password of user **admin** is blank. You must change the default password during first-time login.

   NOTE

   There are two data transmission modes, namely, **Common** and **Security(SSL)**. You can run the **ssl_adm -cmd query** command to query data transmission modes on the server. The **ssl_adm -cmd query** command must be run as user **nmsuser** in Solaris and SUSE Linux OS. The default data transmission mode is **Common**.

   The U2000 is functioning properly if it can initiate in automatic startup mode, indicating that the U2000 is functioning properly.

   If a process cannot start, right-click the process and choose **Start the Process** from the shortcut menu.

   If the U2000 works properly, contact Huawei engineers.

11 Start the U2000 client as user **nmsuser** to log in to the server GUI.

CAUTION

The U2000 should be logged in to through a standalone client in the event that login to the server through the GUI fails and login to the client on the server is not possible.

1. On the desktop of the OS, double-click the **U2000 Client** shortcut icon.
2. In the dialog box that is displayed, enter the U2000 user name and password to open the main window of the client. The user name is **admin** and the password is the one changed in the previous step.

   NOTE

   There are two data transmission modes, namely, **Common** and **Security(SSL)**. You can run the **ssl_adm -cmd query** command to query data transmission modes on the server. The **ssl_adm -cmd query** command must be run as user **nmsuser** in Solaris and SUSE Linux OS. The default data transmission mode is **Common**.

----End

A Separating the Primary Site from the Secondary Site

This topic describes how to separate the primary site from the secondary site. Separating the primary site from the secondary site refers to disconnecting the primary site and the secondary site. In this manner, the HA system is split into two individual sites. To separate the primary site from the secondary site, perform the following operations.

Prerequisite

Ensure that the **/opt** directory has available space. You can run the **df -hk /opt** command to view the remaining space of the **/opt** directory.

Procedure

- Mode 1 (recommended): Separate the primary site from secondary site in GUI mode.
  1. Ensure that the MSuite servers on the primary and secondary sites have been started.

     Run the following command as the **root** user to check whether the MSuite servers are started:

     ```
     # ps -ef | grep java
     ```

     A message similar to the following will be displayed:

     ```
     ...
     root  5694     1   0 19:47:23 ?          61:16 /opt/HWNMSJRE/jre_sol/bin/
     java -server -Dlanguage=en -Xverify:none -Xmx256m -Xm
     ```

     NOTE

     If the displayed information contains **/opt/HWNMSJRE/jre_sol/bin/java -server**, it indicates that the MSuite servers have been started.

     If the MSuite server have not been started, run the following commands as the **root** user to start the MSuite servers:

     ```
     # cd /opt/HWENGR/engineering
     # ./startserver.sh
     ```

  2. Log in to the **Java Desktop System, Release 3** session of the OS of the primary site as the nmsuser user.

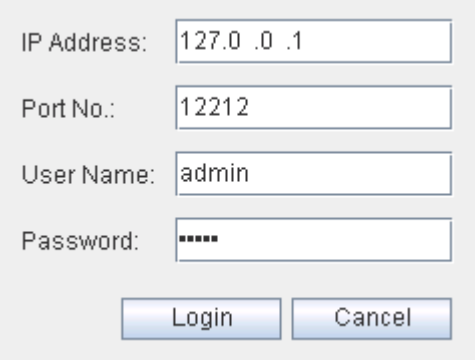
NOTE

As the default password of the **nmsuser** user is not set, it can be blank or any character that can be used when the OS is first logged in to as the **nmsuser** user. The system will prompt you to change the password which must be a string of at least six characters and contain at least one digit or special character. The login window will close after the password is changed. Then, log in to the Java Desktop System, Release 3 session process of the server OS again as the **nmsuser** user.

3. On the primary site, start up the MSuite client running the following commands:

```
$ cd /opt/U2000/engineering
$ ./startclient.sh
```

Wait for about one minute. A dialog box is displayed, as shown in the following figure.



Then, set the related parameters according to the following table.

Parameter	Settings
IP Address	Specifies the system IP address on the primary site. ● If the Network Management System Maintenance Suite client and the Network Management System Maintenance Suite server are on the same computer, you must enter 127.0.0.1 or the system IP address on the primary site. ● If the Network Management System Maintenance Suite client and the Network Management System Maintenance Suite server are on different computers, enter only the system IP address on the primary site.
Port Number	Specifies the port number. The default value is **12212**.
User Name	Specifies the user name. The default value is **admin**.
Password	Specifies the password of the **admin** user. The default password is **admin**.

4. Click **Login** to access the **NMS Maintenance Suite** window.

NOTE

When you log in to the MSuite client, a progress bar showing the progress of querying subsystems and instances is displayed. Wait until the operation is complete.

5. Choose **Deploy** > **Separate Primary Site from Secondary Site**. The **Separate Primary Site from Secondary Site** dialog box is displayed.

6. Click **OK**. The progress bar is displayed indicating the status of separating the primary and secondary sites. Wait until the dialog box is displayed indicating that the separation is complete.
7. Click **OK**.

- Mode 2: Separate the primary site from secondary site in CLI mode.
  1. Ensure that the primary and secondary sites of the on the MSuite server have been started. For details, see Step 1 in mode 1.
  2. Log in to the OS of the primary site as the **nmsuser** user and run the following commands:

     ```
     cd /opt/U2000/engineering
     ./startclient.sh deploy -ip 127.0.0.1 -port 12212 -username admin -password admin splitHA
     ```

     Perform operations as prompted.

----End

Follow-up Procedure

After the active site and standby site are successfully separated, primary and secondary sites are two separate sites. To re-establish the HA system, you need to perform synchronization between the active site and standby site. For details, see **8 Connecting the Primary and Secondary Sites**.

B FAQs

This topic provides answers to the most frequent questions concerning the installation.

B.1 Solaris OS
This topic provides answers to FAQs about clients installed on Solaris OS.

B.2 Veritas HA System
This topic covers FAQs about the Veritas HA system.

B.3 Sybase Database
This topic covers FAQs about the Sybase database.

B.4 U2000 System
This topic covers FAQs about the U2000 system.

B.1 Solaris OS

This topic provides answers to FAQs about clients installed on Solaris OS.

B.1.1 Network Configurations of the Workstation

This topic provides answers to FAQs about the network configurations of the workstation.

B.1.1.1 How to Add the Default Route

Question

How do I add the default route?

Answer

1. Log in the OS as user **root**.
2. Open a terminal window in the Solaris OS.
3. Run the following command:
   ```
   # vi /etc/defaultrouter
   ```
4. Enter an IP address as the default route in the file, for example, 129.9.1.254.
5. Run the **vi** command to save and close the file.
6. Run the following commands to restart the server:
   ```
   # sync;sync;sync;sync
   # shutdown -y -g0 -i6
   ```
7. Log in to the Solaris OS as the **root** user. Run the **netstat -nr** command to view the default route of the system.

----End

B.1.1.2 How to Add a Static Route

Question

How do I add a static route?

Answer

1. Log in to the system as user **root**.
2. Run the following command in the **Terminal** window to view the existing routes in the system:
   # **netstat -nr**
3. Run the following command to add a route:
   # **route add** *network_IP_address* **-netmask** *netmask gateway_IP_address*

   Routes added this way will disappear after the system reboots. To prevent this from happening, create the startup file **S98router** in the **/etc/rc3.d** directory and type the command **route add** *network_IP_address* **-netmask** *netmask gateway_IP_address* into the boot script.

   After creating the **S98router** file, run the following command to set the **S98router** file to be executed:

   # **chmod a+x S98router**

   NOTE

   Run the following command to delete a route:

   # **route delete** *network_IP_address* **-netmask** *netmask gateway_IP_address*

----End

B.1.1.3 How to Query the Gateway of a Sun Workstation

Question

How do I query the gateway of a Sun workstation?

Answer

1. Log in to the OS as user **root** and open the terminal window.
2. Run the following command to query the workstation:
   # **netstat -nr**

   The following message will be displayed:

```
Routing Table: IPv4
  Destination           Gateway           Flags  Ref   Use   Interface
-------------------- -------------------- ----- ----- ------ ---------
10.71.224.0          10.71.225.24         U         1   1006  bge0
224.0.0.0            10.71.225.24         U         1      0  bge0
default              10.71.224.1          UG        1 114902
127.0.0.1            127.0.0.1            UH        6  25558  lo0
```

NOTE

- The contents displayed on the terminal will vary according to the route configuration.
- The gateway with **UG** listed in the **Flags** is the gateway of the workstation. In this example, the IP address of the workstation gateway is *10.71.224.1*. There are five flags (UGHDM) for a specified route.

----End

B.1.1.4 How to Check the NIC Type of a Server

Question

How do I check the NIC type of a server?

Answer

You can run the **more /etc/path_to_inst | grep network** command as user **root** to check the NIC type of a server.

B.1.2 System Settings of the Workstation

This topic covers FAQs about workstation system settings.

B.1.2.1 How to Boot Up the Workstation from the CD-ROM Drive

Question

How do I boot up the workstation from the CD-ROM drive?

Answer

1. At the # prompt, run the following command to display the **OK** prompt (OK>):

   # **init 0**

2. After the OK prompt is displayed, insert the installation DVD of Solaris OS into the CD-ROM drive.

3. Enter **boot cdrom** and press **Enter**.

----End

B.1.2.2 How to Enable Input Modes on Solaris OS

Question

How do I solve the problem that occurs when the switch between the Chinese and English input modes fails on Solaris OS?

Answer

1. In most cases, the problem occurs when input modes is disabled. Enable the input modes if they are disabled.
2. Run the following commands to enable the input modes:

   # **cd /usr/openwin/bin**

   # **./htt -nosm**

   NOTE

   This operation needs to be performed in an environment supporting GUIs. After the input modes are enabled, the **Htt** flag is displayed in the upper left corner of the screen. Press **Ctrl+Space** to switch between input modes. If the operation is performed on the emulation terminal WinaXe, press **Ctrl+Shift+Space** to switch between input modes.

----End

B.1.2.3 How to Set the Interface Language of Solaris OS

Question

How do I set the interface language of Solaris OS?

Answer

1. Power on the workstation, and start Solaris OS.
2. Choose **Options** > **Language**. A dialog box will be displayed prompting you to select a language.
3. Select the system language from the list box according to the conditions at your site.
4. Click **OK**.

   If you want to save the setting of the system language, select **Set selected language as default**.

----End

B.1.2.4 How to Call the GUI Management Tool in Solaris 10 OS

Question

How do I call the GUI management tool in Solaris 10 OS?

Answer

1 Log in to Solaris 10 OS through the GUI. Then, run the following command to call the GUI management tool:

```
# smc &
```

----End

B.1.2.5 How to Switch to the Multi-user Mode or Single-user Mode

Question

How do I switch to the multi-user mode or single-user mode?

Answer

- Run the following command to switch to the multi-user mode:

  ok> **boot**

- Run the following command to switch to the single-user mode:

  ok> **boot -s**

----End

B.1.2.6 How to Open the Terminal Window on the Desktop in the JDS

Question

How do I open the terminal window on the desktop in the Java Desk System (JDS)?

Answer

1 Open the desktop in the JDS.

1. Enter the user name for login, such as **root**.
2. Choose **Options** > **Session** > **Java Desktop System** to select the JDS.
3. Click **OK**. Enter the password for the user, such as **root**.
4. Click **OK** to log in to the desktop in the JDS.

2 Right-click on the desktop in the JDS and choose **Open Terminal** from the shortcut menu to open a terminal window.

----End

B.1.2.7 How to Operate the CD-ROM

Question

How do I operate the CD-ROM?

Answer

1. If the Sun workstation has a built-in CD-ROM drive, perform the following operation:

   The system automatically installs the CD-ROM to the **/cdrom** directory after startup. If there is a CD-ROM in the CD-ROM drive, view the contents of the CD-ROM after accessing the **/cdrom** directory.

2. If the Sun workstation has an external CD-ROM drive, perform the following operation:

   Power on the CD-ROM drive after the SCSI wire is connected. Then, power on the workstation. The system automatically identifies and installs the CD-ROM to the **/cdrom** directory after startup.

3. Use appropriate commands to open the CD-ROM drive.

   If there is a CD-ROM in the CD-ROM drive, run appropriate commands to open the CD-ROM drive.

   Verify that the CD-ROM is not being used by any program and exit the directory for the CD-ROM. Run the following command as user **root**:

   # **eject**

   Open the CD-ROM drive and take out the CD-ROM.

   NOTE

   If the system prompts "Device busy" and the CD-ROM cannot be ejected, run the following command as user **root**:

   # **svcadm disable volfs**

   Press the eject button on the drive panel to take out the CD-ROM.

   The drive becomes unavailable in this situation. Run the following command:

   # **svcadm enable volfs**

   The CD-ROM drive can then be used.

4. Install or start the system from the CD-ROM.

   Insert the CD-ROM to the drive, and then run the following command at the OK prompt on the workstation:

   OK> **boot cdrom**

   By doing this, you can install or start the system from the CD-ROM.

5. Check the SCSI device mounted on the workstation.

   Enter the following command at the OK prompt:

   OK> **probe-scsi**

   By doing this, you can check the SCSI device mounted on the workstation. This command is usually used to verify that the CD-ROM drive is correctly mounted.

----End

B.1.3 FTP and Telnet Service Configuration

This topic covers the FAQs about the FTP and Telnet service configuration.

B.1.3.1 How to Start/Stop the FTP, TFTP, SFTP, and Telnet Services

Question

How do I start/stop the FTP, TFTP, SFTP, and Telnet services?

Answer

Use the following methods to start/stop the FTP, TFTP, SFTP, and Telnet services. You are recommended to restore the original settings afterwards.

- Start the FTP, TFTP, SFTP, and Telnet services as follows:
  - Starting the FTP service
    1. Log in to Solaris OS as user **root**.
    2. Run the following command to start the FTP service:

       # **svcadm enable ftp**
  - Starting the TFTP service
    1. Log in to Solaris OS as user **root**.
    2. Run the following command to verify that the TFTP service is running:

       # **svcs -a|grep tftp**

       The TFTP service is not started if there is no response.
    3. Run the following command to modify the **inetd** configuration file:

       # **vi /etc/inetd.conf**

       Delete # to the left of TFTPD.
    4. Run the following command to start the TFTP service:

       # **/usr/sbin/inetconv -i /etc/inetd.conf**

       # **svcadm enable svc:/network/tftp/udp6:default**
    5. Run the following command to verify that the TFTP service is running:

       # **svcs -a|grep tftp**

       The TFTP service is running if a message is displayed:

       ```
       online         22:07:11 svc:/network/tftp/udp6:default
       ```
  - Starting the SFTP service
    1. Log in to Solaris OS as user **root**.
    2. Run the following command to start the SFTP service:

       # **vi /etc/ssh/sshd_config**

       Modify the "PAMAuthenticationViaKBDInt yes" to "PAMAuthenticationViaKBDInt no", and run the **:wq!** command to save the settings and exit.

       # **svcadm restart network/ssh**

svcadm enable network/ssh

- Starting the Telnet service
  1. Log in to Solaris OS as user **root**.
  2. Run the following command to start the Telnet service:

     # **svcadm enable telnet**

- Stop the FTP, TFTP, SFTP, and Telnet services as follows:
  - Stopping the FTP service
    1. Log in to Solaris OS as user **root**.
    2. Run the following command to stop the FTP service:

       # **svcadm disable ftp**
  - Stopping the TFTP service
    1. Log in to Solaris OS as user **root**.
    2. Run the following command to verify that the TFTP service is stopped:

       # **svcs -a|grep tftp**

       The TFTP service is running if a message similar to the following is displayed:

       ```
       online         22:07:11 svc:/network/tftp/udp6:default
       ```
    3. Run the following command to modify the **inetd** configuration file:

       # **vi /etc/inetd.conf**

       Add # to the left of TFTPD.
    4. Run the following command to verify that the TFTP service is stopped:

       # **svcs -a|grep tftp**

       If there is no response, the TFTP service is stopped.
  - Stopping the SFTP service
    1. Log in to Solaris OS as user **root**.
    2. Run the following command to stop the SFTP service:

       # **svcadm disable network/ssh**
  - Stopping the Telnet service
    1. Log in to Solaris OS as user **root**.
    2. Run the following command to stop the Telnet service:

       # **svcadm disable telnet**

B.1.3.2 How to Enable and Disable the FTP/Telnet Authority of user root on Solaris OS

Question

How do I enable and disable the FTP/Telnet authority for user **root** on Solaris OS?

Answer

1 Enable or disable the FTP authority for user **root** as follows:

- Enabling the FTP authority for user **root**

1. Log in to Solaris OS as user **root**.
2. Run the following commands to enable the FTP authority for user **root**:

```
# svcadm enable ftp
# sed "/^root/s//#root/g" /etc/ftpd/ftpusers > /tmp/ftpusers
# cp /tmp/ftpusers /etc/ftpd/ftpusers
```

- Disabling the FTP authority for user **root**

1. Log in to Solaris OS as user **root**.
2. Run the following commands to enable the FTP authority for user **root**:

```
# svcadm disable ftp
# sed "/^#root/s//root/g" /etc/ftpd/ftpusers > /tmp/ftpusers
# cp /tmp/ftpusers /etc/ftpd/ftpusers
```

2 Enable or disable the Telnet authority for user **root** as follows:

- Enabling the Telnet authority for user **root**

1. Log in to the Solaris OS as user **root**.
2. Run the following commands to enable the Telnet authority of user **root**:

```
# svcadm enable telnet
# sed "/^CONSOLE/s//#CONSOLE/g" /etc/default/login > /tmp/login
# cp /tmp/login /etc/default/login
```

- Disabling the Telnet authority for user **root**

1. Log in to Solaris OS as user **root**.
2. Run the following commands to disable the Telnet authority of the **root** user:

```
# svcadm disable telnet
# sed "/^#CONSOLE/s//CONSOLE/g" /etc/default/login > /tmp/login
# cp /tmp/login /etc/default/login
```

----End

B.1.3.3 How to Transfer Files by Means of FTP

Question

How do I transfer files by means of FTP?

NOTE

The available FTP modes are ASCII (default) and binary.

To ensure that files are available after transfer, determine the FTP transfer mode before transferring files. Generally, license files are transferred in ASCII mode whereas binary files such as NMS installation programs and databases **interfaces** files are transferred in binary mode.

Answer

1 Run the following command to connect to the server by means of FTP:

ftp *server IP address*

Enter the user name and password of the server.

2 Set the FTP transfer mode.

- To use the ASCII mode, run the **ascii** command.
- To use the binary mode, run the **bin** command.

3 Go to the path to files to be transferred.

lcd *path of files to be transferred*

4 Go to the path where the files are to be transferred.

cd *path to which the files are to be transferred*

5 Run the following **put** command to transfer files:

put *names of files to be transferred*

6 After the files are transferred, run the **quit** command to break the FTP connection.

----End

B.1.4 Usage and Maintenance of Workstation

This topic covers the FAQs about the usage and maintenance of the workstation.

B.1.4.1 How to View the Versions and Release Date of the Solaris OS

Question

How do I view the versions and release date of Solaris OS?

Answer

1 Open a terminal window on Solaris OS.

2 Run the following command to view the version information about Solaris OS:

```
# uname -a
```

The Solaris version is Solaris 10 and the core patch version is 141414-07 if the following message is displayed:

```
SunOS NMSServer 5.10 Generic_141414-07 sun4v sparc SUNW,SPARC-Enterprise-T5220
```

3 Run the following command to view the release date of Solaris OS:

more */etc/release*

A message similar to the following will be displayed:

```
......
Copyright 2007 Sun Microsystems, Inc.  All Rights Reserved.
        Use is subject to license terms.
            Assembled 16 August 2007
```

----End

B.1.4.2 How to Change the System Time and Time Zone of Solaris OS

Question

How do I to change the system time and time zone of Solaris OS?

Answer

- To change the time zone of Solaris OS, perform the following operations:
  1. Run the following command to modify the **/etc/TIMEZONE** file:
     ```
     # vi /etc/TIMEZONE
     ```
  2. Change the value of **TZ** to the local time zone. For example, set **TZ** to **PRC**.
  3. Press **Esc**. Press **Shift+;** and enter **wq!**. Then, press **Enter** to forcibly save and close the file.
  4. Run the following commands to restart the server:
     ```
     # sync;sync;sync;sync
     # shutdown -y -g0 -i6
     ```
  5. Run the following command to verify that the time zone is correct:
     ```
     # echo $TZ
     ```
     If the time zone is incorrect, verify that the **/etc/TIMEZONE** file and GMT are set properly.
- To change the system time of Solaris OS, perform the following operations:
  1. Run the **date** command to set the system date and time.
     For example, to set the system date and time to **2005-11-17 16:30:43**, run the following command:
     ```
     # date 111716302005.43
     ```
     The following message will be displayed:
     ```
     Mon Nov 17 16:30:43 CST 2005
     ```
  2. Optional: Run the following commands to restart the server:
     ```
     # sync;sync;sync;sync
     # shutdown -y -g0 -i6
     ```

----End

B.1.4.3 How to View Hardware Configurations for the Sun Workstation

Question

How do I view hardware configurations for the Sun workstation?

Answer

1 Log in to the Sun workstation as the **root** user. Then, run the following commands:

cd /usr/platform/`uname -i`/sbin

./prtdiag

A message similar to the following is displayed:

```
System Configuration: Sun Microsystems  sun4u Sun Fire V445
System clock frequency: 199 MHZ
Memory size: 8GB

==================================== CPUs ====================================
               E$          CPU                    CPU
CPU  Freq      Size        Implementation         Mask    Status      Location
---  --------  ----------  ---------------------  -----   ------      --------
0    1592 MHz  1MB         SUNW,UltraSPARC-IIIi    3.4    on-line     MB/C0/P0
1    1592 MHz  1MB         SUNW,UltraSPARC-IIIi    3.4    on-line     MB/C1/P0
2    1592 MHz  1MB         SUNW,UltraSPARC-IIIi    3.4    on-line     MB/C2/P0
3    1592 MHz  1MB         SUNW,UltraSPARC-IIIi    3.4    on-line     MB/C3/P0

================================= IO Devices =================================
Bus     Freq  Slot +      Name +
Type    MHz   Status      Path                           Model
------  ----  ----------  -----------------------------  --------------------
pci     199   MB          pci14e4,1668 (network)
              okay        /pci@1e,600000/pci@0/pci@1/pci@0/network@4

pci     199   MB          pci14e4,1668 (network)
              okay        /pci@1e,600000/pci@0/pci@1/pci@0/network@4,1

pci     199   MB/PCI2     SUNW,XVR-100 (display)         SUNW,375-3290
              okay        /pci@1e,600000/pci@0/pci@1/pci@0/pci@8/SUNW,XVR-100@1

pci     199   MB          pci10b9,5229 (ide)
              okay        /pci@1f,700000/pci@0/pci@1/pci@0/ide@1f

pci     199   MB          pci14e4,1668 (network)
              okay        /pci@1f,700000/pci@0/pci@2/pci@0/network@4

pci     199   MB          pci14e4,1668 (network)
              okay        /pci@1f,700000/pci@0/pci@2/pci@0/network@4,1

pciex   199   MB          scsi-pciex1000,58 (scsi-2)     LSI,1068E
              okay        /pci@1e,600000/pci@0/pci@2/scsi@0


============================ Memory Configuration ============================
Segment Table:
------------------------------------------------------------------------
Base Address       Size       Interleave Factor  Contains
------------------------------------------------------------------------
0x0                2GB                4          BankIDs 0,1,2,3
0x1000000000       2GB                4          BankIDs 16,17,18,19
0x2000000000       2GB                4          BankIDs 32,33,34,35
0x3000000000       2GB                4          BankIDs 48,49,50,51

Bank Table:
------------------------------------------------------------
```

```
           Physical Location
ID       ControllerID  GroupID   Size       Interleave Way
-------------------------------------------------------------
0        0             0         512MB           0,1,2,3
1        0             1         512MB
2        0             1         512MB
3        0             0         512MB
16       1             0         512MB           0,1,2,3
17       1             1         512MB
18       1             1         512MB
19       1             0         512MB
32       2             0         512MB           0,1,2,3
33       2             1         512MB
34       2             1         512MB
35       2             0         512MB
48       3             0         512MB           0,1,2,3
49       3             1         512MB
50       3             1         512MB
51       3             0         512MB

Memory Module Groups:
-------------------------------------------------
ControllerID   GroupID  Labels         Status
-------------------------------------------------
0              0        MB/C0/P0/B0/D0 okay
0              0        MB/C0/P0/B0/D1 okay
0              1        MB/C0/P0/B1/D0 okay
0              1        MB/C0/P0/B1/D1 okay
1              0        MB/C1/P0/B0/D0 okay
1              0        MB/C1/P0/B0/D1 okay
1              1        MB/C1/P0/B1/D0 okay
1              1        MB/C1/P0/B1/D1 okay
2              0        MB/C2/P0/B0/D0 okay
2              0        MB/C2/P0/B0/D1 okay
2              1        MB/C2/P0/B1/D0 okay
2              1        MB/C2/P0/B1/D1 okay
3              0        MB/C3/P0/B0/D0 okay
3              0        MB/C3/P0/B0/D1 okay
3              1        MB/C3/P0/B1/D0 okay
3              1        MB/C3/P0/B1/D1 okay

============================== USB Devices ==============================

Name          Port#
------------  -----
hub           HUB0
```

Details about the message are as follows:

- The following information indicates a workstation model. In this example, the workstation model is **Sun Fire V445**.

  ```
  System Configuration: Sun Microsystems  sun4u Sun Fire V445
  System
  ```

- The following information indicates the system clock frequency. In this example, the workstation clock frequency is **199 MHZ**.

  ```
  System clock frequency: 199 MHZ
  ```

- The following information indicates the memory configuration for the workstation. In this example, the memory configuration for the workstation is **8GB**.

  ```
  Memory size: 8GB
  ```

- The following information indicates the CPU configuration for the workstation. In this example, the CPU configuration for the workstation is **4Core**.

  ```
  ==================================== CPUs ====================================
                E$          CPU                    CPU
  CPU  Freq     Size        Implementation         Mask    Status      Location
  ---  --------  ----------  ---------------------  -----   ------      --------
  ```

```
0    1592 MHz  1MB         SUNW,UltraSPARC-IIIi    3.4    on-line     MB/C0/P0
1    1592 MHz  1MB         SUNW,UltraSPARC-IIIi    3.4    on-line     MB/C1/P0
2    1592 MHz  1MB         SUNW,UltraSPARC-IIIi    3.4    on-line     MB/C2/P0
3    1592 MHz  1MB         SUNW,UltraSPARC-IIIi    3.4    on-line     MB/C3/P0
```

NOTE

Hardware configurations for a workstation vary according to the workstation model.

----End

B.1.4.4 How to Check Whether the Hard Disk of the Sun Workstation Is Damaged

Question

How do I check whether the hard disk of the Sun workstation is damaged?

Answer

1 During the operation of the Sun workstation, inappropriate powering-off usually causes damage to the hard disk and even renders the Sybase database unavailable. Run the **iostat -E** command to check whether the hard disk of the OS is damaged.

Log in to the Sun workstation as user **root** and run the following command:

iostat -En

A message similar to the following will be displayed:

```
c0t0d0           Soft Errors: 0 Hard Errors: 0 Transport Errors: 0
Vendor: FUJITSU  Product: MAY2073RCSUN72G  Revision: 0501 Serial No: 0742S0EPT7
Size: 73.40GB <73400057856 bytes>
Media Error: 0 Device Not Ready: 0 No Device: 0 Recoverable: 0
Illegal Request: 0 Predictive Failure Analysis: 0
c0t1d0           Soft Errors: 0 Hard Errors: 0 Transport Errors: 0
Vendor: FUJITSU  Product: MAY2073RCSUN72G  Revision: 0501 Serial No: 0742S0EPL9
Size: 73.40GB <73400057856 bytes>
Media Error: 0 Device Not Ready: 0 No Device: 0 Recoverable: 0
Illegal Request: 0 Predictive Failure Analysis: 0
c0t2d0           Soft Errors: 0 Hard Errors: 0 Transport Errors: 0
Vendor: FUJITSU  Product: MBB2073RCSUN72G  Revision: 0505 Serial No: 0805A011C0
Size: 73.40GB <73400057856 bytes>
Media Error: 0 Device Not Ready: 0 No Device: 0 Recoverable: 0
Illegal Request: 0 Predictive Failure Analysis: 0
c1t0d0           Soft Errors: 1 Hard Errors: 0 Transport Errors: 1
Vendor: TSSTcorp Product: CD/DVDW TS-T632A Revision: SR03 Serial No:
Size: 0.00GB <0 bytes>
Media Error: 0 Device Not Ready: 0 No Device: 0 Recoverable: 0
Illegal Request: 1 Predictive Failure Analysis: 0
c0t3d0           Soft Errors: 0 Hard Errors: 0 Transport Errors: 0
Vendor: FUJITSU  Product: MBB2073RCSUN72G  Revision: 0505 Serial No: 0805A011DH
Size: 73.40GB <73400057856 bytes>
Media Error: 0 Device Not Ready: 0 No Device: 0 Recoverable: 0
Illegal Request: 0 Predictive Failure Analysis: 0
```

NOTE

The hard disk is damaged if the information to the rights of **Hard Errors** is not **0**. Send the message series files in the **/var/adm** directory to Huawei engineers so that they can apply for a spare part to replace the hard disk on site.

----End

B.1.4.5 How to Check the Partition of Solaris OS

Question

How do I check the partition of Solaris OS?

Answer

1. Log in to Solaris OS as user **root**.
2. Run the following command to check all disks of the server:
   # **format**

   The following message will be displayed:

```
Searching for disks...done


AVAILABLE DISK SELECTIONS:
       0. c0t0d0 <SUN146G cyl 14087 alt 2 hd 24 sec 848>
          /pci@0,600000/pci@0/pci@8/pci@0/scsi@1/sd@0,0
       1. c0t1d0 <SEAGATE-ST914602SSUN146G-0603 cyl 14087 alt 2 hd 24 sec 848>
   /pci@0,600000/pci@0/pci@8/pci@0/scsi@1/sd@1,0
       2. c1t4d0 <ENGENIO-INF-01-00-0619 cyl 51198 alt 2 hd 128 sec 64>
       /pci@2,600000/SUNW,qlc@0/fp@0,0/ssd@w201600a0b8293a52,0
       3. c2t5d0 <ENGENIO-INF-01-00-0619 cyl 51198 alt 2 hd 128 sec 64>
  /pci@2,600000/SUNW,qlc@0,1/fp@0,0/ssd@w202700a0b8293a52,0
Specify disk (enter its number):
```

3. Enter **0** and press **Enter** to view the information about the c1t0d0 disk. The following message will be displayed:

```
selecting c0t0d0
[disk formatted]
/dev/dsk/c0t0d0s1 is in use by dump. Please see dumpadm(1M).


FORMAT MENU:
        disk       - select a disk
        type       - select (define) a disk type
        partition  - select (define) a partition table
        current    - describe the current disk
        format     - format and analyze the disk
        repair     - repair a defective sector
        label      - write label to the disk
        analyze    - surface analysis
        defect     - defect list management
        backup     - search for backup labels
        verify     - read and display labels
        save       - save new disk/partition definitions
        inquiry    - show vendor, product and revision
        volname    - set 8-character volume name
        !<cmd>    - execute<cmd>, then return
        quit
        format>
```

4. Enter **p** and press **Enter** to select the partition list. The following message will be displayed:

```
PARTITION MENU:

0 - change `0' partition
1 - change `1' partition
2 - change `2' partition
3 - change `3' partition
4 - change `4' partition
5 - change `5' partition
6 - change `6' partition
```

```
7 - change `7' partition
select - select a predefined table
modify - modify a predefined partition table
name - name the current table
print - display the current table
label - write partition map and label to the disk
!<cmd>   - execute<cmd>, then return
quit
partition>
```

5 Enter **p** and press **Enter** to view the partition information of disk c1t0d0, including the raw partition information. The following message will be displayed:

```
Current partition table (original):
Total disk cylinders available: 14087 + 2 (reserved cylinders)

Part      Tag    Flag     Cylinders         Size            Blocks
  0       root    wm       0 -  3091       30.01GB    (3092/0/0)   62928384
  1       swap    wu    3092 -  6389       32.01GB    (3298/0/0)   67120896
  2     backup    wm       0 - 14086      136.71GB    (14087/0/0) 286698624
  3          -    wu       0 - 14086      136.71GB    (14087/0/0) 286698624
  4          -    wu   14083 - 14086       39.75MB    (4/0/0)         81408
  5 unassigned    wm    6390 - 10511       40.00GB    (4122/0/0)   83890944
  6        var    wm   10512 - 13603       30.01GB    (3092/0/0)   62928384
  7 unassigned    wm       0                0         (0/0/0)             0

partition>
```

6 Enter **q** to exit the c1t0d0 disk directory. The following message will be displayed:

```
FORMAT MENU:
        disk       - select a disk
        type       - select (define) a disk type
        partition  - select (define) a partition table
        current    - describe the current disk
        format     - format and analyze the disk
        repair     - repair a defective sector
        label      - write label to the disk
        analyze    - surface analysis
        defect     - defect list management
        backup     - search for backup labels
        verify     - read and display labels
        save       - save new disk/partition definitions
        inquiry    - show vendor, product and revision
        volname    - set 8-character volume name
        !<cmd>    - execute<cmd>, then return
        quit
        format>
```

7 Enter **q** and exit the **format** command.

8 Repeat Step 2 to Step 7, and select other disks to check the partitions.

----End

B.1.4.6 How to Check the Remaining Space of a Disk

Question

How do I check the remaining space of a disk?

Answer

Run the **df -hk** command to check the remaining space of a disk.

For example, run the **df -hk /opt** command to check the remaining space of the **/opt** partition.

B.1.4.7 How to Decompress Files

Question

Compressed files are usually in ***.tar**, ***.tar.gz**, or ***.zip** format. How do I decompress these files?

Answer

1. To decompress a ***.tar** file, perform the following operation:

   The following uses the **abc.tar** file as an example. Run the following command:

   # **tar xvf abc.tar**

2. To decompress a ***.tar.gz** file, perform the following operation:
   - The following uses the **abc.tar.gz** file as an example. Run the following commands:

     # **gunzip abc.tar.gz**

     # **tar xvf abc.tar**
   - The following uses the **solaris10_HuaweiPatch9.0.tar.gz** file as an example. Run the following command:

     # **gzcat solaris10_HuaweiPatch9.0.tar.gz | tar xBpf -**

3. To decompress a ***.zip** file, perform the following operation:

   The following uses the **abc.zip** file as an example. Run the following command:

   # **unzip abc.zip**

----End

B.1.4.8 How to Remotely Log In to the System as User root

Question

Remote login fails after the system is restarted. How do I remotely log in to the system as user **root**?

Answer

1. Log in to the server from the controller. Ensure that the server is running.
2. Check whether user **root** has rights to log in to the server. Ensure that user **root** has rights to log in to the server by means of FTP.
3. Verify the routing information about the server. Ensure that the route is reachable.

----End

B.1.4.9 How to Access the OS from the Controller

Question

How do I access the OS from the controller IP address if login to the OS from the system IP address fails?

Answer

1. Log in to the controller.
   - For M4000 servers, log in to the controller in Telnet or SSH mode.
   - For T5220 servers, log in to the controller in SSH mode.
2. Access the OS.
   - For M4000 servers, run the **console -d 0** command to access the OS.
   - For T5220 servers, run the **start /SP/console** command to access the OS.

----End

B.1.4.10 How to Switch Between the Console, OK Prompt, and # Prompt

Question

How do I switch between the console, **OK** prompt, and # prompt?

NOTE

The switching method varies based on the type of the Sun server used.

Answer

- T5220 Servers
  - Switch from the console to the **OK** prompt.
    1. Log in to the IP address of the system controller in Secure Shell (SSH) mode. Perform the following operations to display the **OK** prompt:

       NOTE

       The T5220 server does not support the login to the system controller in Telnet mode. Log in to the system controller by performing the following operation:

       - Install the SSH client tool, such as the PuTTY, in the console on Windows. Then, you can log in to the system controller through the tool.
       - Run the **ssh *IP address of the system controller*** command on the terminal console of another Sun server to log in to the system controller. If a message similar to the following is displayed, enter **yes** to continue:

         ```
         The authenticity of host '10.71.35.12 (10.71.35.12)' can't be
         established.
         RSA key fingerprint is 0b:23:07:0c:27:72:44:3f:d1:aa:
         12:99:ed:dd:c0:5a.
         Are you sure you want to continue connecting (yes/no)?
         ```

    2. In the command line interface (CLI) that is displayed, enter the user name and password of the system controller. By default, the user name is *root* and the default password is *changeme*.
    3. Enter **set /HOST/bootmode state=reset_nvram script="setenv auto-boot? false"**.

NOTE

There must be a space between **?** and **false**.

The following message will be displayed:

```
Set 'state' to 'reset_nvram'
Set 'script' to 'setenv auto-boot? false'
```

4. Enter **start /SYS**.

   The following message will be displayed:

   ```
   Are you sure you want to start /SYS (y/n)?
   ```

5. Enter **y** to start the server.

   If the message **start: Target already started** is displayed, the system is running. Perform the following operations:

   Enter **stop /SYS**. The following message will be displayed:

   ```
   Are you sure you want to stop /SYS (y/n)?
   ```

   Enter **y**. The following message will be displayed:

   ```
   Stopping /SYS
   ```

   Enter **show /HOST status** repeatedly to check the system status. After a message containing **status = Powered off** is displayed, proceed with the next step.

   Enter **start /SYS**. The following message will be displayed:

   ```
   Are you sure you want to start /SYS (y/n)?
   ```

   Enter **y** to start the server.

6. Enter **start /SP/console**.

   The following message will be displayed:

   ```
   Are you sure you want to start /SP/console (y/n)?
   ```

7. Enter **y** and press **Enter**.

   The following message will be displayed:

   ```
   Serial console started. To stop, type #.
   ...
   Setting NVRAM parameters to default values.


   SPARC Enterprise T5220, No Keyboard
   Copyright 2008 Sun Microsystems, Inc.  All rights reserved.
   OpenBoot 4.28.0, 8064 MB memory available, Serial #85369820.
   Ethernet address 0:21:28:16:a3:dc, Host ID: 8516a3dc.


   auto-boot? =            false
   {0} ok
   ```

- Switch from the **OK** prompt to the # prompt.

  Run the following command:

  `ok` **setenv auto-boot? true**

  NOTE

  There must be a space between **?** and **true**.

  Run the following command to verify that the parameter settings have taken effect:

  `ok` **printenv**

  Run the following command to enable the system to perform another self-check:

  `ok` **reset-all**

  The system will display the **OK** prompt. Enter **boot** to display the # prompt.

- Switch from the # prompt to the console.

  Run the following command:

  # **#.**

  NOTE

  Enter **#** and **.**.

- Switch from the # prompt to the **OK** prompt.

  Run the following command:

  # **init 0**

- M4000 Servers
  - Switch from the console to the **OK** prompt.
    1. Run the **telnet** ***IP address of the controller*** command on the console to log in to the controller IP address by means of Telnet.

       The following message will be displayed:

       ```
       Login:
       ```

    2. Enter the user name, that is, **eis-installer**.

       The following message will be displayed:

       ```
       Password:
       ```

    3. Enter the password of the **eis-installer** user.

       The following message will be displayed:

       ```
       XSCF>
       ```

    4. Enter **showdomainmode -d 0**.

       The following message will be displayed:

       ```
       Host-ID             :8501c2de
       Diagnostic Level    :min
       Secure Mode         :off (host watchdog: unavailable  Break-
       signal:receive)
       Autoboot            :on
       CPU Mode            :auto
       ```

       NOTE

       If **Secure Mode** is **on**, perform the following:

       1. Enter **setdomainmode -d 0 -m secure=off**.

          The following message will be displayed:

          ```
          Diagnostic Level    :min        -> -
          Secure Mode         :on         -> off
          Autoboot            :on         -> -
          CPU Mode            :auto
          The specified modes will be changed.
          Continue? [y|n]
          ```

       2. Enter **y**.

          The following message will be displayed:

          ```
          configured.
          Diagnostic Level    :min
          Secure Mode         :off (host watchdog: unavailable  Break-
          signal:receive)
          Autoboot            :on (autoboot:on)
          CPU Mode            :auto
          ```

    5. Enter **showdomainstatus -a**.

       The following message will be displayed:

```
DID         Domain Status
00          Running
01          -
```

NOTE

The following message will be displayed:

```
DID         Domain Status
00          Powered Off
01          -
```

Run the **poweron -d 0** command. Then, run the **showdomainstatus -a** command repeatedly to check the system status until the system displays the status as **running**. Proceed with the next step.

6. Enter **sendbreak -d 0**.

   The following message will be displayed:

   ```
   Send break signal to DomainID 0? [y|n]
   ```

7. Enter **y**.
8. Enter **console -d 0 -f**.

   The following message will be displayed:

   ```
   Connect to DomainID 0? [y|n]
   ```

9. Enter **y** and press **Enter**.

   ```
   OK
   ```

- Switch from the **OK** prompt to the # prompt.

  Run the following command:

  ok **setenv auto-boot? true**

  NOTE

  There must be a space between **?** and **true**.

  Run the following command to verify that the parameter settings have taken effect:

  ok **printenv**

  Run the following command to enable the system to perform another self-check:

  ok **reset-all**

  The system will display the **OK** prompt. Enter **boot** to display the # prompt.

- Switch from the # prompt to the console.

  Run the following command:

  # **#.**

  NOTE

  Enter **#** and **.**.

- Switch from the # prompt to the **OK** prompt.

  Run the following command:

  # **init 0**

- V890 Servers
  - Switch from the console to the **OK** prompt.

    1. Run the **telnet *IP address of the controller*** command on the console to log in to the controller IP address by means of Telnet.

       The following message will be displayed:

       ```
       Login:
       ```

2. Enter the user name **admin** and password. Generally, the default password of the RSC is **admin123**.
3. Enter **console** to display the **OK** prompt.

   NOTE

   In certain conditions, the following message will be displayed:

   ```
   Warning: User < > currently has write permission to this console
   and
   forcibly removing them will terminate any current write actions
   and all work will be lost.
   Would you like to continue? [y/n]
   ```

   Enter **y**.

   If the V890 server is used for the first time, the system will display the **OK** prompt.

   If the V890 server is installed with the operating system (OS), the system will display the # prompt. Perform the following operations to display the **OK** prompt:

   Enter **~.** to display the **RSC** prompt. (If the ALOM control card is used, enter **#.**.)

   Run the following command at the **RSC** prompt:

   `rsc>` **break**

   The following message will be displayed:

   ```
   Are you sure you want to send a break to the system [y/n]?
   ```

   Enter **y**.

   `rsc>` **console**

- Switch from the **OK** prompt to the # prompt.

  Run the following command:

  `ok` **setenv auto-boot? true**

  NOTE

  There must be a space between **?** and **true**.

  Run the following command to verify that the parameter settings have taken effect:

  `ok` **printenv**

  Run the following command to enable the system to perform another self-check:

  `ok` **reset-all**

  The system will display the **OK** prompt. Enter **boot** to display the # prompt.
- Switch from the # prompt to the console.

  Run the following command:

  # **#.**

  NOTE

  Enter **#** and **.**.
- Switch from the # prompt to the **OK** prompt.

  Run the following command:

  # **init 0**

- V240, V245, V440, and V445 Servers
  - Switch from the console to the **OK** prompt.
    1. Run the **telnet** ***IP address of the controller*** command on the console to log in to the controller IP address by means of Telnet.

       The following message will be displayed:

```
Login:
```

2. Enter the user name and password. The default user name and password are **admin**.
3. Enter **console -f** to display the **OK** prompt.

   NOTE

   In certain conditions, the following message will be displayed:

   ```
   Warning: User < > currently has write permission to this console
   and
   forcibly removing them will terminate any current write actions
   and all work will be lost.
   Would you like to continue? [y/n]
   ```

   Enter **y**.

   If the intended server is used for the first time, the system will display the **OK** prompt.

   If the server is installed with the OS, the system will display the # prompt. Perform the following operations to display the **OK** prompt:

   Enter **#.** to display the ALOM prompt. (If the RSC control card is used, enter **~.**.)

   Run the following command at the ALOM prompt:

   sc> **break**

   The following message will be displayed:

   ```
   Are you sure you want to send a break to the system [y/n]?
   ```

   Enter **y**.

   sc> **console -f**

- Switch from the **OK** prompt to the # prompt.

  Run the following command:

  ok **setenv auto-boot? true**

  NOTE

  There must be a space between **?** and **true**.

  Run the following command to verify that the parameter settings have taken effect:

  ok **printenv**

  Run the following command to enable the system to perform another self-check:

  ok **reset-all**

  The system will display the **OK** prompt. Enter **boot** to display the # prompt.

- Switch from the # prompt to the console.

  Run the following command:

  # **#.**

  NOTE

  Enter **#** and **.**.

- Switch from the # prompt to the **OK** prompt.

  Run the following command:

  # **init 0**

----End

B.1.4.11 How to Use the vi Editor

Question

How do I use the vi editor?

Answer

Run the following command to open the vi editor:

```
vi file name
```

- If a file with the same filename exists, run the **vi** command to open and edit the file.
- If a file with the same filename does not exist, run the **vi** command to create and edit a file.

The edit commands are as follows:

- The command for opening the vi editor is as follows:

  vi *file name*

- The command for entering the command mode is as follows.

Command	Function
ESC	Press **ESC** to exit the text input mode and enter the command mode.

- The commands for inserting text are as follows (must be run in command mode).

Command	Function
a	Appends text at the cursor (append).
A	Appends text at the end of the line where the cursor locates.
i	Adds text in front of the cursor (insert).
I	Adds text to the front of the first non-null character in the line where the cursor locates.
o	Adds text at the beginning of the next line where the cursor locates (open).
O	Adds text at the beginning of the previous line where the cursor locates.

- The commands for moving the cursor are as follows (must be run in command mode).

Command	Function
h	Moves the cursor to the left.
j	Moves the cursor downwards.
k	Moves the cursor upwards.
l	Moves the cursor to the right.

Command	Function
Line number G	Moves the cursor to a specified line. For example, **1G** moves the cursor to the first line.
G	Moves the cursor to the end of the file.

- The commands for deleting texts are as follows (must be run in command mode).

Command	Function
x	Deletes the character where the cursor is located.
dd	Deletes the line where the cursor is located.

- The commands for quitting the vi editor are as follows and must be run in command mode. You are recommended to press **ESC** before running any command listed in **Table B-1**.

Table B-1 Commands for quitting the vi editor

Command	Function
:wq	Saves changes and quits the vi editor.
:q	Quits the vi editor without saving changes.
:q!	Forcibly quits the vi editor without saving changes.
:w	Saves changes without quitting the vi editor.

B.1.4.12 How to Use the Text Editor

Question

How do I use the text editor?

NOTE

Use the text editor only through the GUI.

The text editor is recommended because it is easier to use than the vi editor.

Answer

Run the following command to open the text editor:

```
dtpad file name
```

- If a file with the same filename exists, run the **dtpad** command to open and edit the file.
- If a file with the same filename does not exist, run the **dtpad** command to create and edit a file.

B.1.4.13 How to Query the Process Status

Question

How do I query the process status?

Answer

Run the **ps -ef | grep** ***process name*** command to query the process status.

For example, run the **ps -ef | grep sysmonitor** command to query the status of the **sysmonitor** process.The following message will be displayed:

```
 nmsuser 17156 17032   0 22:13:59 pts/3      0:00 grep sysmonitor  nmsuser 11972
1    0 04:38:10 pts/2      13:00 imap_sysmonitor -cmd start
```

- **imap_sysmonitor** indicates information about the process, where **17156** is the process ID.

  NOTE

  Process information will be displayed if the process is running.

- **grep sysmonitor** indicates the query operation performed by the user and can be ignored.

B.1.4.14 How to Forcibly End a Process

Question

How do I forcibly end a process?

Answer

Run the **kill -9** ***process ID*** command to forcibly end a process.

B.2 Veritas HA System

This topic covers FAQs about the Veritas HA system.

B.2.1 License Management
This topic describes the FAQs about license management.

B.2.2 System Settings
This topic describes the FAQs about the system settings in the HA system.

B.2.1 License Management

This topic describes the FAQs about license management.

B.2.1.1 How to Check the Veritas License

B.2.1.1 How to Check the Veritas License

Question

How to check the Veritas license?

Answer

1 Run the following commands to query the details about the Veritas license.

Do as follows for Veritas license 5.1:

- If the displayed information does not contain **VXKEYLESS = Enabled**, the license is a permanent formal license.
- If the displayed information contains **VXKEYLESS = Enabled**, the license is a temporary license and you must replace it with a formal license in time.

Do as follows for Veritas license 5.0:

- If **PERMANENT** is displayed in the **License Type** field, it indicates the licenses of these components are permanent formal licenses.
- If **DEMO** is displayed in the **License Type** field, it indicates that this license is a temporary license. In this case, the expiry time of the license is also displayed. You need to replace the temporary license with the formal license in time.

vxlicrep

The following message will be displayed:

```
Symantec License Manager vxlicrep utility version 3.02.34.0
Copyright (C) 1996-2008 Symantec Corporation. All rights reserved.

Creating a report on all VERITAS products installed on this system

 ------------------**********************------------------

   License Key                       = XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-X
   Product Name                      = VERITAS Storage Foundation Enterprise HA
   Serial Number                     = 2851
   License Type                      = PERMANENT
   OEM ID                            = 2006
   Site License                      = YES
   Editions Product                  = YES

 Features :=
   Reserved                          = 0
   CPU Count                         = Not Restricted
   Platform                          = un-used
   VxVM#VERITAS Volume Manager       = Enabled
   Global Cluster Option#VERITAS Cluster Server = Enabled

   VXFS#VERITAS File System          = Enabled
   Version                           = 5.1
   Tier#VERITAS Cluster Server       = Unused
   Mode#VERITAS Cluster Server       = VCS
   VERITAS Storage Foundation Enterprise HA = Enabled
   Storage Expert#VERITAS Volume Manager = Enabled
   QLOG#VERITAS File System          = Enabled
   PGR#VERITAS Volume Manager        = Enabled
   Dynamic Lun Expansion#VERITAS Volume Manager = Enabled
   Hardware assisted copy#VERITAS Volume Manager = Enabled
   Cross-platform Data Sharing#VERITAS Volume Manager = Enabled
   File Change Log#VERITAS File System = Enabled
   Cross-platform Data Sharing#VERITAS File System = Enabled
   Extra-Big File Systems#VERITAS File System = Enabled
   Multi-Volume Support#VERITAS File System = Enabled
   FASTRESYNC#VERITAS Volume Manager   = Enabled
   DGSJ#VERITAS Volume Manager       = Enabled
   VXCKPT#VERITAS File System        = Enabled
   Quality of Storage Service#VERITAS File System = Enabled
   VVS_CONFIG#VERITAS Volume Manager   = Enabled
   VXKEYLESS                         = Enabled
```

```
----------------**********----------------

  Product Name                  = VERITAS Volume Manager
  License Type                  = PERMANENT

Features :=
  PGR                           = Enabled
  PGR_TRAINING                  = Enabled
  Site Awareness                = Enabled
  DGSJ                          = Enabled
  VVS_CONFIG                    = Enabled
  Hardware assisted copy        = Enabled
  RAID5SNAP                     = Enabled
  Storage Expert                = Enabled
  Dynamic Lun Expansion         = Enabled
  Cross-platform Data Sharing   = Enabled


----------------**********----------------

  Product Name                  = VERITAS File System
  License Type                  = PERMANENT

Features :=
  VXFDD                         = Enabled
  Quality of Storage Service    = Enabled
  VXCKPT                        = Enabled
  QLOG                          = Enabled
  File Change Log               = Enabled
  Cross-platform Data Sharing   = Enabled
  Extra-Big File Systems        = Enabled
  Multi-Volume Support          = Enabled


----------------**********----------------

  Product Name                  = VERITAS Database Edition for Oracle
  License Type                  = PERMANENT

Features :=
  DATABASE_EDITION              = Enabled
  DBED_ORA_TOOLS                = Enabled
  ODM                           = Enabled


----------------**********----------------

  Product Name                  = VERITAS SANPoint Control
  License Type                  = PERMANENT

Features :=
  SPC Lite                      = Enabled


----------------**********----------------

  License Key                   = XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-X
  Product Name                  = VERITAS Volume Manager
  Serial Number                 = 2851
  License Type                  = PERMANENT
  OEM ID                        = 2006
  Site License                  = YES
  Point Product                 = YES
```

```
Features :=

  Storage Expert                      = Enabled
  VxVM                                = Enabled
  FASTRESYNC                          = Enabled
  DGSJ                                = Enabled
  CPU Count                           = Not Restricted
  PGR                                 = Enabled
  VVS_CONFIG                          = Enabled
  Platform                            = un-used
  Version                             = 5.1
  Dynamic Lun Expansion               = Enabled
  Hardware assisted copy              = Enabled
  Cross-platform Data Sharing         = Enabled
  Maximum number of volumes           = Not Restricted


----------------**********----------

  License Key                         = XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-X
  Product Name                        = VERITAS Cluster Server
  Serial Number                       = 2851
  License Type                        = PERMANENT
  OEM ID                              = 2006
  Site License                        = YES
  Point Product                       = YES

Features :=
  Platform                            = Unused
  Version                             = 5.1
  Tier                                = Unused
  Reserved                            = 0

  Mode                                = VCS
  Global Cluster Option               = Enabled


----------------**********----------

  License Key                         = XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-X
  Product Name                        = VERITAS File System
  Serial Number                       = 2851
  License Type                        = PERMANENT
  OEM ID                              = 2006
  Site License                        = YES
  Point Product                       = YES

Features :=
  VXFS                                = Enabled
  QLOG                                = Enabled
  VXCKPT                              = Enabled

  CPU Count                           = Not Restricted
  Platform                            = un-used
  Version                             = 5.1
  File Change Log                     = Enabled
  Cross-platform Data Sharing         = Enabled
  Extra-Big File Systems              = Enabled
  Multi-Volume Support                = Enabled
  Quality of Storage Service          = Enabled
  Maximum number of file systems      = Not Restricted


----------------**********----------

  License Key                         = XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-X
  Product Name                        = VERITAS Volume Manager
  Serial Number                       = 5924
```

```
  License Type                    = PERMANENT
  OEM ID                          = 2006
  Site License                    = YES
  Editions Product                = YES

Features :=

  VVR                             = Enabled
  CPU Count                       = Not Restricted
  Platform                        = un-used
  Version                         = 5.1
  Maximum number of volumes       = Not Restricted
  VXKEYLESS                       = Enabled
```

NOTE

The preceding information uses that of Veritas license 5.1 as an example. The displayed information is different for Veritas license 5.0.

In the above information, **X** stands for the information about the license key.

The displayed information varies according to the OS.

----End

B.2.2 System Settings

This topic describes the FAQs about the system settings in the HA system.

B.2.2.1 How to Log in and Exit the VCS (Veritas Cluster Server)

Question

How do I log in to and exit the VCS?

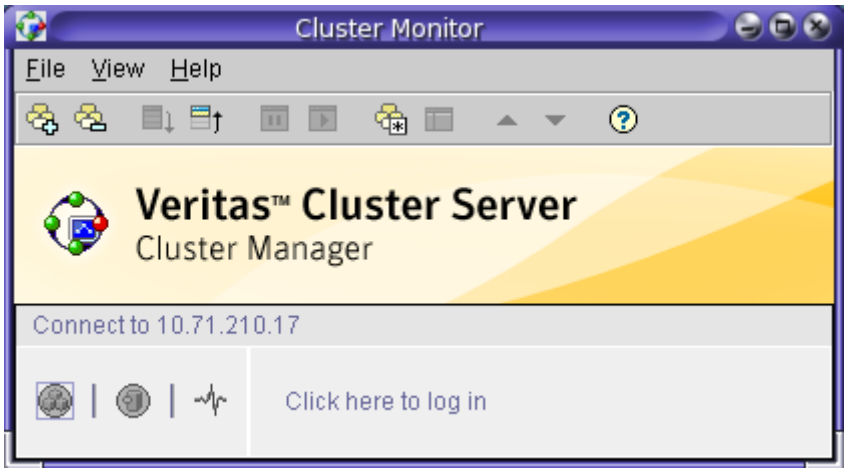
Answer

1 Log in to the VCS.

1. Open the Cluster monitor.

   a. Log in to the OS as user **root**.

b. Open a terminal window and run the following command:
```
# hagui&
```



NOTE

If the login window fails to be displayed and the terminal displays a message indicating that the current status is "STALE_ADMIN_WAIT", run the **# hasys -force *host name of node*** command.

2. Click **Connect to *Cluster name***.

NOTE

If you are logging in to the VCS for the first time, you need to create a new Cluster.

a. Click **File** > **New Cluster**.

b. Enter the IP address of application network.

c. Click **OK**.

3. Enter *User Name* and *Password*.

NOTE

The default user name of the VCS is **admin** and the password is **password**. For system security, modify the password and remember the new password.

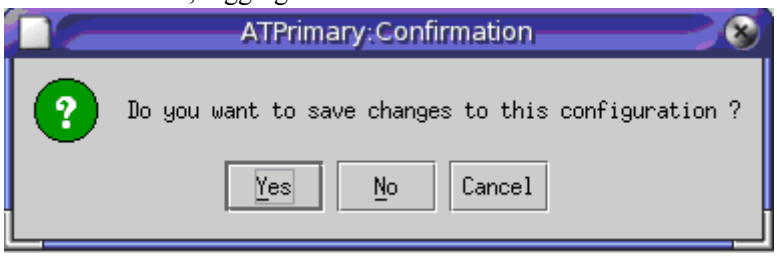
4. Click **OK**.

2 Exit the VCS:

1. Choose **File** > **Log Out** to exit the VCS.

CAUTION

If the configuration changes, click **Yes** in the **Confirmation** dialog box when exiting the VCS. Otherwise, logging in to the VCS fails after the server is restarted.



----End

B.2.2.2 How to Query the RVG Status

Question

How do I query the RVG status?

Answer

1. Log in to the primary site as user **root**.
2. Run the following command to view the RVG status of the active site:
   # **vxprint -Vl**

   The following message will be displayed:

```
Disk group: datadg

Rvg:       datarvg
info:      rid=0.1269 version=4 rvg_version=30 last_tag=3
state:     state=ACTIVE kernel=ENABLED
assoc:     datavols=lv_nms_data
           srl=srl_vol
           rlinks=datarlk
           exports=(none)
           vsets=(none)
att:       rlinks=datarlk
flags:     closed primary enabled attached
device:    minor=31004 bdev=315/31004 cdev=315/31004 path=/dev/vx/dsk/datadg/
datarvg
perms:     user=root group=root mode=0600
```

   Table B-2 describes the RVG status of the primary site.

Table B-2 RVG status of the primary site

Field	Description
Disk group	Indicates the disk group where the RVG is located.
Rvg	Indicates the name of the RVG.
info	Indicates the information about the RVG.
state	Indicates the status of the RVG. In normal cases, the situations are as follows: ● **state** is set to **ACTIVE**. ● **kernel** is set to **ENABLED**.
assoc	Indicates the association information about the RVG. ● **datavols** indicates the data disk volume that the RVG contains. ● **srl** indicates the SRLog disk volume that the RVG contains. ● **rlinks** indicates the RLink that the RVG contains.
att	Indicates the activated Rlink of the RVG.
flags	Indicates the flag of the RVG. In normal cases, the value is **closed primary enabled attached**.

Field	Description
device	Indicates the device information of the RVG, including the device ID and path.
perms	Indicates the right information about the RVG.

3 Log in to the secondary site as user **root**.

4 Run the following command to view the RVG status at the secondary site:

vxprint -Vl

The following message will be displayed:

```
Disk group: datadg

Rvg:      datarvg
info:     rid=0.1269 version=4 rvg_version=30 last_tag=3
state:    state=ACTIVE kernel=ENABLED
assoc:    datavols=lv_nms_data
          srl=srl_vol
          rlinks=datarlk
          exports=(none)
          vsets=(none)
att:      rlinks=datarlk
flags:    closed secondary enabled attached
device:   minor=31004 bdev=315/31004 cdev=315/31004 path=/dev/vx/dsk/datadg/
datarvg
perms:    user=root group=root mode=0600
```

For the description of the RVG status on the secondary site, see **Table B-2**. Normally, **flags** on the secondary site is **closed secondary enabled attached**.

----End

B.2.2.3 How to Query the Rlink Status

Question

How do I query the Rlink status?

Answer

1 Log in to the primary site as user **root**.

2 Run the following command to query the RLink status:

vxprint -Pl <rlinkName>

For example, run the following command to query the status of **datarlk**:

vxprint -Pl datarlk

A message similar to the following will be displayed:

```
Disk group: datadg

Rlink:    datarlk
info:     timeout=500 rid=0.1414
          latency_high_mark=10000 latency_low_mark=9950
```

```
          bandwidth_limit=none checksum=on
state:    state=ACTIVE
          synchronous=off latencyprot=off srlprot=autodcm
assoc:    rvg=datarvg
          remote_host=192.168.1.11 IP_addr=192.168.1.11 port=4145
          remote_dg=datadg
          remote_dg_dgid=1160936796.6.T522022456
          remote_rvg_version=30
          remote_rlink=datarlk
          remote_rlink_rid=0.1405
          local_host=192.168.1.10 IP_addr=192.168.1.10 port=4145
protocol: UDP/IP
flags:    write enabled attached consistent connected asynchronous
```

Table B-3 describes the Rlink status on the primary site.

Table B-3 Rlink status on the primary site

Field	Description	
Disk group	Indicates the disk group where the Rlink is located.	
Rlink	Indicates the name of the Rlink.	
info	Indicates the information about the Rlink. ● **timeout** indicates the timeout period. ● **rid** indicates the ID of the Rlink. ● **latency_high_mark** indicates the highest delay flag. ● **latency_low_mark** indicates the lowest delay flag. ● **bandwidth_limit** indicates the bandwidth limit.	
state	Indicates the status of the Rlink. In normal cases, the situations are as follows: ● **state** is set to **ACTIVE**. ● **synchronous** is set to **off**. ● **latencyprot** is set to **off**. ● **srlprot** is set to **autodcm**.	
assoc	rvg	Indicates the RVG where the Rlink is located.
	remote_host	Indicates the name of the remote host.
	IP_addr	Indicates the IP address of the remote host.
	remote_dg	Indicates the remote disk group.
	port	Indicates the port number of the remote host.
	remote_dg_dgid	Indicates the ID of the remote disk group.
	remote_rvg_version	Indicates the RVG version of the remote host.
	remote_rlink	Indicates the Rlink name of the remote host.
	remote_rlink_rid	Indicates the Rlink ID of the remote host.
	local host	Indicates the name of the local host.
protocol	Indicates the protocol for synchronizing data.	

flags	Indicates the flag of the Rlink. Normally, the value is **write enabled attached consistent connected asynchronous**.

3 Log in to the secondary site as user **root**.

4 Run the following command to query the Rlink status:
vxprint -Pl <rlinkName>

For example, run the following command to query the **datarlk** status:

vxprint -Pl datarlk

A message similar to the following will be displayed:

```
Disk group: datadg

Rlink:    datarlk
info:     timeout=500 rid=0.1405
          latency_high_mark=10000 latency_low_mark=9950
          bandwidth_limit=none checksum=on
state:    state=ACTIVE
          synchronous=off latencyprot=off srlprot=autodcm
assoc:    rvg=datarvg
          remote_host=192.168.1.10 IP_addr=192.168.1.10 port=4145
          remote_dg=datadg
          remote_dg_dgid=1160936853.6.T522022448
          remote_rvg_version=30
          remote_rlink=datarlk
          remote_rlink_rid=0.1414
          local_host=192.168.1.11 IP_addr=192.168.1.11 port=4145
protocol: UDP/IP
flags:    write enabled attached consistent connected
```

For the description of the Rlink status on the secondary site, see **Table B-3**.

----End

B.2.2.4 How to Query the VVR Status

Question

How do I query the VVR status during the maintenance of the Veritas HA system?

Answer

1 Run the following command to view the rvg name of the replication system:

vradmin printrvg

A message similar to the following will be displayed:

```
Replicated Data Set: datarvg
Primary:
        HostName: 10.71.224.48
        RvgName: datarvg
        DgName: datadg
Secondary:
        HostName: 10.71.224.50
        RvgName: datarvg
        DgName: datadg
```

In the preceding message, the rvg name (RvgName) is **datarvg**.

2 Run the following command to view the Rlink name of the replication system. The parameter **datarvg** is obtained in Step 1.

vxprint -l datarvg

A message similar to the following will be displayed:

```
Disk group: datadg

Rvg:      datarvg
info:     rid=0.1451 version=5 rvg_version=30 last_tag=4
state:    state=ACTIVE kernel=ENABLED
assoc:    datavols=lv_nms_data
          srl=srl_vol
          rlinks=datarlk
          exports=(none)
          vsets=(none)
att:      rlinks=datarlk
flags:    closed primary enabled attached
device:   minor=129007 bdev=309/129007 cdev=309/129007 path=/dev/vx/dsk/datadg/
datarvg
perms:    user=root group=root mode=0600
```

In the preceding message, the Rlink name (Rlink) is **datarlk**.

3 Run the following commands to view other status information of the replication system. The parameters **datarvg** and **datarlk** are obtained in Step 1 and Step 2.

- Run the # **vxdisk list** command to query the disk status.
- Run the # **vxdg list** command to query the status of the disk group.
- Run the # **vxprint -ht** command to query the information about the disk volume.
- Run the # **vxprint -l datarvg** command to query the RVG status.
- Run the # **vxprint -l datarlk** command to query the Rlink status.
- Run the # **vxrlink -g datadg status datarlk** command at the primary site to query the replication cache status.

Save the response to the preceding commands.

----End

B.2.2.5 How to Manually Start the VCS Service

Question

How do I manually start the VCS service?

Answer

1 Log in to the OS as user **root**.

2 Run the following command to start the VCS processes:

```
# hastart -onenode
```

----End

B.2.2.6 How to Manually Start the VVR

Question

How do I manually start the VVR?

Answer

1. Log in to the OS as user **root**.
2. Run the following commands to start the VVR:

   # **cd /etc/init.d**

   # **./vras-vradmind.sh start**

   ----End

B.2.2.7 How to Manually Stop the VCS Service

Question

How do I manually stop the VCS service?

Answer

1. Log in to the OS as user **root**.
2. Run the following command to stop the VCS service:

   ```
   # hastop -all -force
   ```

   ----End

B.2.2.8 How to Start/Stop the NMS Before Synchronizing the Primary and Secondary Sites

Question

How to start/stop the NMS before synchronizing the primary and secondary sites of a high availability system?

Answer

1. Log in to the OS as user **root**.
2. Open a CLI.
3. Run the following command to start the VCS client:

   ```
   # hagui&
   ```

4. Choose **File** > **New Cluster**. Then, enter the server IP address and click **OK**.
5. Enter the default user name **admin** and the default password **password** of the VCS client. Then, click **OK**.

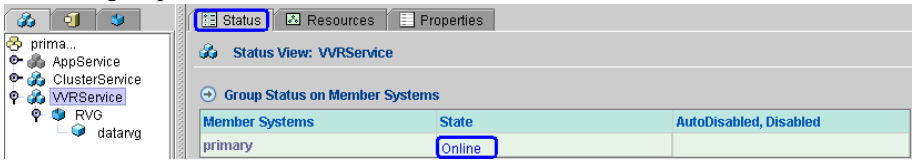
6 Ensure that the datarvg resource in the VVRService resource group has been enabled.

Right-click the datarvg resource and check whether the **Enabled** option is selected. If this option is checked, it has been enabled.

If this option is unchecked, check it.

7 Ensure that the VVRService resource group has been started.

Select the VVRService resource group, click the **Status** tab, and check whether the value in the **State** column is **Online**. If **Online** is displayed as shown in the following figure, the VVRService resource group has been started.



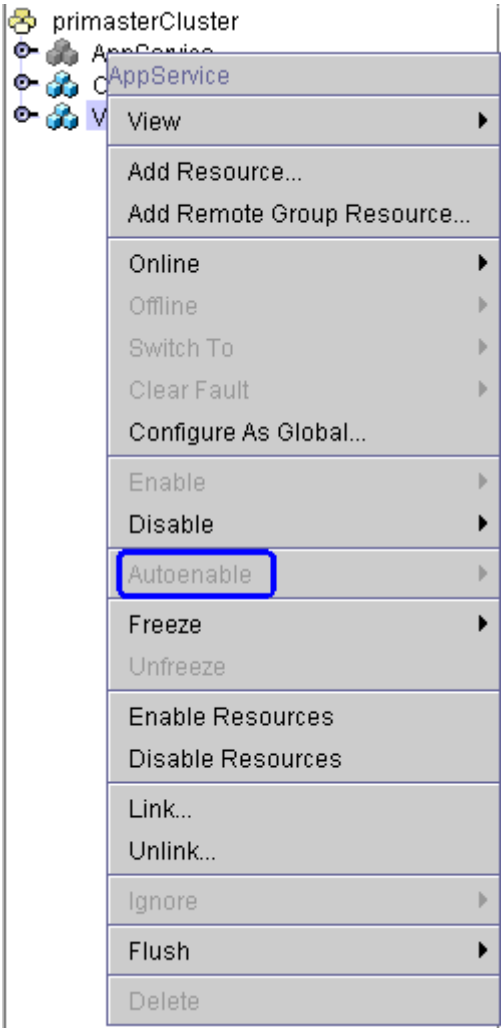
If the VVRService resource group has not been started, do as follows to start it:

1. Right-click the VVRService resource group and choose **Online** > **host name** from the shortcut menu.
2. In the dialog box that is displayed, click **Yes** to make the resource group online.

8 Ensure that all resources in the AppService resource group have been enabled.

Right-click a resource in the AppService resource group and check whether the **Enabled** option is selected. If this option is selected, it indicates that the resource has been enabled. If this option is not selected, you must select it. Repeat this operation on every resource in the AppService resource group.

9 **Optional:** Ensure that **Autoenable** of the AppService resource group has been grayed out, as shown in the following figure.



- If **Autoenable** has been grayed out, no action is required.
- If **Autoenable** has not been grayed out, click **Autoenable** to gray it out.

10 Click  to save the settings.

11 Start the AppService resource group.

1. Right-click the AppService resource group and choose **Online** > **host name** from the shortcut menu.
2. In the dialog box that is displayed, click **Yes** to start the AppService resource group.

12 Stop the AppService resource group.

1. Right-click the AppService resource group and choose **Offline** > **host name** from the shortcut menu.

2. In the dialog box that is displayed, click **Yes** to stop the AppService resource group.

----End

B.2.2.9 How to Ensure Proper Connection of VVR Ports on Primary and Secondary Sites

Question

How to ensure proper connection of VVR ports on primary and secondary sites?

Answer

1 Log in to the OSs of the primary and secondary sites of as the **root** user.

2 On the primary site, connect to the IP address of the secondary site by means of Telnet to check that the VVR port used by the secondary site can be properly connected; on the secondary site, connect to the IP address of the primary site by means of Telnet to check that the VVR port used by the primary site can be properly connected. Run the following command:

NOTE

Ports to be checked are port 4145, port 8199, and port 8989.

```
# telnet IP address of the peer site port number
```

For example, assume that the IP address of the peer site is 10.10.10.10 and the port number is 4145.

```
# telnet 10.10.10.10 4145
```

Information similar to the following is displayed:

```
Trying 10.10.10.10... Connected to 10.10.10.10 Escape character is '^]'.
```

Connected to 10.10.10.10 indicates that port 4145 for 10.10.10.10 can be connected.

Press **Ctrl+]** to return to the Telnet prompt, and enter **quit** to exit Telnet.

```
telnet> quit
```

Information similar to the following is displayed:

```
Connection to 10.10.10.10 closed.
```

Perform the same operations to check the other two ports. The three ports used by the VVR must be connectable.

Ensure that UDP is enabled on the firewall for port 32768 to port 65535.

----End

B.2.2.10 How to Ensure Proper File Transfer Between Primary and Secondary Sites

Question

How to ensure proper file transfer between primary and secondary sites?

Answer

1 Log in to the OSs of the primary and secondary sites of as the **root** user.

2 On the primary site, connect to the IP address of the secondary site by means of FTP to check that the secondary site can properly receive files; on the secondary site, connect to the IP address of the primary site by means of FTP to check that the primary site can properly receive files.

NOTE

- Transferring the **/tmp/test** file from the primary site to the secondary site with the IP address of 10.10.10.10 is used as an example.
- Perform the same operations on the secondary site to check file transfer from the secondary site to the primary site.

1. In the **tmp** path, create a temporary file named **test** with the size of 10 MB.
   ```
   # mkfile 10m /tmp/test
   ```
2. Connect to the IP address of the secondary site by means of FTP.
   ```
   # ftp 10.10.10.10
   ```
   Information similar to the following is displayed:
   ```
   Connected to 10.10.10.10 220 T5220210198 FTP server ready. Name
   (10.10.10.10:root): root 331 Password required for root. Password:
   ```
3. Enter the root user password for the secondary site.

   Information similar to the following is displayed:
   ```
   ftp>
   ```
4. To transfer the **/tmp/test** file to the primary site, run the following command:
   ```
   ftp> put /tmp/test
   ```
   Information similar to the following is displayed:
   ```
   226 Transfer complete.
   ```
   The file is successfully transferred. To exit FTP, enter **bye**.

----End

B.3 Sybase Database

This topic covers FAQs about the Sybase database.

B.3.1 Startup and Shutdown of the Sybase Database

This topic describes the FAQs about the startup and shutdown of the Sybase database.

B.3.1.1 How to Disable the Sybase Database Service

Question

How do I disable the Sybase database service?

Answer

1 Perform the following operations to disable the Sybase database service at the primary site in the HA system:

1. Log in to the primary site as user **root**.
2. Run the following command to start the VCS client at the primary site:

   # **hagui &**
3. In the **Cluster Monitor** window, click the server record in the list.
4. In the dialog box that is displayed, enter the user name and the password of the VCS, and click **OK**.

   NOTE

   The default user of the VCS is **admin** and the default password is **password**.
5. On the VCS client of the primary site, right-click the database node and choose **Offline** > **PrimaryCluster** from the shortcut menu.
6. In the confirmation dialog box, click **Yes**.
7. Run the following command to check whether the Sybase database service is disabled:

   # **ps -ef | grep sybase**

   If the following message is displayed, the Sybase database service has been disabled:

   ```
   root  9629 14603   0 07:46:52 pts/3       0:00 grep sybase
   ```

   NOTE

   By default, the Sybase database service at the secondary site is not running.

----End

B.3.1.2 How to Start the Sybase Database Service

Question

How do I start the Sybase database service?

Answer

1 Perform the following operations to start the Sybase database service in the HA system:

1. Run the following command to start the VCS client:

   ```
   # hagui &
   ```
2. Choose **File** > **New Cluster** from the main menu. In the window that is displayed, enter the IP address of the server and click **OK**.
3. Enter the default user name **admin** and the default password **password** of the VCS client. Click **OK**.
4. Expand the **AppService** node in the navigation tree, and expand the **SybaseBk** node. Right-click **BackupServer** and choose **Online** > ***host_name*** from the shortcut menu.
5. In the dialog box that is displayed, click **Yes**.

   Wait until **BackupServer** and **DatabaseServer** on the **Resources** tab page are available, which indicates that the Sybase database service is running.

----End

B.3.1.3 How to Verify That the Sybase Process Is Running

Question

How do I verify that the Sybase process is running?

Answer

1 Perform the following operations to start the Sybase database service in the HA system:

1. Run the following command to start the VCS client:

   ```
   # hagui &
   ```

2. Choose **File** > **New Cluster** from the main menu. In the window that is displayed, enter the IP address of the server and click **OK**.
3. Enter the default user name **admin** and the default password **password** of the VCS client. Click **OK**.
4. Expand the **AppService** node in the navigation tree, and expand the **SybaseBk** node. Right-click **BackupServer** and choose **Online** > ***host_name*** from the shortcut menu.
5. In the dialog box that is displayed, click **Yes**.

   Wait until **BackupServer** and **DatabaseServer** on the **Resources** tab page are available, which indicates that the Sybase database service is running.

----End

B.3.2 Sybase Database Maintenance

This topic describes the FAQs about the Sybase database maintenance.

B.3.2.1 How to Verify That the Sybase Database Has Been Installed

Question

How do I verify that the Sybase database has been installed?

Answer

NOTE

- The Sybase database will be automatically installed when the U2000 is installed if the Sybase database does not exist on the system.
- If the Sybase database exists on the system, a dialog box will be displayed asking you whether or not you want to reuse the Sybase database. There is no need to reinstall the Sybase database if it is reused (saves time, but not recommended).

- Consult with the computer administrator to see if the Sybase database has been installed.
- Verify that the installation directory and file of the Sybase database exist. A sample directory is **/opt/sybase**.
- Verify that the version of the Sybase database is correct. For details, see **B.3.2.2 How to Check the Sybase Database Version**.
- Verify that the Sybase database is running. For details, see **B.3.1.3 How to Verify That the Sybase Process Is Running**. For details about how to start the Sybase database, see **B.3.1.2 How to Start the Sybase Database Service**.

----End

B.3.2.2 How to Check the Sybase Database Version

Question

How do I perform the required check on the Sybase database version to see if it is correct after the Sybase database is installed?

Answer

1 Switch to user **sybase**, and connect to the Sybase database. Run the following commands:

su - sybase

$ **cd /opt/sybase/OCS*/bin**

$ **./isql -SDBSVR -Usa -Pchangeme**

NOTE

In the **./isql -SDBSVR -Usa -Pchangeme** command, *changeme* is the password of user **sa** of the Sybase database.

2 Run the following commands to check the Sybase database version:

1> **use master**

2> **go**

1> **select @@version**

2> **go**

NOTE

There must be a space between **select** and **@** in the **select @@version** command.

A message similar to the following will be displayed:

```
-----------------------

 Adaptive Server Enterprise/15.0.3/EBF 16548 ESD#1/P/Sun_svr4/OS 5.8/ase1503/268
        0/64-bit/FBO/Thu Mar  5 09:39:28 2009
(1 row affected)
```

The preceding message indicates that Sybase database version is SYBASE 15.0.3.

----End

B.3.2.3 How to View the Server Name of the Sybase Database

Question

How do I view the server name of the Sybase database?

Answer

1. Log in to the OS as user **sybase**.
2. Run the following command to view the server name of the Sybase database:

   $ **more /opt/sybase/interfaces**

   A message similar to the following will be displayed:

```
DBSVR
        master tcp ether 10.71.225.89 4100
        query tcp ether 10.71.225.89 4100
        master tcp ether 10.71.225.89 4100
        query tcp ether 10.71.225.89 4100
        master tcp ether 127.0.0.1 4100
        query tcp ether 127.0.0.1 4100

DBSVR_back
        master tcp ether 10.71.225.89 4200
        query tcp ether 10.71.225.89 4200
        master tcp ether 10.71.225.89 4200
        query tcp ether 10.71.225.89 4200
        master tcp ether 127.0.0.1 4200
        query tcp ether 127.0.0.1 4200
```

   NOTE

   Run the following commands to change the server name of the Sybase database to **DBSVR**:

   $ **cd /opt/HWENGR/upgrade/scripts/solaris**

   $ **./_modifyInterfaces.sh old_main_DBServer_name DBSVR**

   $ **./_modifyCfgFile.sh old_main_DBServer_name DBSVR**

   $ **./_modifyLogFile.sh old_main_DBServer_name DBSVR**

   $ **./_modifyRunFile.sh old_main_DBServer_name DBSVR**

   In the preceding commands, **old_main_DBServer_name** indicates the name of the server to be reused.

----End

B.3.2.4 How to Change the Password of User sa for the Sybase Database

Question

How do I change the password of user **sa** for the Sybase database?

Answer

1. Shut down the NMS server and client.

   Log in to the primary site and run the following command to start the VCS client:

   # **hagui &**

   In the **Cluster Monitor** window, click a server record in the information list.

   In the login dialog box that is displayed, enter the user name and password of the VCS. Click **OK** to log in to the VCS client. The default user name and password of the VCS are **admin** and **password**.

   Right-click **NMSServer** and choose **Offline** > ***Host name*** from the shortcut menu.

   In the confirmation dialog box, click **Yes**.

   NOTE

   Ensure that the database is running.

2. Log in to the network management maintenance suite (MSuite) client.
   1. On the computer where the MSuite client is installed, double-click the **U2000 MSuite** shortcut icon on the desktop. Wait about one minute. The **Login** dialog box is displayed.
   2. Set the login parameters and click **OK**. The **NMS maintenance suite** window will be displayed.
      - IP Address: Indicates the system IP address of the computer where the MSuite server is installed.
      - Port No.: The default port ID is **12212**. There is no need to change the default value during login.
      - User Name and Password: The default user name and password are **admin**.
3. On the MSuite client, choose **Deploy** > **Change Database Administrator Password**. The **Change Database Administrator Password** dialog box is displayed.
4. Enter the old password and new password.

   NOTE

   A password must be 6-30 characters long and consists of letters or digits. Special characters are not allowed.
5. Click **OK**. The password is changed.

   ----End

B.3.2.5 How to View the Bit Number of the Sybase Database

Question

How do I view the bit number of the Sybase database?

Answer

1 Run the following commands to view the bit number of the Sybase database:

cd /opt/sybase/OCS*/bin

./isql -SDBSVR -Usa -Pchangeme

1>**select @@version**

2>**go**

NOTE

- In the **./isql -SDBSVR -Usa -Pchangeme** command, *changeme* is the password of user **sa** of the Sybase database.
- There must be a space between **select** and **@** in the **select @@version** command.

The following message will be displayed:

```
Adaptive Server Enterprise/12.5.3/EBF 13325 ESD#5/P/Sun_svr4/OS 5.8/ase1253/193
9/64-bit/FBO/Tue Dec 6 09:13:20 2005
```

`64-bit` indicates the bit number of the Sybase database.

----End

B.3.2.6 How to View the Details of the Sybase Database

Question

How do I view the details about the Sybase database during routine maintenance?

Answer

1 Run the following commands to view the details of all databases:

cd /opt/sybase/OCS*/bin

./isql -SDBSVR -Usa -Pchangeme

1>**sp_helpdb**

2>**go**

NOTE

In the **./isql -SDBSVR -Usa -Pchangeme** command, *changeme* is the password of user **sa** of the Sybase database.

The information about the Sybase database will be displayed, including the name, size, owner, and status.

2 Run the following commands to view the details of a specific database:

1>**sp_helpdb database_name**

2>**go**

NOTE

In the **sp_helpdb database_name** command, *database_name* is the name of the Sybase database.

Database space used can also be viewed.

----End

B.3.2.7 How to Change the Server Name of the Sybase Database to DBSVR

Question

If the OS is configured and the NMS installation needs to reuse the installed database, the database server name needs to be changed to **DBSVR**. How do I change the server name?

Answer

1. Log in to the OS as user **root**.
2. Run the following commands to view the server name of the Sybase database:

```
# more /opt/sybase/interfaces
```

Information similar to the following is displayed:

```
DBSVR
        master tcp ether 10.71.225.89 4100
        query tcp ether 10.71.225.89 4100
        master tcp ether 10.71.225.89 4100
        query tcp ether 10.71.225.89 4100
        master tcp ether 127.0.0.1 4100
        query tcp ether 127.0.0.1 4100

DBSVR_back
        master tcp ether 10.71.225.89 4200
        query tcp ether 10.71.225.89 4200
        master tcp ether 10.71.225.89 4200
        query tcp ether 10.71.225.89 4200
        master tcp ether 127.0.0.1 4200
        query tcp ether 127.0.0.1 4200
```

3. Run the following commands to change the database server name to **DBSVR** if the name is not **DBSVR**:

```
# . /opt/sybase/SYBASE.sh
# cd /opt/HWENGR/upgrade/scripts/solaris
# ./_modifyInterfaces.sh old_main_DBServer_name DBSVR
# ./_modifyCfgFile.sh old_main_DBServer_name DBSVR
# ./_modifyLogFile.sh old_main_DBServer_name DBSVR
# ./_modifyRunFile.sh old_main_DBServer_name DBSVR
```

In the preceding command, *old_main_DBServer_name* indicates the name of the server to be reused.

----End

B.3.2.8 How to Delete Redundant Database Items

Question

If the NMS installation needs to reuse the installed database, redundant database items need to be deleted. How do I delete redundant database items?

Answer

1 Log in to the OS as user **root**.

2 Run the following commands to view databases:

```
# su - sybase
$ . /opt/sybase/SYBASE.sh
$ cd /opt/sybase/OCS*/bin
$ ./isql -SDBSVR -Usa -Pchangeme
```

NOTE

In the **./isql -SDBSVR -Usa -Pchangeme** command, *changeme* is the password of user **sa** of the Sybase database.

```
1> sp_helpdb
2> go
```

Information similar to the following is displayed:

```
 name                 db_size       owner                  dbid
        created

status

 -------------------- ------------ ---------------------- ------
...
 XFTPDB                        150.0 MB sa                        12
        Mar 06, 2009
        select into/bulkcopy/pllsort, trunc log on
chkpt
 master                        240.0 MB sa                         1
        Mar 05, 2009
        mixed log and
data
 model                           2.0 MB sa                         3
        Mar 05, 2009
        select into/bulkcopy/pllsort, trunc log on chkpt, mixed log and
data
 sybsystemdb                     2.0 MB sa                     31513
        Mar 05, 2009
        mixed log and
data
 sybsystemprocs                250.0 MB sa                     31514
        Mar 05, 2009
        trunc log on chkpt, mixed log and
data
 tempdb                       1003.0 MB sa                         2
        Mar 29, 2009
        select into/bulkcopy/pllsort, trunc log on chkpt, mixed log and
data

(1 row affected)
(return status = 0)
1>
```

Look over the displayed message and delete any redundant databases other than **master**, **model**, **sybsystemdb**, **sybsystemprocs**, **tempdb** exist.

NOTE

- If the NMS of Chinese edition is installed, illegible characters may be displayed when you log in to the system using the remote terminal login tool (CLI-based). If this happens, set the encoding scheme of the remote terminal login tool to **UTF-8**.
- If the remote terminal login tool does not support the ability to set the encoding scheme, log in to the system by using the GUI.

3 Perform the following operations to delete the information about the redundant databases: (The following uses the **XFTPDB** as an example.)

1. Run the following commands to view the device information in the **XFTPDB** database:

```
1> sp_helpdb XFTPDB
2> go
```

Information similar to the following is displayed:

```
 name                 db_size       owner                  dbid
        created

status

 ---------------------- ------------ ---------------------- ------
...
 XFTPDB                        150.0 MB sa                          12
        Mar 06, 2009
        select into/bulkcopy/pllsort, trunc log on
chkpt

(1 row affected)
 device_fragments              size          usage
        created             free kbytes
 ----------------------------- ------------- --------------------
        ------------------- ----------------
 XFTPDBdata                           100.0 MB data only
        Mar  6 2009  4:13PM           100742
 XFTPDBlog                             50.0 MB log only
        Mar  6 2009  4:13PM not applicable

 ------------------------------------------------------------
 log only free kbytes = 50998
(return status = 0)
1>
```

2. Run the following commands to delete the **XFTPDB** database and the **XFTPDBdata** and **XFTPDBlog** items in the **XFTPDB** database:

```
1> drop database XFTPDB
2> go
1> sp_dropdevice XFTPDBdata
2> go
1> sp_dropdevice XFTPDBlog
2> go
```

3. Run the following commands to exit the SQL and log out as user **sybase**:

```
1> exit
$ exit
```

4. Run the following commands to go to the **sybase** directory and delete the associated files of the device information from the **XFTPDB** database:

```
# cd /opt/sybase/data
# rm XFTPDBdata.dat
# rm XFTPDBlog.dat
```

----End

B.3.2.9 How to Change the Character Set of the Database to UTF-8

Question

If the OS is configured and the NMS installation needs to reuse the installed database, the character set of the database needs to be changed to **UTF-8**. How do I change the character set?

Answer

1 Log in to the OS as user **root**.

2 Run the following commands to view the character set of the database:

```
# su - sybase
$ . /opt/sybase/SYBASE.sh
$ cd /opt/sybase/OCS*/bin
$ ./isql -SDBSVR -Usa -Pchangeme
```

NOTE

In the **./isql -SDBSVR -Usa -Pchangeme** command, *changeme* is the password of user **sa** of the Sybase database.

```
1> sp_helpsort
2> go
```

Information similar to the following is displayed:

```
...
     Unicode 3.1 UTF-8 Character Set
     Binary sort order for the ISO 10646-1, UTF-8 multibyte encoding character set
(utf8).
(return status = 0)
1>
```

3 Run the following commands to exit the SQL and log out as user **sybase**:

```
1> exit
$ exit
```

4 Run the following commands to change the character set to **UTF-8** if it is not **UTF-8**:

```
# cd /opt/HWENGR/engineering/script/sybase
# ./transferCharset.sh database_installation_path DBSVR sa password_of_sa
```

----End

B.4 U2000 System

This topic covers FAQs about the U2000 system.

B.4.1 How to Verify That the U2000 Is Installed

Question

How do I verify that the U2000 is installed?

Answer

1. Log in to the OS as user **nmsuser**.
2. Check whether the icons of the U2000 client and U2000 System Monitor exist on the desktop. If they exist, it indicates that the U2000 has been installed.
3. If login to the desktop fails, run the following commands to view the **/opt/U2000** directory: If this directory exists and is not empty, it indicates that the U2000 is installed.

   $ **cd /opt/U2000**

   $ **ls**

B.4.2 How to Check Whether the U2000 Processes of the High Availability System (Solaris) Are Started

Question

How to check whether the U2000 processes of the high availability system (Solaris) are started?

Answer

1 Log in to the OS of the active site as the **nmsuser** user.

2 Check the U2000 processes.

Run the following command to check whether the U2000 is running:

```
$ daem_ps
```

Information similar to the following is displayed:

```
nmsuser 27069     1   0 10:31:39 ?           1:39 imapmrb
nmsuser 27079     1   0 10:31:39 ?           0:00 imapwatchdog -cmd start
nmsuser 27075     1   0 10:31:39 ?           0:50 imapsysd -cmd start
nmsuser 27086     1   0 10:31:39 ?           0:09 imapeventmgr
nmsuser 23679     1   1 17:57:06 pts/8       0:02 imap_sysmonitor -cmd start
nmsuser 27116     1   0 10:31:40 ?           0:52 ResourceMonitor -cmd start
```

NOTE

The U2000 is running if the displayed information contains **imap_sysmonitor -cmd start**.

----End

B.4.3 How to Start the U2000 Processes of the High Availability System (Solaris)

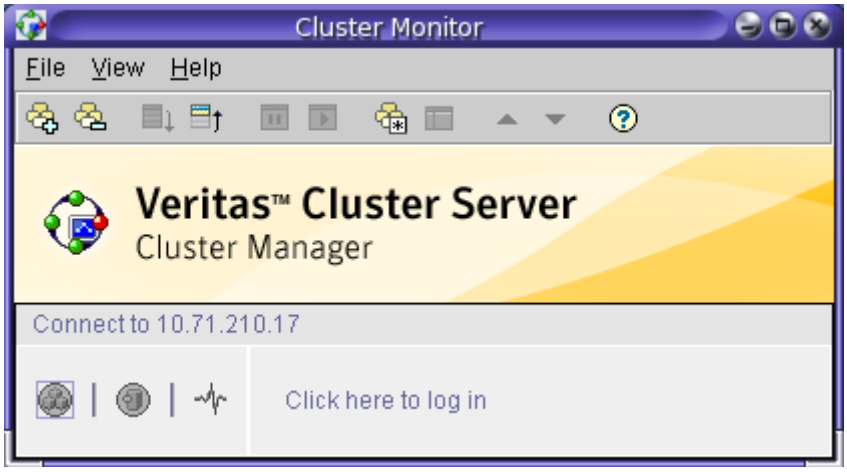
Question

How do I start the U2000 processes of the high availability system (Solaris)?

Answer

1. Log in to the OS of the primary site as user **root**.
2. Log in to the VCS.
   1. Open a terminal window, run the following command:

      ```
      # hagui&
      ```

      NOTE

      If the login window fails to be displayed and the terminal displays a message indicating that the current status is "STALE_ADMIN_WAIT", run the **# hasys -force *host name of node*** command.

   2. Click **Connect to *Cluster name***.

      NOTE

      If you are logging in to the VCS for the first time, you need to create a new Cluster.

      a. Click **File** > **New Cluster**.

      b. Enter the IP address of application network.

      c. Click **OK**.

   3. Enter *User Name* and *Password*.

      NOTE

      The default user name of the VCS is **admin** and the password is **password**. For system security, modify the password and remember the new password.

3. In the **Cluster Explorer** window, right-click the **AppService** resource group in the navigation tree and choose **Online** > **primary** from the shortcut menu to start the Sybase process and U2000 server process.

   TIP

   Click the **Resources** tab to view the start status of each resource.

   Normally, on the **Status** tab page, **Online** is displayed for **State** in the **Group Status on Member Systems** area on the active site, and **Online on primary** is displayed for **Status** in the **Resource Status** area.

NOTE

- In actual configuration, use the actual host name.
- If a fault has occurred during start of the AppService process, right-click **AppService** and choose **clear fault** from the shortcut menu to clear the fault. Then, choose **Online** > ***host_name*** to start the AppService process.

4 In the dialog box that is displayed, click **Yes**.

----End

B.4.4 How to End the U2000 Processes of the High Availability System (Solaris)

Question

How do I end the U2000 processes of the high availability system (Solaris)?

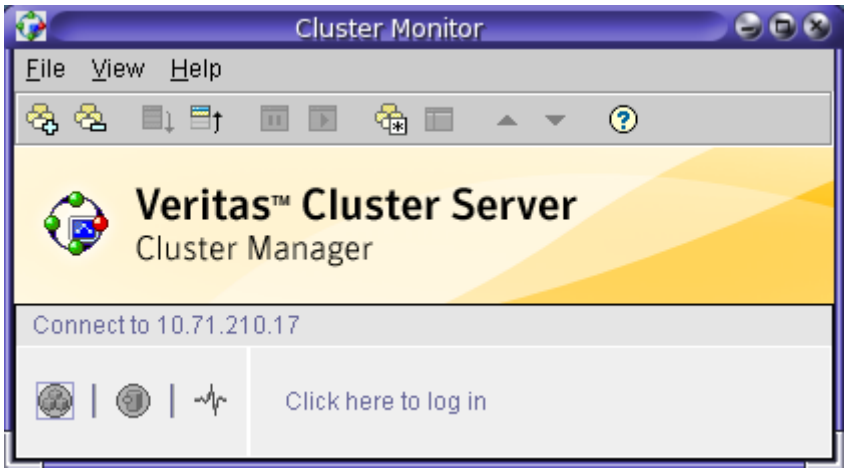
Answer

1 Log in to the OS of the active site as the **root** user.

2 Log in to the VCS.

1. Open a terminal window, run the following command:

```
# hagui&
```



NOTE

If the login window fails to be displayed and the terminal displays a message indicating that the current status is "STALE_ADMIN_WAIT", run the **# hasys -force *host name of node*** command.

2. Click **Connect to *Cluster name***.

NOTE

If you are logging in to the VCS for the first time, you need to create a new Cluster.

a. Click **File** > **New Cluster**.

b. Enter the IP address of application network.

c. Click **OK**.

3. Enter *User Name* and *Password*.

NOTE

The default user name of the VCS is **admin** and the password is **password**. For system security, modify the password and remember the new password.

3 Select the **AppService** resource group from the navigation tree, right-click, and choose **Offline** > **Host name** from the shortcut menu.

Wait about three minutes. If **Group Status on Member Systems** is displayed as **Offline**, it indicates that the U2000 processes are ended.

----End

B.4.5 How to Determine Which Types of Software Are Preinstalled

Question

Servers come preinstalled with software from Huawei. The U2000 servers come preinstalled to different extents according to the scheme and software purchased. How do I determine which types of software are preinstalled?

Answer

The U2000 is installed based on the BOM.

- If the U2000 license BOM is available, the U2000 HA system needs to be installed according to the license BOM while the primary site and secondary site are separated as much as possible. Technical support engineers need to change the IP address, check that the network between the primary site and secondary site is functioning properly, and then connect the two sites.
- If the U2000 license BOM is unavailable, only the OS needs to be installed.

B.4.6 Which Installation Packages Are Required for U2000 Installation

Question

Which installation packages are required for U2000 installation?

Answer

Prepare installation packages according to the U2000 installation scheme.

Table B-4 Software required for installation

Software	Medium Description
Solaris 10 OS	You can install Solaris 10 OS by using the quick installation DVD or the common installation DVD. ● Quick installation DVD: U2000***version***_server_os_solaris_SPARC_sun4v_dvd2 or U2000***version***_server_os_solaris_SPARC_sun4u_dvd1 **NOTE** ● Ensure that the quick installation DVD U2000***version***_server_os_solaris_SPARC_sun4v_dvd2 is available if the hardware type of the selected server is sun4v (the T5220 server for example). ● Ensure that the quick installation DVD U2000***version***_server_os_solaris_SPARC_sun4u_dvd1 is available if the hardware of the selected server is sun4u (the M4000 server for example). Installation engineers can run the **uname -m** command to view the hardware type of a server after logging in to the server OS as user **root**. ● Common installation DVD: Solaris 10 Software (10/08 SPARC Platform Edition) **NOTE** Before installing Solaris 10 OS by using the common installation DVD, prepare the OS patch DVD: U2000***version***_server_patch_solaris_SPARC_dvd3, or OS patch package U2000***version***_server_ospatch_solaris_SPARC.tar.
Database	Installation DVD or installation package ● Installation DVD: U2000***version***_server_db_solaris_SPARC_dvd4 ● Installation package: U2000***version***_server_db_solaris_SPARC.tar
Veritas Software	Veritas software installation DVD or installation package ● Veritas software installation DVD: Storage Foundation and HA Solutions 5.1 for Solaris SPARC or VERITAS Storage Foundation and High Availability Solution, 5.0 Maintenance Pack 3 for Solaris ● Veritas software installation package: veritas5.1_solaris.tar.gz ● Veritas patch installation DVD: U2000***version***_server_patch_solaris_SPARC_dvd3 ● Veritas patch Installation package: U2000***version***_server_veritas5-1_patch_solaris_SPARC.tar

Software	Medium Description
U2000 server software	Installation DVD or installation package ● Installation DVD: U2000***version***_server_nms_solaris_SPARC_dvd5 ● Installation package: **NOTE** Prepare software packages required by the components to be installed. Do not prepare U2000***version***_client_solaris_SPARC.tar software packages. If the U2000***version***_client_solaris_SPARC.tar and the following software packages are decompressed into the same path, the U2000 installation will fail. – Basic component: U2000***version***_server_nmsbase_solaris_SPARC.tar **It must be available.** It is used to install the U2000. – Core component: U2000***version***_server_nmscore_solaris_SPARC.tar **It must be available.** It is used to install the U2000. – Transport domain component: U2000***version***_server_nmstrans_solaris_SPARC.tar **It is required only if the U2000 needs to manage Huawei transport equipment**. Huawei transport equipment includes: – MSTP equipment – WDM equipment – NA WDM equipment – Submarine equipment – RTN equipment – PTN equipment – IP domain component: U2000***version***_server_nmsip_solaris_SPARC.tar **It is required only if the U2000 needs to manage Huawei IP equipment**. Huawei IP equipment includes: – Routers – Switches – Metro service equipment – Broadband access equipment – VoIP gateways – Firewalls – Service inspection gateway – SVN equipment – Access domain component: U2000***version***_server_nmsaccess_solaris_SPARC.tar **It is required only if the U2000 needs to manage Huawei access equipment**. Huawei access equipment includes: – FTTx equipment

Software	Medium Description
	- MSAN equipment - DSLAM equipment - StorageTek 2540 disk array manager CAM (optional). Prepare this component if the StorageTek 2540 disk array is configured: U2000***version***_server_ospatch_solaris_SPARC.tar

B.4.7 How to Handle Messages Indicating That the Port Is Occupied During Installation or Uninstall

Question

How do I handle messages indicating that the port is occupied during use of the MSuite, installation, or uninstall?

In the Solaris OS, the message is as follows:

```
The communication port (12212,12213,12214,12215) of the installation framework is
used. Run the "/usr/bin/netstat -an -P tcp" command to query the usage status of
the port, or try later.
```

Answer

- Wait about one minute and try again after the port is released automatically.
- In the Solaris or SUSE Linux OS, run the following command to view process IDs:

  ```
  # ps -ef | grep java root 19913 19907   0 04:04:09 pts/1      0:00 grep java ...
  root 18382 18311   0 03:42:33 pts/2      12:20 /opt/HWNMSJRE/jre_sol/bin/java
  -server -Dequinox.conf=engineering/conf/installE ...
  ```

  Locate the process that contains the command output: **/opt/HWNMSJRE/jre_sol/bin/java -server** and end the process by running the **kill** command. The following is a sample **kill** command:

  ```
  # kill -9 18382
  ```

----End

B.4.8 How to Rectify the Application GUI Startup Failure Caused by User Switching

Question

After a user logs in to the graphical desktop system as user **root** and runs the **su - nmsuser** command to switch to user **nmsuser**, applications such as the NMS maintenance suite client, U2000 client, and U2000 System Monitor client fail to start. How do I rectify this fault?

Answer

1. Use either of the following methods to rectify the fault.
   - Method 1: Log out of the graphical desktop system and then log in as user **nmsuser**. Then, start an application in the desktop system.

- Method 2: Perform the following operations in the current window:
  1. Run the following command to switch back to user **root**:
     ```
     $ exit
     ```
     NOTE

     The command prompt for user **root** is **#**. If **#** is not displayed after you run the **exit** command, run the **exit** command again.
  2. Run the following command to check the **DISPLAY** variable of user **root**. Then, record the value of the **DISPLAY** variable.
     ```
     # echo $DISPLAY
     ```
  3. Run the following commands to switch to user **nmsuser** and set the **DISPLAY** variable.
     ```
     # xhost +
     # su - nmsuserr
     $ export DISPLAY=DISPLAY value
     ```
     NOTE

     In the preceding command, **DISPLAY value** is the recorded value of the **DISPLAY** variable.
  4. Run the appropriate command to start the application.

----End

B.4.9 How to View the U2000 and Sybase Database Installation Paths

Question

How do I view the U2000 and Sybase database installation paths?

Answer

Generally, the U2000 installation path is **/opt/U2000** and the Sybase database installation path is **/opt/sybase**.

To view the installation paths, perform the following steps:

1 Log in to the OS as user **root**.

2 Check the **ICMR_conf.xml** configuration file to confirm the installation paths.

Run the following commands to check the **ICMR_conf.xml** configuration file:

```
# cd /etc/ICMR
# more ICMR_conf.xml
```

A message similar to the following will be displayed:

```
<CONFIGITEMS>
<NETCONFIGFILE>/etc/ICMR/netCfg/OS/os_net_config.cfg</NETCONFIGFILE>
<DATABASEINSTALLPATH>/opt/sybase</DATABASEINSTALLPATH>
<IFCONFIGSYSNET>no</IFCONFIGSYSNET>
<NMSINSTALLPATH>/opt/U2000</NMSINSTALLPATH>
<FINISHTASKLIST>tasks::installtype_request,tasks::instSybase_request,tasks::instNM
S_request,tasks::single_network_request,tasks::modify_sys_paras,tasks::enable_mult
ipath,tasks::mirrorDisk,tasks::mount_array_disks</FINISHTASKLIST>
<INSTALLTYPE>1</INSTALLTYPE>
<DEBUGLEVEL>9</DEBUGLEVEL>
</CONFIGITEMS>
```

Confirm the installation paths according to the preceding message:

- The Sybase database installation path is **/opt/sybase** if **<DATABASEINSTALLPATH>/opt/sybase</DATABASEINSTALLPATH>** is displayed.
- The U2000 installation path is **/opt/U2000** if **<NMSINSTALLPATH>/opt/U2000</NMSINSTALLPATH>** is displayed.

----End

B.4.10 How to View Network Configurations for the Primary Site or Secondary Site Installed with a HA System

Question

How do I view network configurations for the primary site or secondary site installed with a high availability (HA) system?

Answer

NOTE

The following uses viewing configurations for the primary site as an example. Viewing configurations for the secondary site is similar to that for the primary site.

1. Log in to the OS of the primary site as user **root**.
2. View the **vcs_net_config.cfg** file. Saving this file to a local disk is recommended.

   Run the following commands to view the **vcs_net_config.cfg** file:

   ```
   # cd /etc/ICMR/netCfg/VCS/
   # more vcs_net_config.cfg
   ```

   A message similar to the following will be displayed:

   ```
   ...

   #The following are meanings of configuration item
   ClearFlag=yes
   SystemIP=10.78.218.52
   SystemHostname=primary
   SystemNetmask=255.255.255.0
   SystemNic=bge0
   SystemRouter=10.78.218.1

   ...
   HBCFG=no
   HBIP=10.78.218.52
   HBHostname=primary
   HBNetmask=255.255.255.0
   ...
   # To use another NIC to back up PHBNic, configure the following parameters.
   HBIsIPMP=no

   HBStandbyNic=
   HBStandbyIP=
   HBStandbyNetmask=255.255.255.0
   HBStandbyHostname=HBSlave

   #VVR network configure, support the IPMP
   VVRCFG=no

   VVRIP=
   VVRHostname=VVRService
   VVRNetmask=255.255.255.0
   ```

```
VVRMasterNic=
VVRMasterIP=
VVRMasterHostname=VVRMaster
VVRMasterNetmask=255.255.255.0

# To use another NIC to back up PHBNic, configure the following parameters.
VVRIsIPMP=

VVRStandbyNic=
VVRStandbyIP=
VVRStandbyHostname=VVRSlave
VVRStandbyNetmask=255.255.255.0

#APP network configure, support the IPMP
APPCfg=yes

APPIP=10.78.218.52
APPHostname=primary
APPNetmask=255.255.255.0
APPMasterNic=bge0

APPMasterIP=
APPMasterHostname=APPMaster
APPMasterNetmask=255.255.255.0
        # To use anther NIC to back up the HBNic, configure the following
parameters.
        APPIsIPMP=no
        APPStandbyNic=
        APPStandbyIP=
        APPStandbyNetmask=255.255.255.0
        APPStandbyHostname=APPSlave
```

The preceding information shows the system IP address, the host name, the subnet mask, the default route, and the relationships between the system IP address and the heartbeat network, replication network, and NMS application network. Details are as follows:

- **SystemIP=10.78.218.52**: The system IP address is **10.78.218.52**.
- **SystemHostname=primary**: The system host name is **primary**.
- **HBCFG=no**: The system IP address is used as the heartbeat IP address (there is no need to set a heartbeat IP address).
- **HBIsIPMP=no**: IPMP is not configured for the heartbeat IP address.
- **VVRCFG=no**: The heartbeat IP address is used as the replication IP address (there is no need to set a replication IP address).
- **APPCfg=yes**: The application IP address needs to be set.

3 Run the following command to view and record routing information:

```
# netstat -rn
```

A message similar to the following will be displayed:

```
Routing Table: IPv4
  Destination           Gateway           Flags  Ref     Use     Interface
-------------------- -------------------- ----- ----- ---------- ---------
default              10.78.218.1          UG        1     129077
10.78.218.0          10.78.218.52         U         1       1776 bge0
224.0.0.0            10.78.218.52         U         1          0 bge0
127.0.0.1            127.0.0.1            UH       12    1243318 lo0
```

----End

B.4.11 How to Rectify the Mouse Detection Failure and Open the GUI After the T5220 Is Connected to the KVM

Question

The OS was installed by using the quick installation DVD. After the T5220 is connected to the KVM, the GUI cannot be opened. How do I rectify this fault?

Answer

1 To set the I/O mode, run the following commands:

eeprom output-device=screen

eeprom input-device=keyboard

2 To set the screen resolution and refresh rate, perform the following operations:

1. To view information about the current video card, run the following command:

   # **fbconfig -list**

   A message similar to the following will be displayed:

```
Device File Name            Device Model     Configuration Program
----------------            ------------     --------------
/dev/fbs/nfb0 [a|b]                          SUNWnfb_config
```

2. To view the screen resolution and refresh rate supported for the current video card, run the following command:

   # **fbconfig -res \?**

   A message similar to the following will be displayed:

```
Valid values for -res option are:
        VESA_STD_640x480x60
            ...
            ...
Notes:
Monitor 1 edid data not available, monitor may not support all resolutions.
Monitor 2 edid data not available, monitor may not support all resolutions.

Use unsupported resolutions at your own risk.

* Abbreviations such as "1280x1024x75" may also be used
```

3. To view the current configurations for the video card, run the following command:

   # **fbconfig -propt**

   A message similar to the following will be displayed:

```
--- OpenWindows Configuration for /dev/fb0 ---

OWconfig: machine
Video Mode: not set

Screen Information:
        Doublewide: Disable
        Doublehigh: Disable
        Clone: Disable
        Offset/Overlap: [0, 0]
```

```
        Output Configuration: Direct
        Fake8 Rendering: Disable
```

4. The screen resolution and refresh rate are not set if **Video Mode** is set to **not set**. To set the screen resolution and refresh rate, run the following commands:

   # **fbconfig -dev** */dev/fbs/nfb0* **-res** *1024x768x60* **now**

   A message similar to the following will be displayed:

```
SUNWnfb_config: Warning: no edid data available from monitor A
SUNWnfb_config: Cannot verify that 1024x768x60 is a supported
        video resolution for this monitor
SUNWnfb_config: Use 1024x768x60 anyway (yes/no) ?
```

   Enter **y**, and then press **Enter**. A message similar to the following will be displayed:

```
Setting 1024x768x60
```

5. To view the current configurations for the video card, run the following command:

   # **fbconfig -propt**

   The setting has taken effect if a message similar to the following is displayed.

```
--- Open Windows Configuration for /dev/fb0 ---

OWconfig: machine
Video Mode: 1024x768x60

Screen Information:
        Doublewide: Disable
        Doublehigh: Disable
        Clone: Disable
        Offset/Overlap: [0, 0]
        Output Configuration: Direct
        Fake8 Rendering: Disable
```

3 To restart the OS, run the following command. After the OS is restarted, connect the T2550 to the KVM.

sync;sync;sync;sync

shutdown -y -g0 -i6

----End

B.4.12 How to Check Downloaded Software Packages by Using MD5 Software

Question

How do I check downloaded software packages by using MD5 software?

Answer

1 Download the **MD5_Code_English** file from http://support.huawei.com. The **MD5_Code_English** file contains MD5 code information after all software and document packages are decompressed.

NOTE

Perform the following operations to obtain the **MD5_Code_English** file:

1. Access **http://support.huawei.com**.
2. Choose **Software Center** > **Version Software** > **Network OSS&Service** > **iManager U2000** > **iManager U2000** > **iManager U2000** > **iManager U2000 V100R002** > **iManager U2000 V100R002C01SPC002**.
3. Download the **MD5_Code_English** file in the **Release Document** column.

2 Navigate to **http://www.winmd5.com** and download the WinMD5.

3 Double-click **WinMD5 1.2.exe** to run the WinMD5.

4 Drag the downloaded software package to the window for running the WinMD5. The WinMD5 automatically generates MD5 code information about the downloaded software package and then compares the information with the counterpart in the **MD5_Code_English** file.

- The downloaded software package is correct if the information about the software package is consistent with the counterpart in the **MD5_Code_English** file.
- The software package must be re-downloaded if the information about the software package is inconsistent with the counterpart in the **MD5_Code_English** file.

----End

B.4.13 How to Rectify the Failure to Connect to the Sybase Database During U2000 Installation

Question

How to rectify the failure to connect to the Sybase database during U2000 installation?

Answer

1 This fault occurs if the IP address recorded in the **interfaces** file in the Sybase database is different from the IP address of the U2000 server. To rectify this fault, modify the IP address recorded in the **interfaces** file.

2 To modify the **interfaces** file, run the following command:

$ **vi /opt/sybase/interfaces**

Information similar to the following is displayed:

```
DBSVR master tcp ether 129.9.1.20 4100 query tcp ether 129.9.1.20 4100 master tcp
ether 129.9.1.20 4100 query tcp ether 129.9.1.20 4100 master tcp ether 127.0.0.1
4100 query tcp ether 127.0.0.1 4100

DBSVR_back master tcp ether 129.9.1.20 4200 query tcp ether 129.9.1.20 4200 master
tcp ether 129.9.1.20 4200 query tcp ether 129.9.1.20 4200 master tcp ether
127.0.0.1 4200 query tcp ether 127.0.0.1 4200
```

Change the IP address (for example, 129.9.1.20) recorded in the **interfaces** file to the IP address of the U2000 server.

----End

B.4.14 How to Set the Communication Mode of the Server in a High Availability System (Solaris)?

Question

The server in a high availability system (Solaris) has two communication modes, namely, common and Security Socket Layer (SSL). How to set the common or SSL mode?

Answer

CAUTION

In a high availability system (Solaris), the communication mode of the server is automatically synchronized from the primary site to the secondary site. Therefore, only the procedure for setting the communication mode on the primary site is described here.

1. Log in to the OS as the **root** user and run the following commands to query the communication mode in use:

   ```
   # cd /opt/U2000/server # . ./svc_profile.sh # ssl_adm -cmd query
   ```

   NOTE

   Leave a space between the dot (.) and **./svc_profile.sh**.

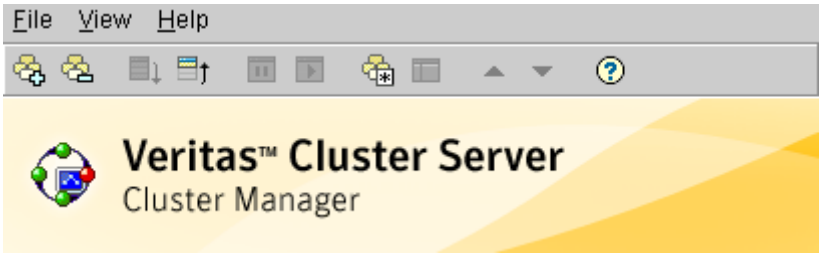
2. Stop the U2000 processes.

   The U2000 processes consist of the U2000 server process and the Sybase process.

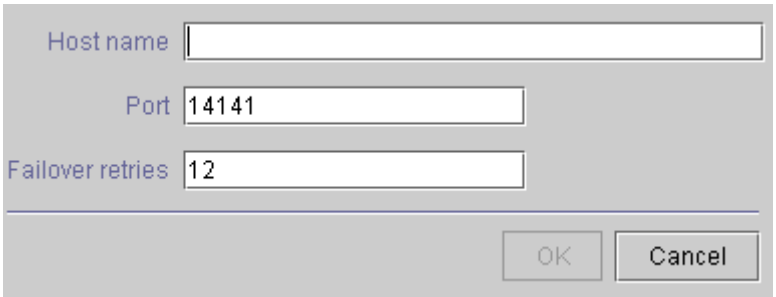
   Check whether the U2000 processes are stopped and perform the following operations:

   1. Access the **Java Desktop System, Release 3** session of the OS of the server of the active site as the **root** user.
   2. Run the following command to start the VCS client:

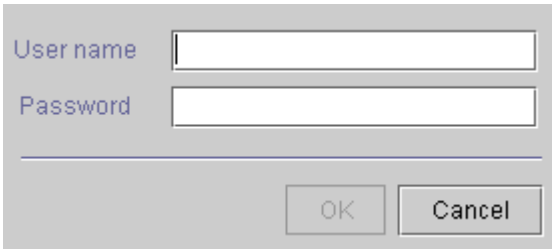
      ```
      # hagui &
      ```

   3. Choose **File** > **New Cluster**. A dialog box is displayed, as shown in the following figure.

4. Enter the IP address of the Heartbeat network service of the primary site. Then, click **OK**.



5. Enter the default user name **admin** and the default password **password** of the VCS client. Then, click **OK**.
6. Select the **AppService** resource group from the navigation tree, click the **Status** tab, and then view the status of the U2000 processes.
   - If **Group Status on Member Systems** is displayed as **Offline**, it indicates that the U2000 processes are stopped.
   - If **Group Status on Member Systems** is displayed as **Online**, it indicates that the U2000 processes are started. Do as follows to stop the U2000 processes:

     Right-click **AppService** and choose **Offline** > ***host_name*** from the shortcut menu.

3 Run the following commands to set the communication mode of the server:

```
# ssl_adm -cmd setmode mode parameter
```

NOTE

In the preceding command, *mode parameter* can be **normal**, **ssl**, or **both**. The description of each value is as follows:

- **normal**: Indicates that the U2000 server communicates with clients only in normal mode without security assurance.
- **ssl**: Indicates that the U2000 server communicates with clients only in security mode. This mode ensures the communication security.
- **both**: Indicates that both the normal and SSL modes are applicable to the U2000 server to communicate with clients.

4 In the **Cluster Explorer** window, right-click the **AppService** resource group in the navigation tree and choose **Online** > **primary** from the shortcut menu to start the Sybase process and U2000 server process.

TIP

Click the **Resources** tab to view the start status of each resource.

Normally, on the **Status** tab page, **Online** is displayed for **State** in the **Group Status on Member Systems** area on the active site, and **Online on primary** is displayed for **Status** in the **Resource Status** area.

NOTE

- In actual configuration, use the actual host name.
- If a fault has occurred during start of the AppService process, right-click **AppService** and choose **clear fault** from the shortcut menu to clear the fault. Then, choose **Online** > ***host_name*** to start the AppService process.

5 In the dialog box that is displayed, click **Yes**.

----End

C Uninstalling the U2000 Software

This topic describes how to uninstall the U2000 software. Uninstall the U2000 software prior to reinstallation.

C.1 Uninstalling U2000 Software

This topic describes how to uninstall U2000 software.

Prerequisite

All servers on the primary and secondary sites must be started on the MSuite server side.

CAUTION

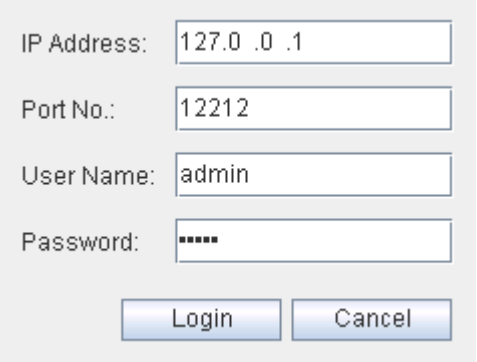
Step 1 to Step 2 needs to be performed only on the server on the active site. Step 3 to Step 10 must be performed on both the primary and secondary sites.

Procedure

1. Log in to the **Java Desktop System, Release 3** session of the master server at primary site OS as the nmsuser user.
2. Disconnect the primary site from the secondary site.
   1. On the server on the active site, run the following commands to start the MSuite client:

      ```
      $ cd /opt/U2000/engineering
      $ ./startclient.sh
      ```

      Wait for about one minute. A dialog box is displayed, as shown in the following figure.

      Then, set the related parameters according to the following table.

Parameter	Settings
IP Address	Specifies the system IP address on the primary site. ● If the Network Management System Maintenance Suite client and the Network Management System Maintenance Suite server are on the same computer, you must enter 127.0.0.1 or the system IP address on the primary site. ● If the Network Management System Maintenance Suite client and the Network Management System Maintenance Suite server are on different computers, enter only the system IP address on the primary site.
Port Number	Specifies the port number. The default value is **12212**.
User Name	Specifies the user name. The default value is **admin**.
Password	Specifies the password of the **admin** user. The default password is **admin**.

2. Click **Login** to access the **NMS Maintenance Suite** window.

   NOTE

   When you log in to the MSuite client, a progress bar showing the progress of querying subsystems and instances is displayed. Wait until the operation is complete.

3. Choose **Deploy** > **Separate Primary and Secondary Nodes**. A progress bar is displayed, indicating the progress of disconnecting the primary site from the secondary site. Wait for about five minutes until a dialog box is displayed indicating that the operation is complete.
4. Click **OK**.
5. Choose **System** > **Log Out** from the main menu. The **Log Out** dialog box is displayed.
6. Click **OK**.

3 Ensure that all U2000 processes on the active site have been stopped and the database has been started on the active site and standby site.

Run the following command to check whether the U2000 processes have been started:

```
$ daem_ps
```

A message similar to the following will be displayed:

```
nmsuser 27069     1   0 10:31:39 ?           1:39 imapmrb
nmsuser 27079     1   0 10:31:39 ?           0:00 imapwatchdog -cmd start
nmsuser 27075     1   0 10:31:39 ?           0:50 imapsysd -cmd start
nmsuser 27086     1   0 10:31:39 ?           0:09 imapeventmgr
nmsuser 23679     1   1 17:57:06 pts/8       0:02 imap_sysmonitor -cmd start
nmsuser 27116     1   0 10:31:40 ?           0:52 ResourceMonitor -cmd start
```

NOTE

If the displayed information contains **imap_sysmonitor -cmd start**, it indicates that the U2000 process has been started.

If the U2000 process has been started, do as follows to stop the U2000 process and start the sybase process:

1. On the primary site, log out as the **nmsuser** user and then log in the OS again as the **root** user.

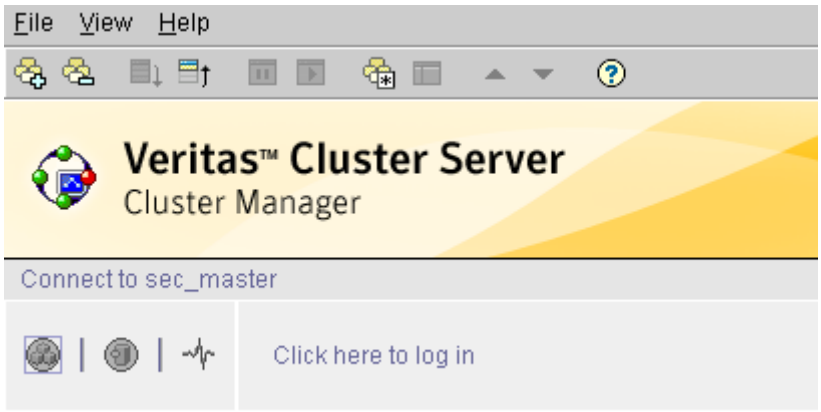
2. Open a CLI. Then, run the following command to start the VCS client:

   NOTE

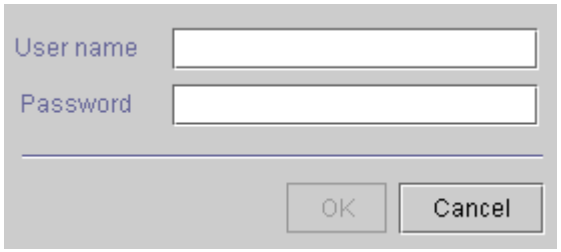
   If the server does not have the GUI desktop, run the following commands to stop the U2000 processes and start the database:

   ```
   # hares -offline NMSServer -sys host name
   # hares -online DatabaseServer -sys host name
   # hares -online BackupServer -sys host name
   ```

   ```
   # hagui &
   ```

3. Click **Click here to log in**.

4. Enter the default user name (**admin**) and initial password (**password**) for the VCS client. Then, click **OK**.
5. In the resource tree, select **NMSServer**, right-click, and then choose **Offline** > ***host name*** from the shortcut menu.
6. In the confirmation dialog box, click **Yes**.

NOTE

- If the NMS process resource **NMSServer** is in the **Offline on Primaster** state, it indicates that the U2000 processes have been stopped.
- If the database resource **BackupServer** is in the **Online on *host name*** state, it indicates that the database has been started.

4 Run the following commands on the server on the primary and secondary sites to stop the MSuite server:

```
# cd /opt/HWENGR/engineering
# ./stopserver.sh
```

5 Run the following command on the servers at the primary and secondary sites to go to the path where the **uninstall.sh** script is stored and run the script:

NOTE

Two modes are available to uninstall the U2000. One is the GUI mode and the other is the CLI mode. The procedure for uninstalling the U2000 in GUI mode is described in the following sections. Installation engineers are recommended to uninstall the U2000 through the CLI if they cannot log in to the GUI of the OS.

Run the **./uninstall.sh -cmd** command to uninstall the U2000 in the **/opt/HWENGR** path through the CLI.

```
# cd /opt/HWENGR
# ./uninstall.sh
```

The **Confirm Uninstallation** dialog box will be displayed.

6 Click **Yes**. A dialog box showing the progress of the uninstall will be displayed.

NOTE

The duration of the uninstall depends on the quantity of installed components. Wait patiently.

7 After the uninstall is complete, the **Uninstallation Complete** dialog box is displayed.

8 Click **Finish**.

9 Run the following command to delete the **/opt/HWENGR** path. Ensure that the current environment is the initial installation environment.

```
# rm -rf /opt/HWENGR
```

----End

C.2 Verifying the Uninstall Status of the Server Software

This topic describes how to verify that the U2000 server software is uninstalled.

Procedure

1 Log in to the OS of the server as user **root**.

2 Confirm that the installation path is correct during the uninstall.

- If the server is not mounted with disk arrays, the NMS installation path**/opt/U2000** will be deleted.
- If the server is mounted with disk arrays, the NMS installation path **/opt/U2000** will be empty.

The installation paths **/opt/HWENGR**, **/opt/HWICMR** and **/opt/HWNMSJRE**, are deleted.

3 Confirm the **nmsuser** user that must be deleted during the uninstall.

Run the following command to switch to user **nmsuser**:

```
# su - nmsuser
```

A message similar to the following will be displayed:

```
su: unknown id: nmsuser
```

----End

D Getting Started

This topic describes certain common operations that can be performed on the Solaris workstation. After learning this topic, you can improve the efficiency of the operations in the Solaris OS.

Syntax Structure of Command Lines

The syntax structure of command lines is as follows:

```
command option parameter
```

The Solaris commands are case-sensitive. That is, the OS considers an uppercase letter and its corresponding lowercase letter two different letters. For example, when you want to use the command for displaying the files in the certain directory, the OS can correctly run the **ls** command, but it cannot run the **Ls** command because the **Ls** command is considered as an invalid system command. The options in the Solaris commands are used to change the command execution method. Generally, the options start with the en-dash (-).

For example, run the following command to display the files and the related details in the **/opt** directory:

```
ls -al /opt
```

Switching to the bash Mode

It is recommended that you switch the system to the bash mode after logging in to the OS to reduce the period used for entering commands. Generally, after logging in to the OS, you can run the **bash** command to switch to the bash mode, as shown in the following figure.

The following basic features of the bash mode help you interact with the system better:

- Command line editing: enables you move the cursor among command lines or edit text.
- History command: allows you to edit or restore the command that has been entered in command lines.

For example, if you enter the first two or three letters of a command or a file and then press **Tab**, the system automatically fills in the desired command or file.

Switching Users

The Solaris OS has strict user management rules. Different OS users can access only associated applications.

- To switch OS users, run the following command:

  `su - OS user name`

  Leave a space between **-** and **OS user name**.

  For example, to switch to the **nmsuser** user, run the following command:

  `su - nmsuser`

- To exit an OS user, run the following command:

  `exit`

  NOTE

  To switch back to the **root** user, run the **exit** command several times until the prompt changes to **#**.

Directory Browsing and Control Commands

Command/Usage	Example	Description
cd *directory*	cd */opt*	Switches to another directory.
ls *option file directory*	ls *-al /opt*	Displays the directory contents or file information.
mkdir *directory*	mkdir *install*	Creates a directory.
pwd	pwd	Displays the current directory of the user.
rm *file name*	rm *file.tar*	Deletes a file.
rmdir *directory*	rmdir *temp*	Deletes an empty directory.

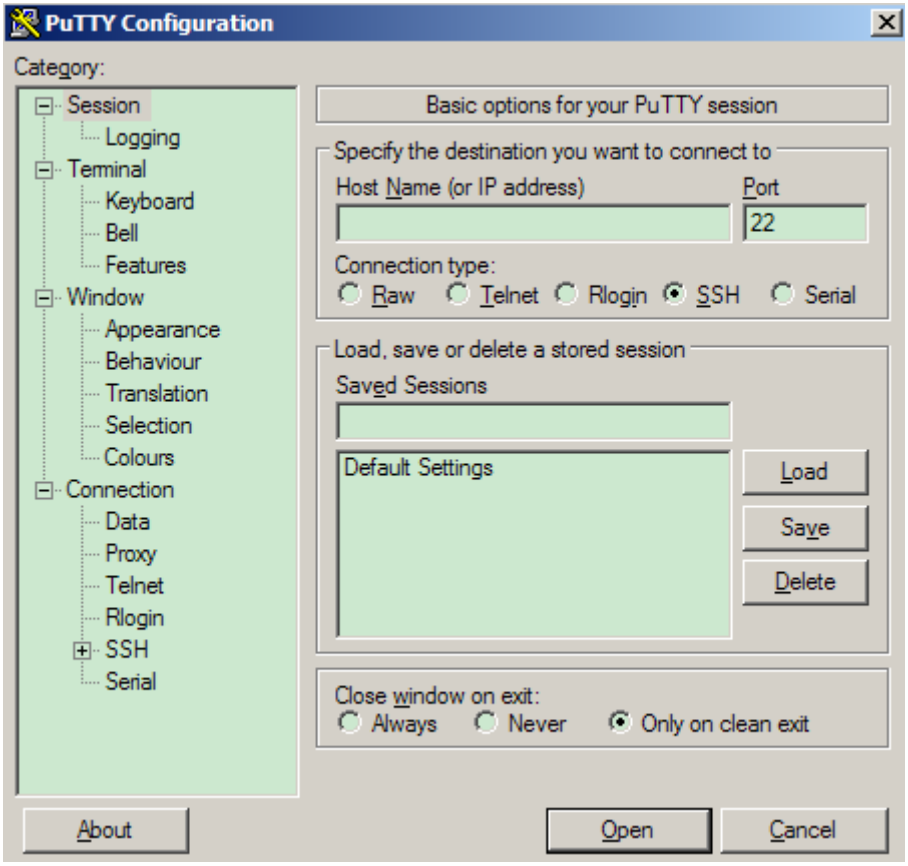
Logging In to the Solaris OS Through Remote Login Software

There are many remote login software products, such as the PuTTY. This topic takes the PuTTY as an example. The PuTTY is used to log in to the server from a remote site through command lines.

CAUTION

Make sure that the remote login software is installed.

1. Double-click the shortcut icon of the PuTTY software on the desktop. The following dialog box is displayed.



The following table shows the login configurations.

Parameter	Description
Host Name (or IP address)	Specifies the IP address of the server to be logged in to, for example, 10.71.225.89.
Connection type	Specifies the connection type. You need to select a connection type as required. Generally, select **Telnet** or **SSH**.
Saved Sessions	This parameter cannot be set.
Close window on exit	This parameter cannot be set. The default value is **Only on clean exit**.

2. Set the parameters for logging in to the server. Then, click **Open**. The login dialog box is displayed.
3. Enter the login user name, and then press **Enter**.
4. Enter the login password, and then press **Enter**.

Accessing the CLI of the Windows OS

1. Choose **Start** > **Run** on the Windows OS desktop.
2. In the **Run** dialog box, enter **cmd**, and then click **OK**. The CLI is displayed.

Logging In to the Solaris OS Through the Windows OS CLI

1. In the CLI, enter **telnet IP address of the server to be logged in to**, and then press **Enter**.
   ```
   Login:
   ```
2. Enter the name of the user who logs in to the OS of the server, for example, **root**. Then, press **Enter**.
   ```
   Password:
   ```
3. Enter the login password of the user. Press **Enter** to log in to the OS. Generally, the default login password of the **root** user is **root**.

Restarting the Solaris OS

Run the following commands to restart the OS:

```
# sync;sync;sync;sync
# shutdown -y -g0 -i6
```

When you restart the OS, the remote login user exits. It takes approximately 3 to 5 minutes to restart the OS. After the OS is restarted, re-log in to the server by referring to the preceding login method.

E Powering Off the High Availability System (Solaris)

This topic describes how to power off the system. Do not power off the U2000 when it is properly managing NEs. The U2000 only needs to be shut down in special circumstances (such as switching the power supply).

Context

- Always follow site-specific procedures for powering off the server to ensure that it is safely shut down.
- The system may fail to recover if the **halt** command is used to shut down the server or if the server is directly powered off.

Procedure

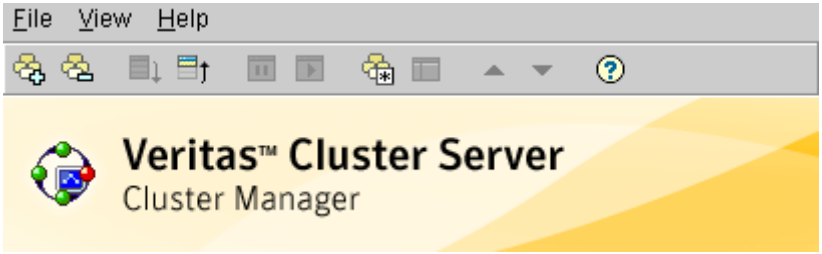
1. Exit all running U2000 clients.
2. Stop the U2000 processes.

   The U2000 processes consist of the U2000 server process and the Sybase process.

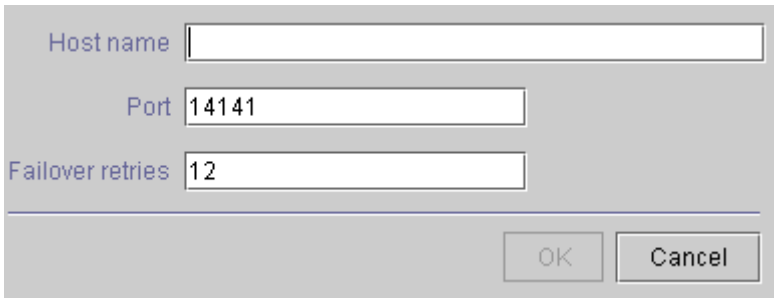
   Check whether the U2000 processes are stopped and perform the following operations:

   1. Access the **Java Desktop System, Release 3** session of the OS of the server of the active site as the **root** user.
   2. Run the following command to start the VCS client:

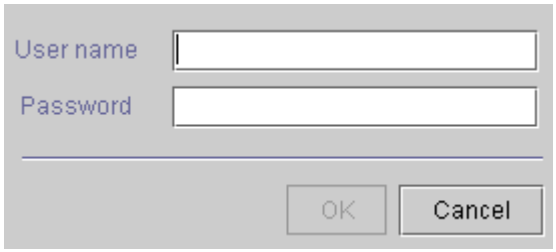
      ```
      # hagui &
      ```

   3. Choose **File** > **New Cluster**. A dialog box is displayed, as shown in the following figure.



4. Enter the IP address of the Heartbeat network service of the primary site. Then, click **OK**.



5. Enter the default user name **admin** and the default password **password** of the VCS client. Then, click **OK**.
6. Select the **AppService** resource group from the navigation tree, click the **Status** tab, and then view the status of the U2000 processes.
   - If **Group Status on Member Systems** is displayed as **Offline**, it indicates that the U2000 processes are stopped.
   - If **Group Status on Member Systems** is displayed as **Online**, it indicates that the U2000 processes are started. Do as follows to stop the U2000 processes:

     Right-click **AppService** and choose **Offline** > ***host_name*** from the shortcut menu.

3 Log in to the server of the active site as user **root** and run the following commands to stop the VCS service:

```
# cd /opt/VRTSvcs/bin
# hastop -local -force
```

4 Run the following command to verify that the VCS service is stopped:

```
# ps -ef|grep had
```

A message similar to the following will be displayed:

```
root 27663 17299   0 00:31:00 pts/2  0:00 grep had
```

NOTE

If the **had** and **hadshadow** processes are not displayed, the VCS service is successfully stopped; otherwise, run the **kill -9 process ID** command to stop the related processes.

5 Log in to the server of the standby site as the **root** user and perform the preceding two steps to stop the VCS service on the server of the standby site.

6 Shut down the OS of the standby site.

1. Log in to the OS of the standby site as the **root** user.
2. Run the following command to shut down the OS of the standby site:

```
# sync;sync;sync;sync
# shutdown -y -g0 -i5
```

7 Run the following command to shut down the OS of the active site:

```
# sync;sync;sync;sync
# shutdown -y -g0 -i5
```

----End

F Manually Installing the Solaris OS and Its Patches

This topic describes how to manually install the OS by using the Solaris installation DVD delivered with the product and how to install patches by using the patch package.

F.1 Installing the OS Through the GUI
This topic describes how to install Solaris 10 OS through the GUI if the server is connected to the KVMS or monitor.

F.2 Installing the OS Through the CLI
This topic describes how to install Solaris 10 OS through the CLI if the server is not connected to the KVMS or monitor.

F.3 Installing the Solaris OS Patches
This topic describes how to install the Solaris OS patches. To ensure the reliable system performance, the **huawei_patch_9.0.1** patch must be installed immediately after the Solaris OS is installed.

F.1 Installing the OS Through the GUI

This topic describes how to install Solaris 10 OS through the GUI if the server is connected to the KVMS or monitor.

Prerequisite

- The Solaris 10 OS disk, that is, Solaris 10 Operating System (10/08), is on-hand.
- Obtain the following information:
  - Host name
  - Network interface
  - System IP address
  - Subnet mask
  - Default Route IP address
- The server is connected to the keyboard, video, mouse, switch (KVMS) or monitor.

Context

- The system will go straight to the OK prompt if Solaris OS has not been installed on the server.
- The system will go to the OK prompt if Solaris OS is installed on the server when user **root** runs the **init 0** command.

Procedure

1. Power on the Sun server and insert the Solaris 10 OS installation DVD into the DVD-ROM drive.
2. Press **STOP+A**. At the **OK** prompt, run the following command:

   ```
   ok boot cdrom
   ```

   Press **Enter**. The system will restart. After five minutes, the system will prompt you to select the language for the installation program.
3. Move the pointer to the text box. Enter **0** to select **English** and press **Enter**.
4. In the **Welcome** dialog box, click **Next**.
5. In the **Network Connectivity** dialog box, select **Networked** and click **Next**.
6. **Optional:** In the **Configure Multiple Network Interfaces** dialog box, select a primary network interface such as e1000g0, and click **Next**.

   NOTE

   - If the server contains only one network interface, the **Configure Multiple Network Interfaces** dialog box will not be displayed.
   - You are recommended to select the first network interface in scenarios where the server contains multiple network interfaces (the **Configure Multiple Network Interfaces** dialog box will be displayed).
   - The network interface name is related to the network adapter type. The common types of network adapters are *e1000g*, *bge*, and *ce*.

7 In the **DHCP for e1000g0** dialog box, select **No** and click **Next**.

8 In the **Host Name for e1000g0** dialog box, enter the planned host name and click **Next**.

9 In the **IP Address for e1000g0** dialog box, enter the planned IP address and click **Next**.

10 In the **Netmask for e1000g0** dialog box, enter the planned subnet mask and click **Next**.

11 In the **IPv6 for e1000g0** dialog box, select **No** and click **Next**.

12 In the **Set the Default Route for e1000g0** dialog box, select **Specify one** and click **Next**.

CAUTION

The default route is not recommended if the NMS security policies are used. After installing the NMS, manually configure the static route. For details about how to manually configure the static route, see **B.1.1.2 How to Add a Static Route**.

13 In the **Set the Default Route for e1000g0** dialog box, enter the route IP address and click **Next**.

14 In the **Kerberos** dialog box, select **No** for the **Kerberos** security and click **Next**.

15 In the **Name Service** dialog box, select **None** for the name service and click **Next**.

16 In the**NFSv4 Domain Name** dialog box, select **Use the NFSv4 domain derived by the system** and click **Next**.

17 In the **Time Zone** dialog box, select **Geographic Continent/Country/Region** and click **Next**.

18 In the **Country or Region** dialog box, select the appropriate country and region. For example, select **Asia** and **China**. Then, click **Next**.

19 In the **Date and Time** dialog box, set the time and click **Next**.

CAUTION

In the OS, the system time must be set correctly according to the specified format. Stable system time is of vital importance to the system. Hence, do not modify the system time while the server is running.

20 In the **Root Password** dialog box, enter the password of user **root** twice and click **Next**.

NOTE

Do not forget the password of user **root**.

21 In the **Enabling Remote Services** dialog box, select **Yes** and click **Next**.

22 In the **Confirm Information** dialog box, confirm that the configuration is correct and click **Confirm**; click **Back** to modify the configuration.

23 In the **Welcome** dialog box, click **Next**.

24 In the **Installer Options** dialog box, select **Yes** for **Reboot automatically after software installation** and **Eject CD/DVD automatically after software installation**. Then, click **Next**.

25 In the **Specify Media** dialog box, select **CD/DVD** and click **Next**.

26 In the **License** dialog box, select **Accept** and click **Next**.

NOTE

If the **Select Upgrade** or **Initial Install** dialog box is displayed during installation, the system can be upgraded. You can select **Initial Install** if the original system configuration is not required.

27 In the **Select Type of Install** dialog box, select **Custom Install** and click **Next**.

28 In the **Select Software Localizations** dialog box, select **English (United States) (en_US)** and **English (United States, UTF-8) (en_US.UTF-8)** for **North America** and click **Next**.

29 In the **Select System Locale** dialog box, select **POSIX C (C)** and click **Next**.

30 In the **Additional Products** dialog box, select **None** and click **Next**.

31 In the **Select Solaris Software Group** dialog box, select **Default Packages for Entire Group Plus OEM** and click **Next**.

32 In the **Disk Selection** dialog box, select all disks and click **Next**.

33 In the **Preserve Data** dialog box, select **No** and click **Next**.

34 In the **Lay Out File Systems** dialog box, select the desired disks to lay out file systems, and click **Modify** to partition the disks.

CAUTION

Select the disks to be partitioned according to the disk partition plan. For details, see **G Planning Disk Partitions**. Assume that you need to partition the c1t0d0 and c1t1d0 disks need to be partitioned, both disks must be selected during this step; otherwise, the selected disks cannot be partitioned. It is important that the correct disks are selected because this step cannot be undone.

NOTE

- The sector names shown as **0**, **1**, **3**, **4**, **5**, **6**, and **7** respectively refer to c1t0d0s0, c1t0d0s1, c1t0d0s3, c1t0d0s4, c1t0d0s5, c1t0d0s6, and c1t0d0s7. The size of the overlap partition corresponding to the c1t0d0s2 disk is the same size as the entire disk. Therefore, there is no need to set the size.
- The disk names vary according to device model.

35 Click **OK**. In the **Lay Out File Systems** dialog box, click **Next**.

36 In the **Ready to Install** dialog box, click **Install Now**.

A dialog box will be displayed that shows the progress of the installation. The duration of the installation process depends on the server configuration. Generally, the installation lasts 60 minutes.

NOTE

- Click **Continue** each of the three times that the **Pause** dialog box is displayed during installation. The system will automatically restart and the installation will continue if this operation is not performed.
- After the installation is complete, the DVD-ROM door will automatically open. Take out the DVD.

37 After the system restarts, log in to the Solaris OS as user **root**.

If login to Solaris OS as user **root** is possible, Solaris OS is successfully installed. Otherwise, install the OS again.

----End

Follow-up Procedure

After the Solaris OS is installed, verify that the system character set is correct, and enable user **root** to remotely log in to the system and use the FTP tool.

1. Run the following command to verify that the system character set is correct:

   ```
   # locale -a
   ```

   If the following information is included in the command output, the character set of Solaris OS is correct. Otherwise, reinstall the OS.

   ```
   C
   en_US.UTF-8
   ```

2. Enable the **root** user to remotely log in to the system.

   (1) Run the **vi** command to modify the **/etc/default/login** file:

   ```
   # vi /etc/default/login
   ```

   (2) Add **#** to the left of *CONSOLE=/dev/console* to comment out this line. The following message will be displayed:

   ```
   ¡¡
   # If CONSOLE is set, root can only login on that device.
   # Comment this line out to allow remote login by root.
   #
   # CONSOLE=/dev/console
   ...
   ```

   (3) Press **ESC**. Press **Shift+;**. Enter **wq!**. Then, press **Enter** to forcibly save the file and exit.

3. Enable the **root** user to use the FTP tool.

   (1) Run the **vi** command to modify the **/etc/ftpd/ftpusers** file.

   (2) Add **#** to the left of *root* to comment out this line. The following message will be displayed:

   ```
   # ident "@(#)ftpusers 1.5 04/02/20 SMI"
   #
   # List of users denied access to the FTP server, see ftpusers(4)
   #
   #root
    daemon
    bin
    sys
   ...
   ```

   (3) Press **ESC**. Press **Shift+;**. Enter **wq!**. Then, press **Enter** to forcibly save the file and exit.

4. Run the following commands to restart the server:

   ```
   # sync;sync;sync;sync
   # shutdown -y -g0 -i6
   ```

F.2 Installing the OS Through the CLI

This topic describes how to install Solaris 10 OS through the CLI if the server is not connected to the KVMS or monitor.

Prerequisite

- The Solaris 10 OS disk, that is, Solaris 10 Operating System (10/08), is on-hand.
- Obtain the following information:
  - Host name
  - Network interface
  - System IP address
  - Subnet mask
  - Default Route IP address
- The IP address of the system controller is configured. For details about how to configure the IP address, see **4.1 Configuring Controller IP Addresses for Workstation**.

Procedure

1 **Optional:** If the T5220 server is used, perform the following operations to display the **OK** prompt:

1. Log in to the system controller in SSH mode.

   NOTE

   The T5220 server does not support login through Telnet. Log in to the system controller performing the following:

   - Install the tool software of the SSH client on the Windows terminal to log in to the system controller, for example: **Putty**.
   - Run the **ssh** *SC_IP_Address* command on the terminals of other Sun servers. If the following message is displayed, enter **yes**:

     ```
     The authenticity of host '129.9.1.20 (129.9.1.20)' can't be
     established.
     RSA key fingerprint is 0b:23:07:0c:27:72:44:3f:d1:aa:12:99:ed:dd:c0:5a.
     Are you sure you want to continue connecting (yes/no)?
     ```

2. In the CLI, enter the user name and password of the system controller. The default user name and password are **root** and **changeme**.
3. Enter **set /HOST/bootmode state=reset_nvram script="setenv auto-boot? false"**.

   NOTE

   There must be a space between **?** and **false**.

   The following message will be displayed:

   ```
   Set 'state' to 'reset_nvram'
   Set 'script' to 'setenv auto-boot? false'
   ```

4. Enter **start /SYS**.

   The following message will be displayed:

   ```
   Are you sure you want to start /SYS (y/n)?
   ```

5. Enter **y** to start the T5220.

   The system is running if the following message is displayed:

   ```
   start: Target already started
   ```

   Perform the following operations:

   a. Enter **stop /SYS**.

      The following message will be displayed:

      ```
      Are you sure you want to stop /SYS (y/n)?
      ```

b. Enter **y**.

The following message will be displayed:

```
Stopping /SYS
```

c. Enter **show /HOST status** repeatedly to check the system status.

Proceed with the subsequent operations until the following message is displayed:

```
status = Powered off
```

d. Enter **start /SYS**.

The following message will be displayed:

```
Are you sure you want to start /SYS (y/n)?
```

e. Enter **y** to start the T5220.

6. Enter **start /SP/console -f**.

The following message will be displayed:

```
Are you sure you want to start /SP/console (y/n)?
```

7. Enter **y** and press **Enter**.

NOTE

If a prompt is displayed, enter **y** and press **Enter**.

The following message will be displayed:

```
Serial console started.  To stop, type #.
...
Setting NVRAM parameters to default values.


SPARC Enterprise T5220, No Keyboard
Copyright 2008 Sun Microsystems, Inc.  All rights reserved.
OpenBoot 4.28.0, 8064 MB memory available, Serial #85369820.
Ethernet address 0:21:28:16:a3:dc, Host ID: 8516a3dc.


auto-boot? =            false
{0} ok
```

2 Optional: If the M4000 server is used, perform the following to display the **OK** prompt:

1. Log in to the system controller through Telnet. Run the **telnet *Controller IP Address*** command on the controller.

The following message will be displayed:

```
Login:
```

2. Enter **eis-installer** as the user name.

The following message will be displayed:

```
Password:
```

3. Enter the password of user **eis-installer**.

The following message will be displayed:

```
XSCF>
```

4. Enter **showdomainmode -d 0**.

The following message will be displayed:

```
Host-ID             : 8501c2de
Diagnostic Level    : min
Secure Mode         : off (host watchdog: unavailable Break-signal: receive)
Autoboot            : on
CPU Mode            : auto
```

NOTE

If the **Secure Mode** item is in the **on** state, perform the following:

a. Enter **setdomainmode -d 0 -m secure=off**.

The following message will be displayed:

```
Diagnostic Level    :min        -> -
Secure Mode         : on         -> off
Autoboot            : on         -> -
CPU Mode            : auto
The specified modes will be changed.
Continue? [y|n]
```

b. Enter **y**.

The following message will be displayed:

```
configured.
Diagnostic Level    : min
Secure Mode         : off (host watchdog: unavailable Break-signal:
receive)
Autoboot            : on (autoboot:on)
CPU Mode            : auto
```

5. Enter **showdomainstatus -a**.

The following message will be displayed:

```
DID         Domain Status
00          Running
01          -
```

NOTE

If the following message is displayed, run the **poweron -d 0** command:

```
DID         Domain Status
00          Powered Off
01          -
```

Run the **showdomainstatus -a** command repeatedly to check the system status. Proceed with the next step only after the status is displayed as **running**.

6. Enter **sendbreak -d 0**.

The following message will be displayed:

```
Send break signal to DomainID 0? [y|n]
```

7. Enter **y**.

8. Enter **console -d 0 -f**.

The following message will be displayed:

```
Connect to DomainID 0? [y|n]
```

9. Enter **y** and press **Enter**.

```
OK
```

3 Insert the Solaris 10 installation DVD into the DVD-ROM drive.

4 Run the following command to boot the system for installation preparation:

```
ok boot cdrom
```

Press **Enter**. The system will restart. After five minutes, the system will prompt you to select the language for the installation program.

5 In the **Select a Language** dialog box, the system prompts "Please make a choice (0-9), or press h or ? for help:." Enter **0** and select **English**. Then, press **Enter**.

NOTE

The language selected in this step only applies to the language environment of this installation process. It is irrelevant to the languages supported by the Solaris OS after installation.

6 In the **What type of terminal are you using?** dialog box, the system prompts "Type the number of your choice and press Return:". Enter **3** and set the type of the terminal used during OS installation to **DEC VT100**. Then, press **Enter**.

7 In the **The Solaris Installation Program** dialog box, press **F2**.

NOTE

- If **F2** does not function, press **Esc+2** instead.
- If ↑ or ↓ does not function, use **Ctrl+B** or **Ctrl+N** instead.

8 In the **Identify This System** dialog box, press **F2**.

9 In the **Network Connectivity** dialog box, click **Yes** to connect the network. Then, press **F2**.

NOTE

You can use ↑ and ↓ to move the cursor to the required bracket. Then, press **Enter**. The selection is complete if **X** is displayed in the bracket.

10 **Optional:** In the **Configure Multiple Network Interfaces** dialog box, select a primary network interface, such as *e1000g0*. Then, press **F2**.

NOTE

- If the server contains only one network interface, skip this step.
- If the server contains multiple network interfaces, the **Configure Multiple Network Interfaces** dialog box will be displayed. In this scenario, you are recommended that you select the first network interface as the primary network interface for connecting to the public network.
- The network interface name is related to the network adapter type. The common types of network adapters are *e1000g*, *bge*, and *ce*.

11 In the **DHCP for e1000g0** dialog box, select **No** to disable DHCP and press **F2**.

12 In the **Host Name for e1000g0** dialog box, enter the planned host name and press **F2**.

13 In the **IP Address for e1000g0** dialog box, enter the planned server IP address and press **F2**.

14 In the **Subnet for e1000g0** dialog box, select **Yes** and press **F2**.

15 In the **Netmask for e1000g0** dialog box, enter the planned subnet mask and press **F2**.

16 In the **IPv6 for e1000g0** dialog box, select **No** to disable IPv6 and press **F2**.

17 In the **Set the Default Route for e1000g0** dialog box, select **Specify one** and press **F2**.

CAUTION

The default route is not recommended if the NMS security policies are used. After installing the NMS, manually configure the static route. For details about how to manually configure the static route, see **B.1.1.2 How to Add a Static Route**.

18 In the **Set the Default Route for e1000g0** dialog box, enter the route IP address. Then, press **F2**.

19 In the **Confirm Information for e1000g0** dialog box, confirm that the configuration is correct and press **F2**.

NOTE

If any information is incorrect, you can press **F4** to return to the **Network Connectivity** dialog box, and modify the settings of the network connection.

20 In the **Configure Security Policy** dialog box, select **No** to skip the configuration of Kerberos security. Then, press **F2**.

21 In the **Confirm Information** dialog box, confirm that the security configuration is correct and press **F2**.

NOTE

If any information is incorrect, press **F4** to return to the **Configure Security Policy** dialog box, and modify the settings of security policies.

22 In the **Name Service** dialog box, select **None** to skip the configuration of the name server. Then, press **F2**.

23 In the **Confirm Information** dialog box, confirm that the name server configuration is correct and press **F2**.

NOTE

If any information is incorrect, press **F4** to return to the **Name Service** dialog box, and modify the settings of the name server.

24 In the **NFSv4 Domain Name** dialog box, select **Use the NFSv4 domain derived by the system**. Then, press **F2**.

25 In the **Confirm Information for NFSv4 Domain** dialog box, ensure that **NFSv4 Domain Name: Value to be derived dynamically** is displayed. Then, press **F2**.

26 In the **Time Zone** dialog box, select the appropriate geographical area, such as **Asia**, according to your location. Then, press **F2**.

CAUTION

Do not select **other - offset from GMT** or **other - specify time zone file**. Otherwise, a system time error may occur.

27 In the **Country or Region** dialog box, select the appropriate country or region, such as **China**, according to your location. Then, press **F2**.

28 In the **Date and Time** dialog box, set precise system time. Then, press **F2**.

CAUTION

In the OS, the system time must be set correctly according to the specified format. Stable system time is of vital importance to the system. Hence, do not modify the system time while the server is running.

29 In the **Confirm Information** dialog box, confirm that the preceding configuration is correct and press **F2**.

30 In the **Root Password** dialog box, enter the password of the **root** user twice to set the password. Then, press **F2**.

NOTE

Do not forget the password of user **root**.

31 In the **Identify This System** dialog box, confirm that the configuration is correct and press **F2**.

32 In the **Enabling remote services** dialog box, select **Yes** and press **F2**.

33 In the **Solaris Interactive Installation** dialog box, press **F2** to select the **Standard** installation.

34 In the **Eject a CD/DVD Automatically?** dialog box, select **Automatically eject CD/DVD** to automatically install the software through the drive. Then, press **F2**.

35 In the **Reboot After Installation?** dialog box, select **Auto Reboot** to set the restart mode to automatic restart. Then, press **F2**.

36 In the **Solaris Interactive Installation** dialog box, press **F2** to start initial installation.

37 In the **Select Geographic Regions** dialog box, press **Enter** to expand the **Asia** list. Select **Simplified Chinese EUC**, **Simplified Chinese GB18030**, **Simplified Chinese GBK**, and **Simplified Chinese UTF-8**. Expand the **North America** list. Select **U.S.A.(UTF-8)** and **U.S.A. (en_US.ISO8859-1)**. Then, press **F2**.

NOTE

The selections in this step determine the languages supported by the Solaris OS to be installed. Use ↑ and ↓ to move the cursor to the selected list. Then, press **Enter**. The subitems will be displayed. Use ↑ and ↓, or ← and → to move the cursor to the required bracket. Press **Enter**. If **X** is displayed in the bracket, the language is selected.

38 In the **Select System Locale** dialog box, select **POSIX C (C)** and press **F2**.

39 In the **Additional Products** dialog box, select **None** and press **F2**.

40 In the **Choose Filesystem Type** dialog box, select **UFS** and press **F2**.

41 In the **Select Software** dialog box, select **Entire Distribution plus OEM support** and press **F2**.

42 In the **Select Disks** dialog box, select all disks and press **F2**.

43 In the **Preserve Data?** dialog box, press **F2**. The data on the disk is not preserved.

44 In the **Automatically Layout File Systems?** dialog box, press **F4** to manually partition disks and plan the file system.

45 In the **File System and Disk Layout** dialog box, select the disk to be partitioned, and press **F4** to manually define disk partitions.

CAUTION

Select the disks to be partitioned according to the disk partition plan. For details, see **G Planning Disk Partitions**. Assume that you need to partition the c1t0d0 and c1t1d0 disks need to be partitioned, both disks must be selected during this step; otherwise, the selected disks cannot be partitioned. It is important that the correct disks are selected because this step cannot be undone.

NOTE

- The sector names shown as **0**, **1**, **3**, **4**, **5**, **6**, and **7** respectively refer to c1t0d0s0, c1t0d0s1, c1t0d0s3, c1t0d0s4, c1t0d0s5, c1t0d0s6, and c1t0d0s7. The size of the overlap partition corresponding to the c1t0d0s2 disk is the same size as the entire disk. Therefore, there is no need to set the size.
- The disk names vary according to device model.

46 In the **Select Disk to Customize** dialog box, perform the following to partition the selected disks:

1. Select the first disk. Move the cursor to the line of the c1t0d0 disk and press **F4**. The **Customize Disk: c1t0d0** dialog box will be displayed.
2. Define the partition and press **F2**. The **Select Disk to Customize** dialog box will be displayed.
3. Select other disks. For details, see the preceding steps for disk partitioning.

   NOTE

   You do not need to perform this step if the server is equipped with two disks or four disks without any disk array.

47 In the **File System and Disk Layout** dialog box, confirm that the disk partition plan is correct and press **F2**.

48 In the **Mount Remote File Systems?** dialog box, press **F2** to continue without installing the distributed file system.

49 In the **Profile** dialog box, confirm that the preceding configuration is correct and press **F2**.

NOTE

If the Solaris OS has been installed on the server and the currently planned boot partition is not on the disk where the original boot partition is located, a warning will indicate that the default boot device changed. In the **Warning** dialog box, press **F2** to ignore the warning and proceed with the following steps.

50 The duration of the installation process will vary according to the server configuration. Generally, the installation lasts 60 minutes.

NOTE

During system installation, a progress bar will be displayed.

When the following message is displayed, enter **c**:

```
Pausing for 30 seconds at the "Summary" screen. The wizard will continue to the next
step unless you select "Pause". Enter 'p' to pause. Enter 'c' to continue.
```

The system will continue the installation.

When the following message is displayed, enter **c**:

```
Pausing for 90 seconds at the "Reboot" screen. The wizard will continue to the next
step unless you select "Pause". Enter 'p' to pause. Enter 'c' to continue.
```

The system will restart automatically.

If no operation is performed, the OS will automatically restart after 90 seconds.

CAUTION

After the installation, the DVD-ROM door will automatically open. Take out the disk.

51 In the **Configure Keyboard Layout** dialog box that is displayed after system restart, select **US-English**. Then, press **F2** to complete all configurations and access the Solaris OS.

If login to Solaris OS as user **root** is possible, Solaris OS is successfully installed. Otherwise, install the OS again.

----End

Follow-up Procedure

After the Solaris OS is installed, verify that the system character set is correct, and enable user **root** to remotely log in to the system and use the FTP tool.

1. Run the following command to verify that the system character set is correct:

   ```
   # locale -a
   ```

   If the following information is included in the command output, the character set of Solaris OS is correct. Otherwise, reinstall the OS.

   ```
   C
   en_US.UTF-8
   ```

2. Enable the **root** user to remotely log in to the system.

   (1) Run the **vi** command to modify the **/etc/default/login** file:

   ```
   # vi /etc/default/login
   ```

   (2) Add **#** to the left of *CONSOLE=/dev/console* to comment out this line. The following message will be displayed:

   ```
   ¡¡
   # If CONSOLE is set, root can only login on that device.
   # Comment this line out to allow remote login by root.
   #
   # CONSOLE=/dev/console
   ...
   ```

   (3) Press **ESC**. Press **Shift+;**. Enter **wq!**. Then, press **Enter** to forcibly save the file and exit.

3. Enable the **root** user to use the FTP tool.

   (1) Run the **vi** command to modify the **/etc/ftpd/ftpusers** file.

   (2) Add **#** to the left of *root* to comment out this line. The following message will be displayed:

   ```
   # ident "@(#)ftpusers 1.5 04/02/20 SMI"
   #
   # List of users denied access to the FTP server, see ftpusers(4)
   #
   #root
    daemon
    bin
    sys
   ...
   ```

   (3) Press **ESC**. Press **Shift+;**. Enter **wq!**. Then, press **Enter** to forcibly save the file and exit.

4. Run the following commands to restart the server:

   ```
   # sync;sync;sync;sync
   # shutdown -y -g0 -i6
   ```

F.3 Installing the Solaris OS Patches

This topic describes how to install the Solaris OS patches. To ensure the reliable system performance, the **huawei_patch_9.0.1** patch must be installed immediately after the Solaris OS is installed.

Prerequisite

- The installation package for Solaris 10 OS patches is on-hand. The installation package is U2000***version***_server_ospatch_solaris_SPARC.tar.

  NOTE

  Before you install the OS patches, the DVD-ROM drive of the server will be unavailable. Copy the software package **Solaris10_huawei_patch_9.0.1.tar.gz** from the DVD U2000***version***_server_patch_solaris_SPARC_dvd3 to a computer. Then, FTP the software package to the **/opt/patches/sun** path of the server in binary mode.

  The installation software package must be uploaded to the **/opt** path of the server in binary mode through FTP. Run the **tar xvf** *name_of_installation_software_package* command to decompress the installation package.

- The system allows user **root** to log in remotely and use the FTP tool.

Procedure

1 Log in to the OS through the serial port as user **root**.

2 Ensure that the disk partitioning of the system is correct.

1. Run the following command to check the disk partitioning of the system:

   ```
   # format
   ```

   Partitioned disks and their serial numbers will be displayed.

2. Enter the serial number of a disk to be checked, such as 0, and press **Enter**. The format menu will be displayed.
3. Run the **partition** command and press **Enter**. The partition menu will be displayed.
4. Run the **print** command and press **Enter**. The disk partitioning information will be displayed.

   According to the displayed disk partitioning information, check whether the current disk partitioning of the system is consistent with the disk partition plan. If they are inconsistent, reinstall the OS and then partition disks according to the disk partition plan.

   A message similar to the following will be displayed:

   ```
   Part      Tag    Flag     Cylinders         Size            Blocks
     0       root    wm       0 -  8243       80.00GB    (8244/0/0)  167781888
     1       swap    wu    8244 -  9892       16.00GB    (1649/0/0)   33560448
     2     backup    wm       0 - 14086      136.71GB    (14087/0/0) 286698624
     3 unassigned    wu       0                 0         (0/0/0)             0
     4 unassigned    wu       0                 0         (0/0/0)             0
     5 unassigned    wu       0                 0         (0/0/0)             0
     6        usr    wm    9893 - 11953       20.00GB    (2061/0/0)   41945472
     7        var    wm   11954 - 14014       20.00GB    (2061/0/0)   41945472
   ```

NOTE

The **Part** column lists fragments. The **Tag** column lists the partitions. The **Size** column lists the partition sizes.

5. Run the **quit** command and press **Enter** to exit the partition menu.
6. Run the **quit** command and press **Enter** to exit the format menu.

3 Run the following commands to display the **OK** prompt:

```
# sync;sync;sync;sync;
# init 0
```

NOTE

About 5 to 10 minutes later, the **OK** prompt will be displayed.

4 Run the following commands to enter the single-user mode:

```
ok>  boot -s
```

NOTE

About 5 to 10 minutes later, the **>** prompt will be displayed, indicating the single-use mode.

5 Run the following commands to mount on the file system:

```
# mountall > /dev/null 2>&1
```

6 Run the following commands to decompress the **Solaris10_huawei_patch_9.0.1.tar.gz** file:

```
# cd /opt/patches/sun
# gzcat Solaris10_huawei_patch_9.0.1.tar.gz | tar xvf -
```

7 Run the following commands to switch to the path where the **QuickSetup.sh** file is stored and then run the **QuickSetup.sh** file:

```
# cd /opt/patches/sun/sun
# sh QuickSetup.sh
```

8 The system will start installing patches. The entire installation process takes about 40 minutes.

The patch installation is complete if the following message is displayed:

```
Success! <install_all_patches> OK!
************************************************************************
Setting system parameters
************************************************************************
************************************************************************
Restart the operation system
************************************************************************
Are you sure to restart the operation system right now?<y/n>
```

Enter **y** and press **Enter**.

9 After the system restarts, log in to the OS as user **root**.

----End

Follow-up Procedure

1. Run the following command to view the patch version of the system:

   ```
   # uname -rv
   ```

   Information similar to **5.10 Generic_141414-07** is displayed. Here, **5.10 Generic_141414-07** indicates the patch version of the Solaris 10(10/08) OS.

   If the patch version is **5.10 Generic_141414-07**, it indicates that the OS patches are successfully installed. Otherwise, you must reinstall OS patches.

2. Run the following command to verify that the system character set is correct:

   ```
   # locale -a
   ```

   If the following message is displayed, the character set of Solaris OS is correct. Otherwise, reinstall the OS.

   ```
   C
   en_US.UTF-8
   ```

3. If the OceanStor S2600 disk array is used, ensure that the **expect** plug-in was installed on the server before configuring the disk array.

   (1) Log in to the server OS as user **root**.

   (2) Run the following command to verify that the **expect** plug-in has been installed:

   ```
   # which expect
   ```

   (3)
   - If the **expect** plug-in installation path is displayed, the **expect** plug-in has been installed and you do not need to run the **autoinstall.sh** script.

     The following is an example path:

     ```
     /usr/bin/expect
     ```

   - If the **expect** plug-in installation path is not displayed, run the **autoinstall.sh** script to install the **expect** plug-in.

     a. Run the following commands to go to the installation path of the Solaris patch and decompress the **expect.tar.gz** file:

     ```
     # cd /opt/patches/expect
     # gzcat expect.tar.gz | tar xvf -
     ```

     b. Run the following commands to install the **expect** plug-in:

     ```
     # ./autoinstall.sh
     ```

4. If the patches are successfully installed, perform the following operations to delete the patch package to free up disk space:

   (1) Run the following commands to delete the OS patch package:

   ```
   # cd /opt
   # rm U2000V100R002C01_server_ospatch_solaris_SPARC.tar
   ```

   (2) Run the following command to delete the OS patch path:

   ```
   # rm -rf /opt/patches
   ```

G Planning Disk Partitions

This topic describes the disk partitioning scheme that is determined according to the sizes and quantities of the server hard disks.

Specify the disk partitioning plan before manually installing the OS. This part can be skipped if the OS is installed with the quick installation DVD because the installation software automatically partitions disks according to the disk size.

CAUTION

- The second slice represents the total capacity of the hard disk. Do not change it during the partitioning process. Otherwise, the OS may not function properly.
- Partition 3 and partition 4 are reserved for disk mirroring. During the partitioning process, do not enter the name or size of the partition.
- The following table lists only the slices for partitioning. In the case of the slices that do not need to be partitioned, you do not need to enter the associated name or size during the partitioning process. For example, in the case of 2 x 73 GB disks, do not enter partition names **/usr** and **/var** in the partitioning process.

- The following section provides example disk partitioning schemes for the primary and secondary sites.
  - If a server is equipped with two hard disks, the first hard disk must be partitioned regardless of whether a disk array is connected. The second hard disk does not require partitioning because it serves as a mirror disk for the first hard disk. **Table G-1** and **Table G-2** show the partitioning scheme for the first hard disk of a two-disk server.

Table G-1 Partitioning scheme for a two-disk server without any disk array

Hard Disk	Fragment	Partition	2 x 300 GB Hard Disk (MB)	2 x 146 GB Hard Disk (MB)	2 x 73 GB Hard Disk (MB)
First hard disk	0	/	20000	12000	15000
	1	swap	16000	8000	6000

Hard Disk	Fragment	Partition	2 x 300 GB Hard Disk (MB)	2 x 146 GB Hard Disk (MB)	2 x 73 GB Hard Disk (MB)
	5	/opt	120000	65000	29000
	6	/var	20000	8000	The **/var** partition is not required.
	7	/export/ home	1000	1000	The **/export/ home** partition is not required.

Table G-2 Partitioning scheme for a two-disk server with a disk array

Hard Disk	Fragment	Partition	2 x 300 GB Hard Disk (MB)	2 x 146 GB Hard Disk (MB)	2 x 73 GB Hard Disk (MB)
First hard disk	0	/	30000	30000	15000
	1	swap	16000	16000	16000
	5	/opt	172000	30000	20000
	6	/var	30000	30000	15000
	7	/export/ home	30000	29000	1000

- If a server is equipped with four hard disks and is not connected to any disk array, only the first hard disk needs to be partitioned. The third and fourth hard disks do not require partitioning because they serve as mirror disks for the first and second hard disks. **Table G-3** shows the partitioning scheme for the first hard disk of a four-disk server when the server is not connected to any disk array.

Table G-3 Partitioning scheme for a four-disk server without any disk array

Hard Disk	Fragment	Partition	4 x 300 GB Hard Disk (MB)	4 x 146 GB Hard Disk (MB)	4 x 73 GB Hard Disk (MB)
First hard disk	0	/	50000	12000	15000
	1	swap	16000	8000	6000
	5	/opt	152000	104000	46000
	6	/var	50000	10000	The **/var** partition is not required.

Hard Disk	Fragment	Partition	4 x 300 GB Hard Disk (MB)	4 x 146 GB Hard Disk (MB)	4 x 73 GB Hard Disk (MB)
	7	/export/home	10000	1000	The **/export/home** partition is not required.

If a server is equipped with four hard disks and is connected to a disk array, the first and second hard disks need to be partitioned. The third and fourth hard disks do not require partitioning because they serve as mirror disks for the first and second hard disks. **Table G-4** shows the partitioning scheme for the first and second hard disks of a four-disk server when the server is connected to a disk array.

Table G-4 Partitioning scheme for a four-disk server with a disk array

Hard Disk	Fragment	Partition	4 x 300 GB Hard Disk (MB)	4 x 146 GB Hard Disk (MB)	4 x 73 GB Hard Disk (MB)
First hard disk	0	/	132000	50000	20000
	1	swap	16000	16000	16000
	6	/var	100000	40000	20000
	7	/export/home	30000	29000	11000
Second hard disk	5	/opt	278000	135000	67000

- If a server is equipped with six hard disks and is not connected to any disk array, only the first and second hard disks need to be partitioned. The fourth, fifth, and sixth hard disks do not require partitioning because they serve as mirror disks for the first, second, and third hard disks. **Table G-5** shows the partitioning scheme for the first and second hard disks of a six-disk server when the server is not connected to any disk array.

Table G-5 Partitioning scheme for a six-disk server without any disk array

Hard Disk	Fragment	Partition	6 x 300 GB Hard Disk (MB)	6 x 146 GB Hard Disk (MB)	6 x 73 GB Hard Disk (MB)
First hard disk	0	/	50000	20000	12000
	1	swap	16000	16000	16000

Hard Disk	Fragment	Partition	6 x 300 GB Hard Disk (MB)	6 x 146 GB Hard Disk (MB)	6 x 73 GB Hard Disk (MB)
	5	/opt/backup	142000	77000	18000
	6	/var	50000	20000	20000
	7	/export/home	20000	2000	1000
Second hard disk	5	/opt	278000	135000	67000

If a server is equipped with six hard disks and is connected to a disk array, the first, second, and third hard disks need to be partitioned. The fourth, fifth, and sixth hard disks do not require partitioning because they serve as mirror disks for the first, second, and third hard disks. **Table G-6** shows the partitioning scheme for the first, second, and third hard disks of a six-disk server when the server is connected to a disk array.

Table G-6 Partitioning scheme for a six-disk server with a disk array

Hard Disk	Fragment	Partition	6 x 300 GB Hard Disk (MB)	6 x 146 GB Hard Disk (MB)	6 x 73 GB Hard Disk (MB)
First hard disk	0	/	162000	79000	21000
	1	swap	16000	16000	16000
	6	/var	100000	40000	30000
Second hard disk	5	/opt	278000	135000	67000
Third hard disk	7	/export/home	278000	135000	67000

H Configuring Disk Arrays

This topic describes how to configure the OceanStor S3100, OceanStor S2600, and StorageTek 2540 disk arrays.

H.1 Configuring the OceanStor S2600 Disk Array by Using the ISM

This topic describes how to configure the OceanStor S2600 disk array using the ISM.

Prerequisite

- The IP addresses for both controllers of the OceanStor S2600 disk array are configured.
- The primary and secondary power supplies of the disk array have been powered on. For more information, see **5 Powering On a Server**.
- The Window management terminal must communicate properly with the disk array controller.
- Users are logged in to the ISM from the Windows management terminal by using the Internet Explorer 6.0, Internet Explorer 7.0, or Internet Explorer 8.0.

Context

NOTE

The ISM software will lock up if an operation is not performed within 10 minutes after login. Enter the password again to log in if lock up occurs.

You need to respectively configure the disk arrays on the primary site and secondary site. The following takes the configuration of the disk array on the primary site as an example.

The following table shows the configuration requirements on the OceanStor S2600 disk array.

CAUTION

The following requirements are for the OceanStor S2600 (6 x 300 GB) disk arrays only. A OceanStor S2600 disk array (6 x 300 GB) is equipped with six hard disks, each of which is 300 GB in size. If the selected disk arrays are not the OceanStor S2600 disk arrays (6 x 300 GB), contact Huawei engineers for details about how to configure the disk arrays.

Configure Item	Settings
Hot-spare disk	The sixth disk is designated as the global hot-spare disk.
Host group and host	Set the host group name to **HostGroup001**. Set the host name to **.** For the primary site, the host name is set to **Primaster**; for the secondary site, the host name is set to **Secmaster**.
RAID group	● Set the RAID group name to **RAID001**. ● Set the RAID Level to **RAID5**. ● Set the disk type to **SAS**. ● The first five disks serve as the RAID group.

Configure Item	Settings
LUN	Configure one LUN as follows: ● LUN information – Name: LUN001 – Capacity: 1000 GB – Stripe unit size: 32 KB – Home controller: controller A ● Cache strategy – Prefetch strategy: intelligent – Write strategy: write back (mirroring) ● Mapping mode Mapping object: host group name **HostGroup001**
Port	● Set the type to **FC**. ● Set the name associated with the first identifier to **port1**. ● Set the name associated with the second identifier to **port2**.

Procedure

1 Log in to the ISM.

1. Open the Internet Explorer on the Windows management terminal.
2. Enter **http://XXX.XXX.XXX.XXX** in the address bar of the Internet Explorer (where XXX.XXX.XXX.XXX indicates the IP address of the management network port of the storage array controller). Such as *http://129.9.1.10*.

   NOTE

   If "The page cannot be displayed" is displayed on the Internet Explorer, the Windows management terminal and the disk array controller fail to communicate with each other. Check the network connection.

   The system will navigate to the default login window of the ISM, as shown in the following figure.

3. Click **Click Here to Launch OceanStor ISM**. The system will check whether the ISM is installed on the Windows management terminal.

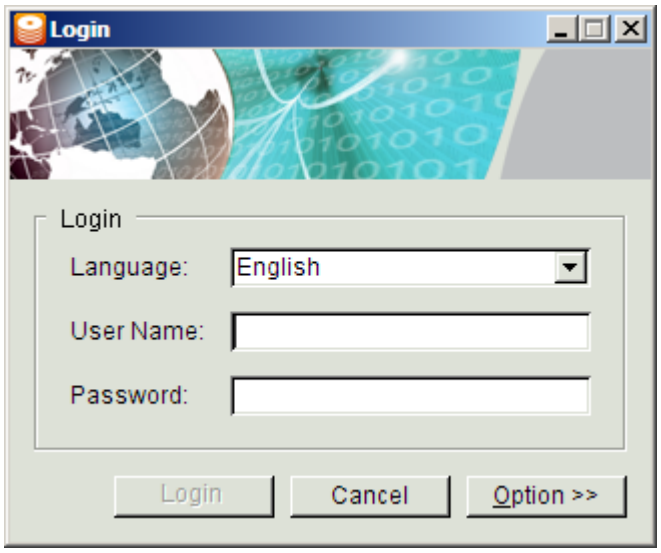
CAUTION

- Before installing the ISM, install the Java runtime environment (JRE). The JRE version must be 1.5.0 or later (excluding version 1.5.0.16). In the CLI, run the **java -version** command to view the JRE version. If the JRE is not installed, click **Please Setup JRE**.
- Do not use JRE 1.5.0.16. Downloading the ISM may fail due to the bugs in JRE 1.5.0.16.

If the ISM is not installed on the Windows management terminal, the system will automatically download and install the ISM by means of the Java web start (JWS). If the ISM is installed on the Windows management terminal, the system will automatically check the software version. If the version of the ISM is not the latest version, the system will automatically upgrade the software to the latest version.

4. In the **Warning - Security** dialog box, select **Always trust content from this publisher** and click **Run**.
5. Decide whether or not to create an ISM shortcut on the desktop and in the Start menu.

The system will open the login window of the ISM, as shown in the following figure.



6. Select the required language from the **Language** drop-down list. Then, enter the user name in **User Name** and the user password in **Password**.

   NOTE

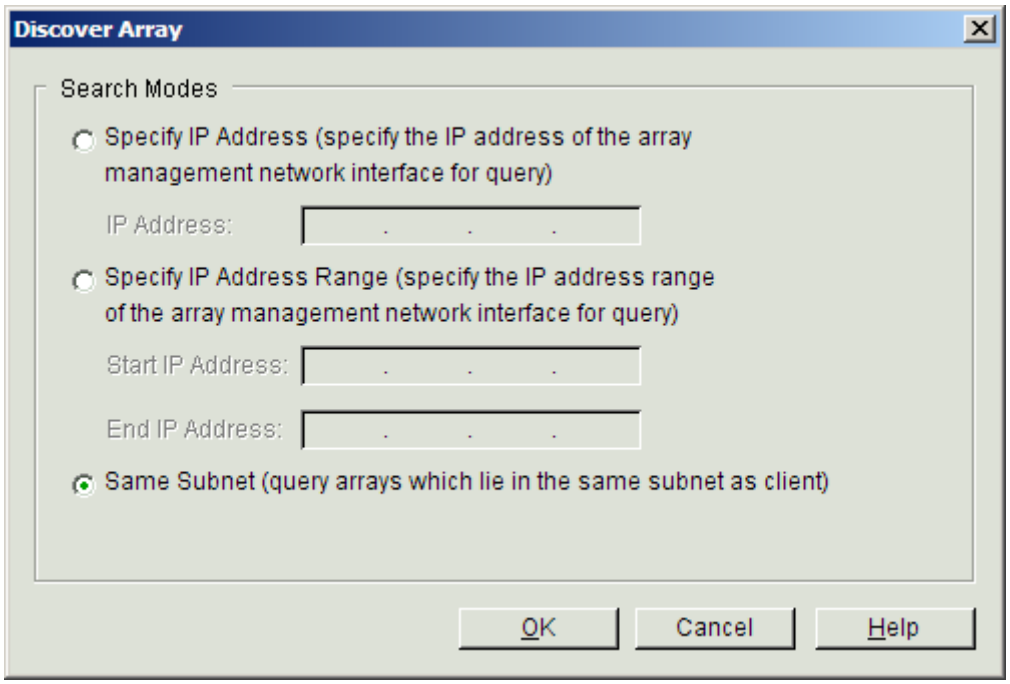
   - A disk array can be discovered only when the entered user name and password are the same as those of the disk array.
   - The default user name and password for logging in to the ISM are **admin** and **123456**. After login, change the password immediately and keep the password confidential.

7. Click **Login** to access the Welcome window, as shown in the following figure:

2 Discover disk arrays.

1. In the Welcome window of the ISM, click **Discover array**.

   The **Discover array** dialog box will be displayed, as shown in the following figure.



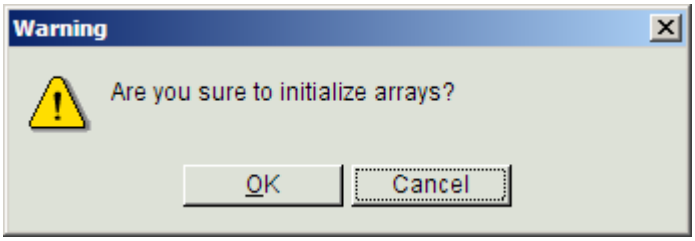
2. Select a mode for discovering disk arrays according to the conditions at your site. **Table H-1** describes the parameters for discovering disk arrays.

Table H-1 Parameters for discovering disk arrays

Parameter	Description
Specify IP Address	Indicates that disk arrays are discovered according to the IP address of the management network port on the specified disk array. When you specify the IP address, the first field on the left ranges from 1 to 223 (except 127), the last field ranges from 1 to 254, and the other fields range from 0 to 255.
Specify IP Address Range	Indicates that disk arrays are discovered according to the IP address segment of the management network port on the specified disk array. **Start IP Address** and **End IP Address** indicate the start IP address and end IP address of disk arrays to be discovered. When setting this parameter, pay attention to the following points: ● The discovery range is the IP subnet segment of the ISM client. ● The first field on the left ranges from 1 to 223 (except 127), the last field ranges from 1 to 254, and the other fields range from 0 to 255. ● The start IP address must be smaller than or equal to the end IP address.
Same Subnet	Indicates that the discovery range is the IP subnet segment of the ISM client. This mode is the default discovery mode of the system.

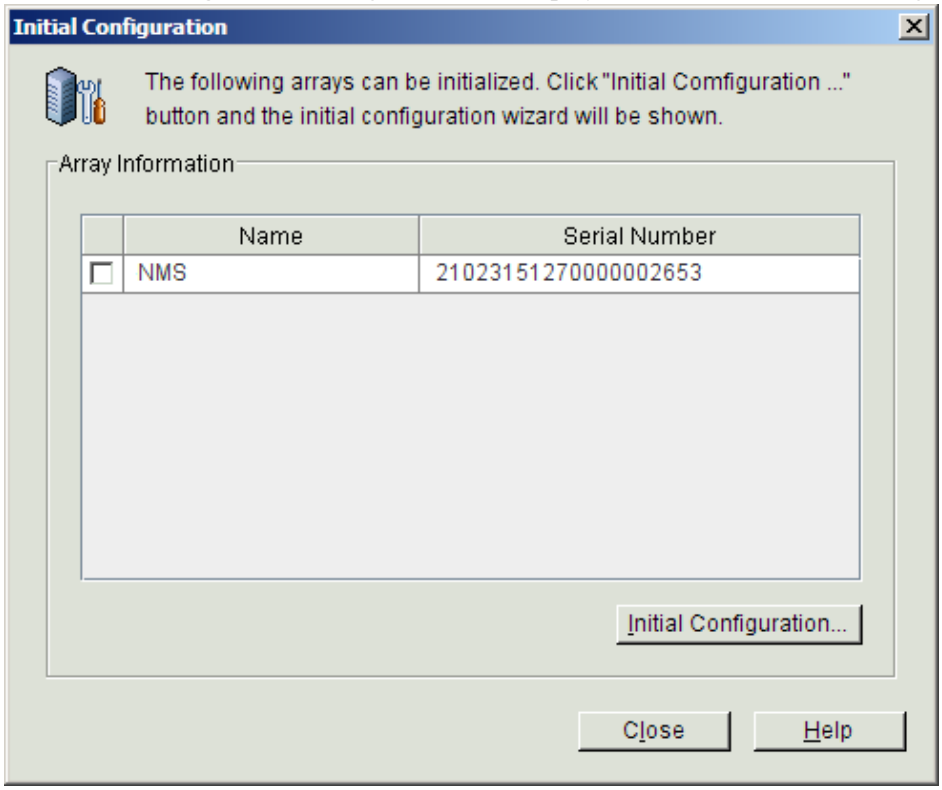
3. Click **OK**. After disk arrays are discovered, the **Info** dialog box will be displayed, prompting an operation success.

4. Click **OK**. The **Warning** dialog box will be displayed.

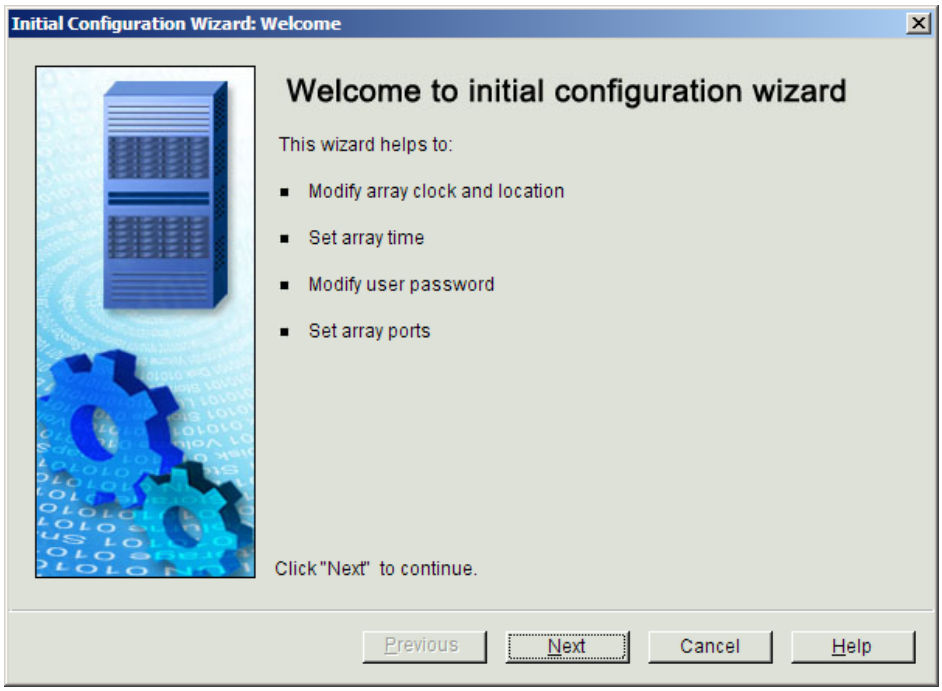


3 Initialize the configuration.

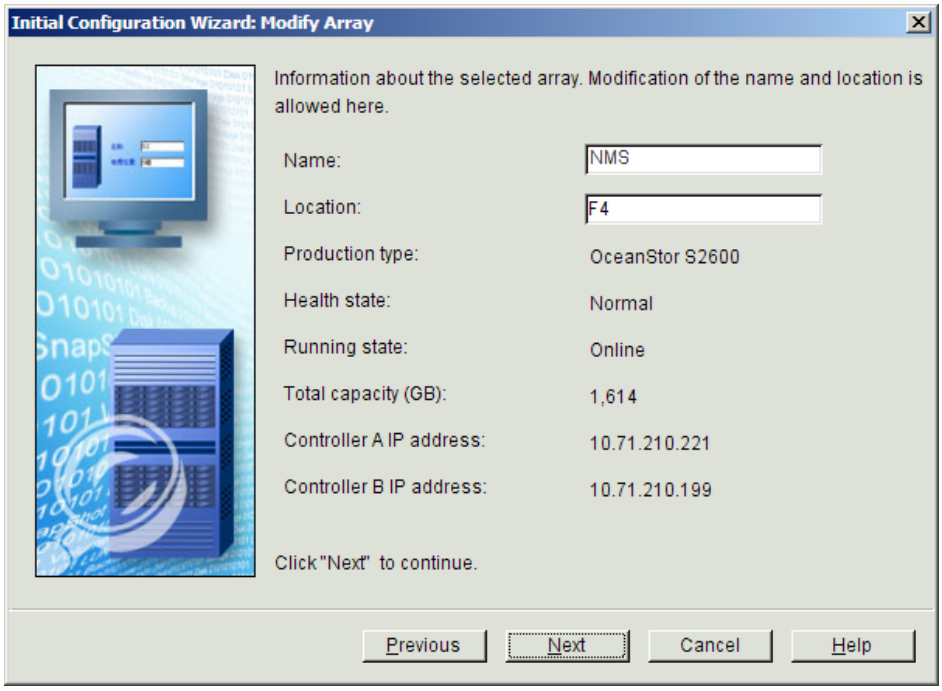
1. In the **Warning** dialog box, click **OK** to initialize the disk array.
   The **Initial Configuration** dialog box will be displayed, as shown in the following figure.



2. Select the disk array to be configured and click **Initial Configuration**. The **Initial Configuration Wizard: Welcome** dialog box will be displayed.



3. Click **Next**. The **Initial Configuration Wizard: Modify Array** dialog box will be displayed.

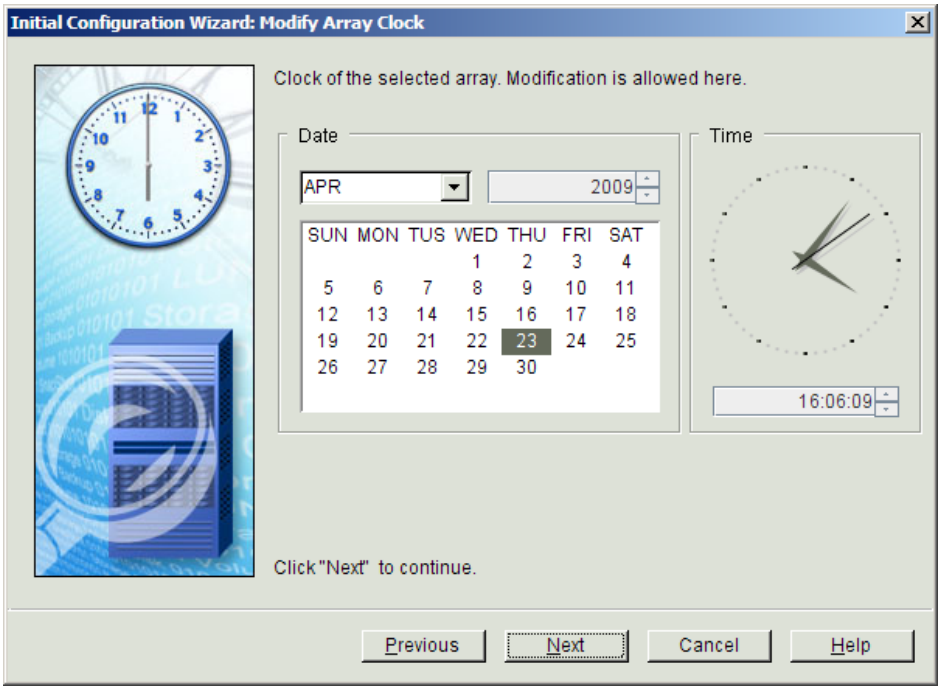


4. Enter the name of the disk array in the **Name** text box and the location information in the **Location** text box. **Table H-2** describes the parameters for modifying a disk array.

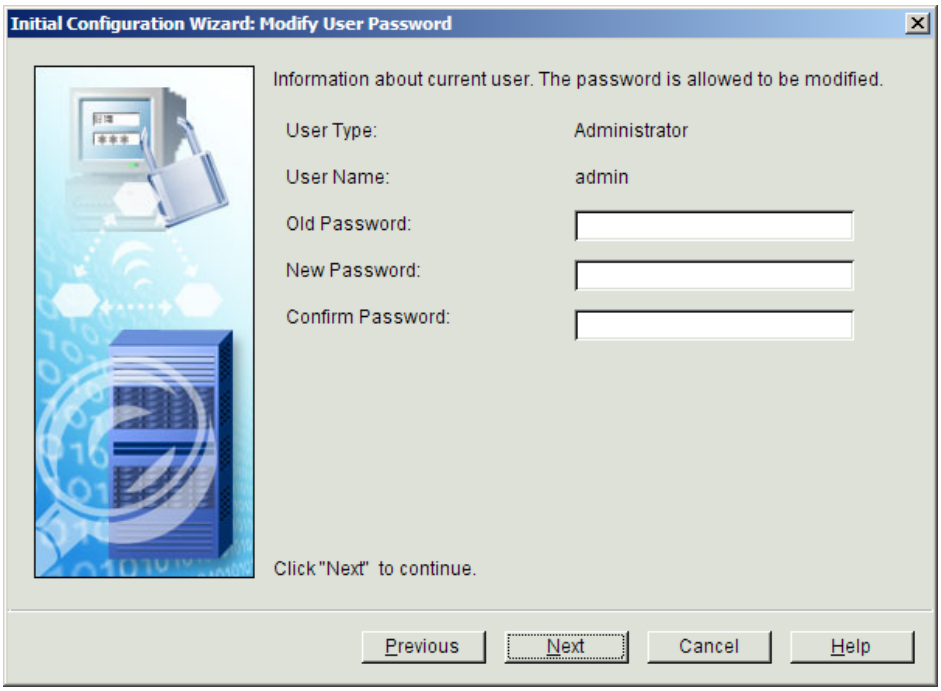
Table H-2 Parameters for modifying a disk array

Parameter	Description
Name	Specifies the name of the OceanStor S2600 disk array to be configured. When setting this parameter, note that: ● This parameter contains only the characters and numerals in DBC case, underscores (_), en-dash symbols (-), and simplified Chinese characters. ● This parameter consists of 1 to 32 characters. A Chinese character counts for two DBC characters.
Location	Specifies the location of the OceanStor S2600 disk array to be configured. When setting this parameter, note that: ● This parameter contains only the characters and numerals in DBC case, underscores (_), en-dash symbols (-), and simplified Chinese characters. ● This parameter consists of 1 to 32 characters. A Chinese character counts for two DBC characters.

5. Click **Next**. The **Initial Configuration Wizard: Modify Array Clock** dialog box will be displayed.



6. Select the required date and time, and then click **Next**. The **Initial Configuration Wizard: Modify User Password** dialog box will be displayed.



7. Change the login password of the user. **Table H-3** describes the parameters for changing the user password.

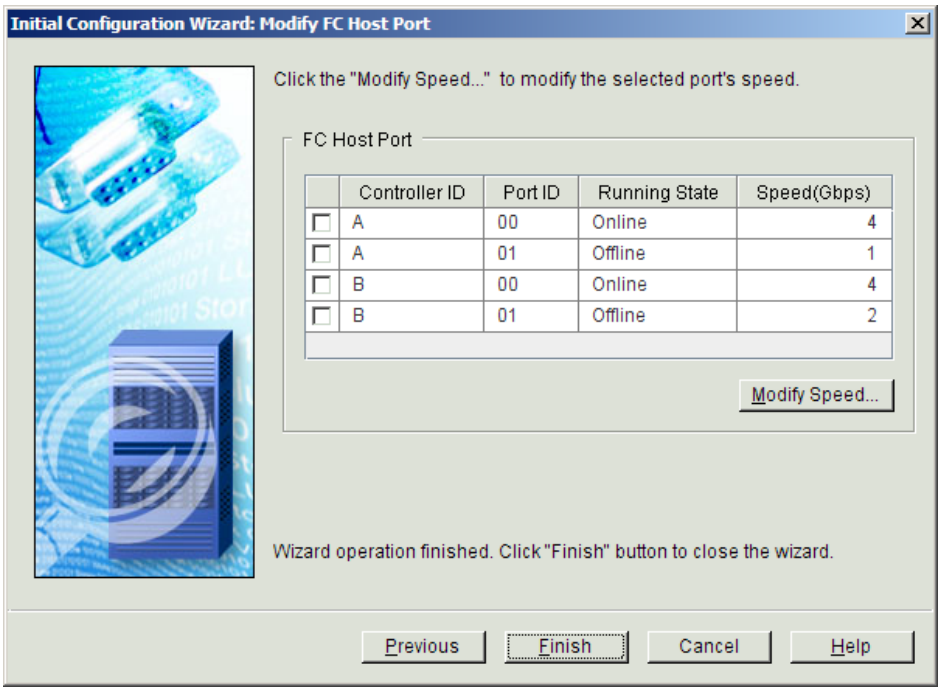
Table H-3 Parameters for changing the user password

Parameter	Description
Old Password	Specifies the original password. The default password is **123456**.
New Password	Specifies the new password. It ranges from 6 to 16 characters.
Confirm Password	Confirms the new password. When setting this parameter, pay attention to the following points: ● This parameter ranges from 6 to 16 characters. ● This parameter value must be the same as the value of **New Password**.

8. Click **Next**. The **Initial Configuration Wizard: Modify FC Host Port** dialog box will be displayed.

NOTE

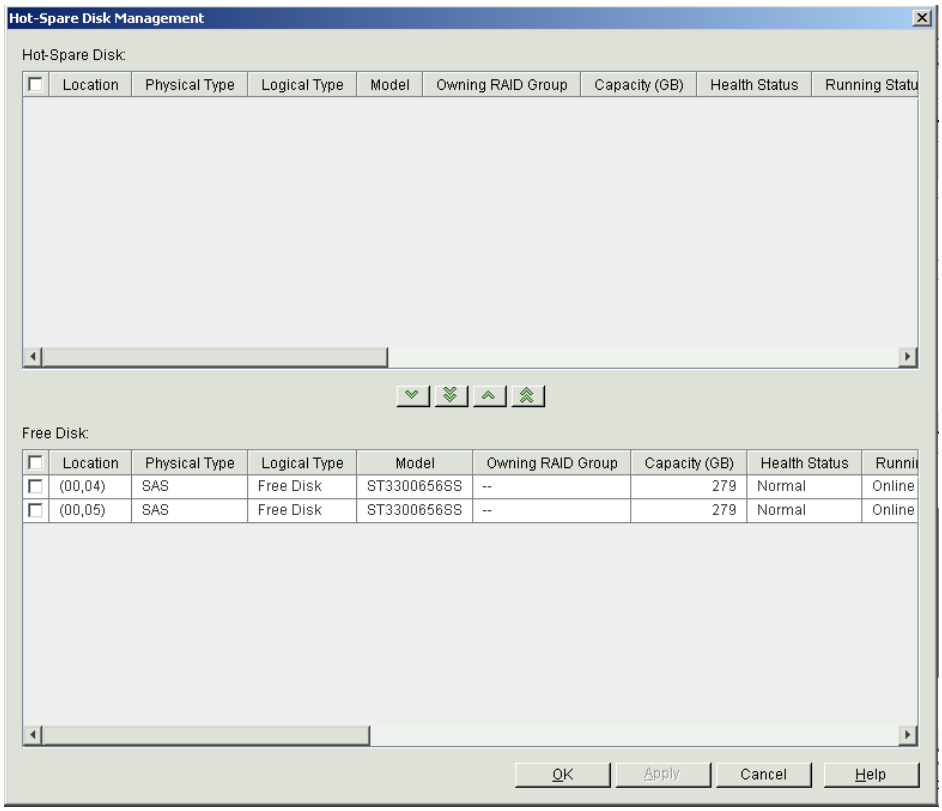
Click **Modify Speed** if the port rate needs to be changed. The default rate of an online port is 4 Gbit/s.



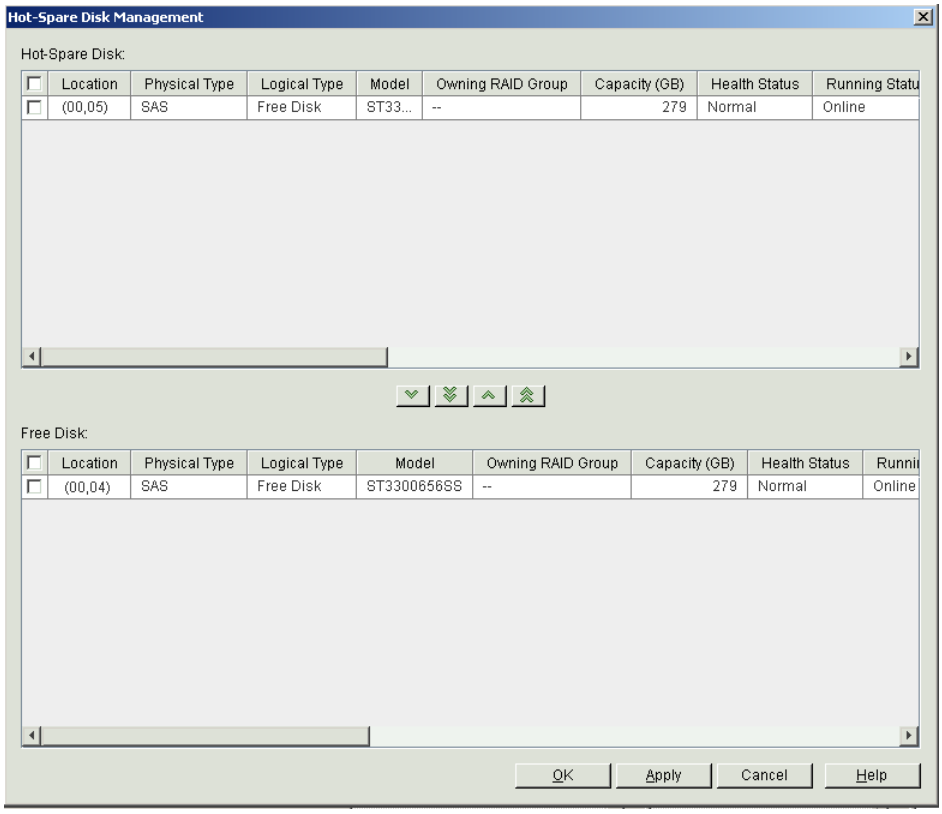
9. Click **Finish** to complete the initial configuration.
10. Click **Close** to exit.

4 Configure the hot-spare disk.

1. Click the **Physical View** tab in the navigation tree, and then select the OceanStor S2600 disk array to be configured.
2. Choose **Configuration** > **Hot-Spare Disk Management** from the main menu. The **Hot-Spare Disk Management** dialog box will be displayed.



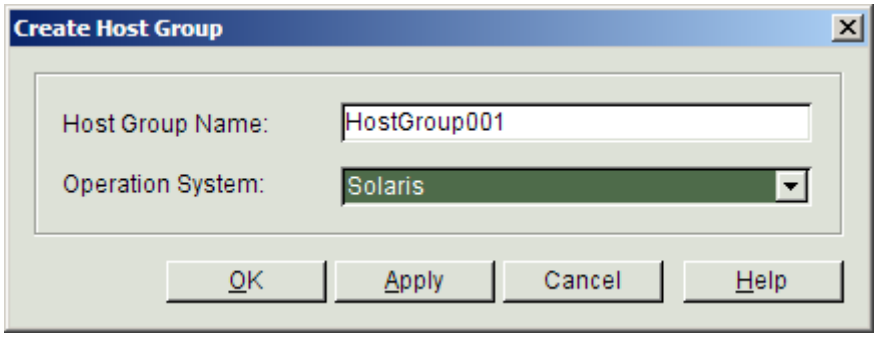
3. Select disk location **(00,05)** from the free disk list and click the third button () in the middle portion of the dialog box to add the selected disk to the hot spare disk list.



4. Click **OK** to close the **Hot-Spare Disk Management** dialog box. Click **OK** in the **Warning** dialog box. Then, click **OK** in the **Info** dialog box.

5 Create a host group and host.

1. Choose **Logical View** from the navigation tree and select the OceanStor S2600 disk array to be configured.
2. Choose **Configuration** > **Create Host Group** from the main menu. The **Create Host Group** dialog box will be displayed.



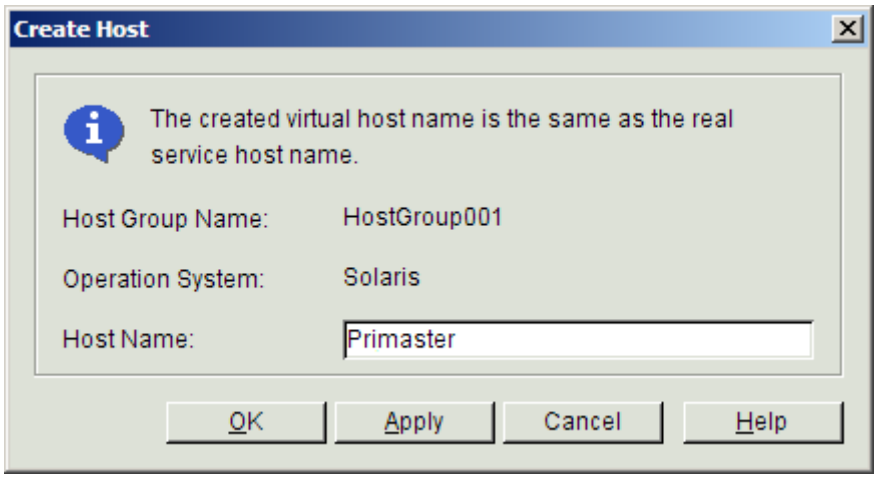
3. Select **Solaris**, and then click **OK**.

   The **Info** dialog box is displayed indicating that the operation was completed.

   NOTE

   In this step, the selected OS corresponds to the OS of the server connected to the disk array.

4. Click **OK** to complete creating the host group.
5. Choose the host group from the navigation tree, and then choose **Configuration** > **Create Host** from the main menu. The **Create Host** dialog box will be displayed.



6. Enter the host name and click **OK** to continue.

   TIP

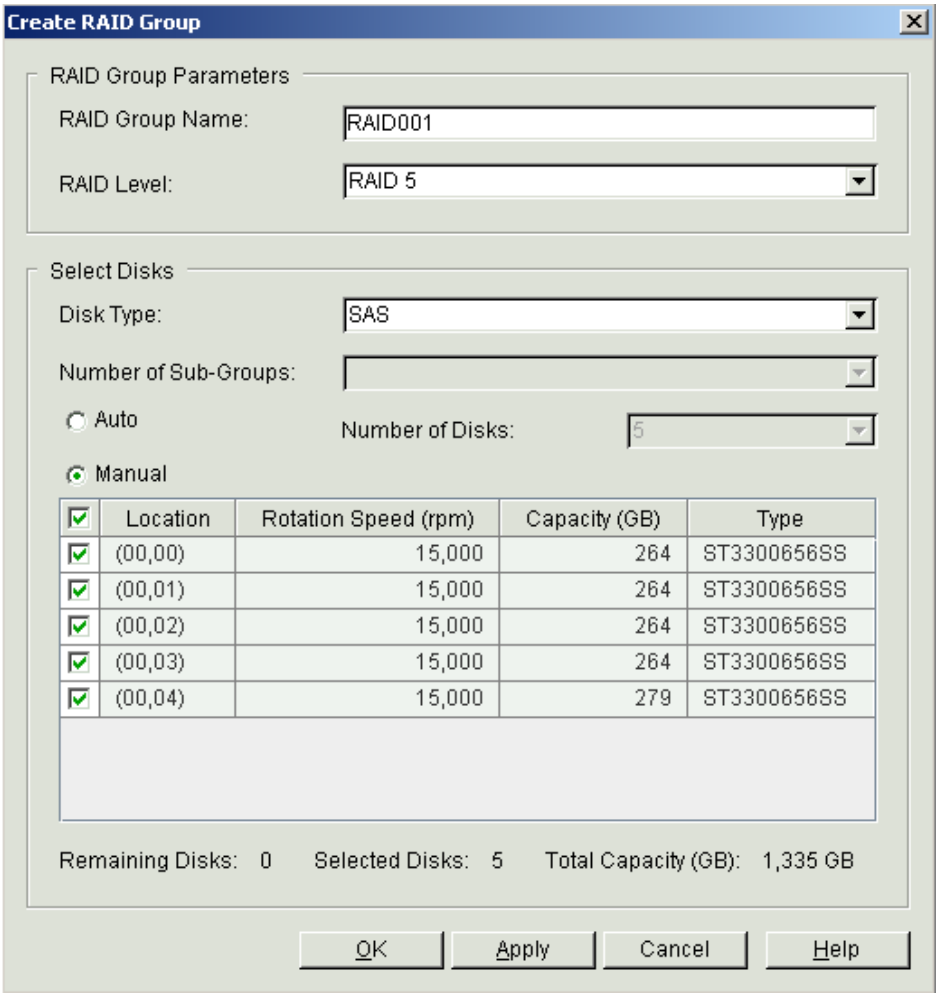
   It is recommended to enter the host name of the server connected to the disk array so that the host name is easy to remember.

   The **Info** dialog box will be displayed indicating that the operation was completed.
7. Click **OK** to complete creating the host.

6 Create a RAID group.

1. Choose **Logical View** from the navigation tree and select the OceanStor S2600 disk array to be configured.

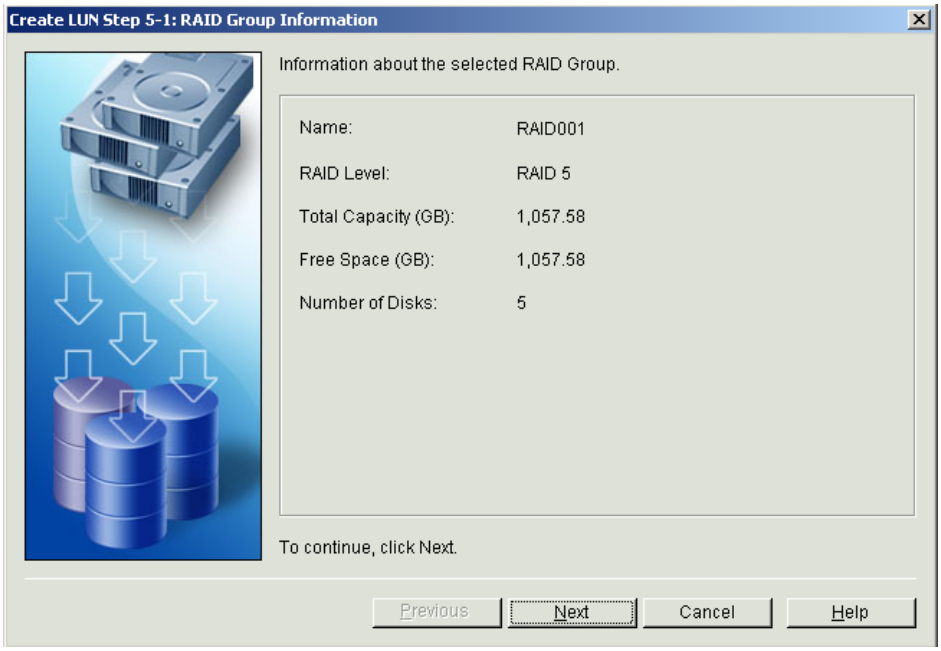
2. Choose **Configuration** > **Create RAID Group** from the main menu. In the **Create RAID Group** dialog box, modify the settings, as shown in the following figure.



3. Click **OK**. The **Info** dialog box will be displayed indicating that the operation was completed.
4. Click **OK**. Creation of the RAID group is completed.

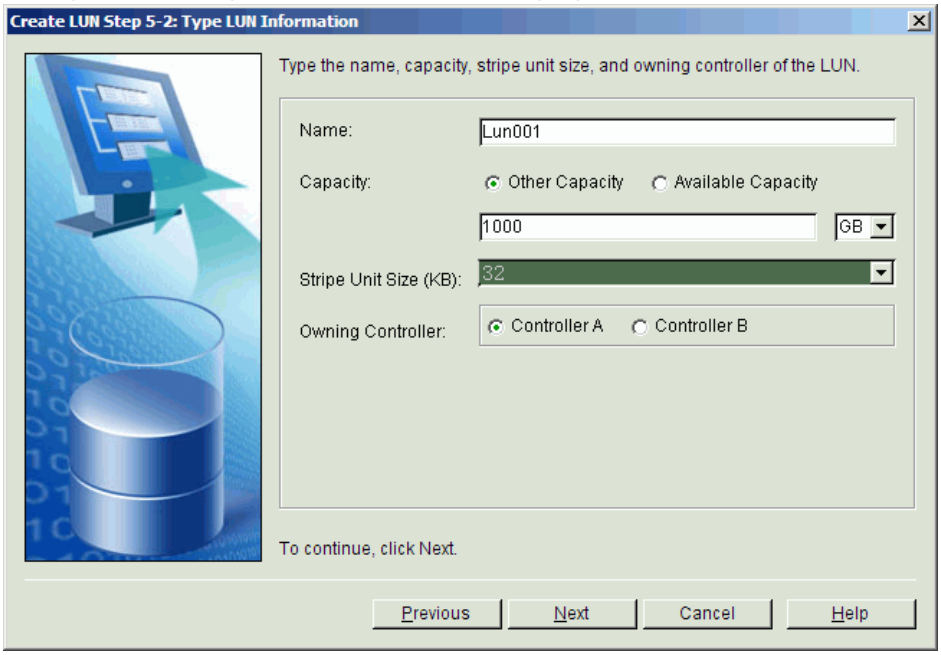
7 Create Lun001.

1. Click the **Logical View** tab in the navigation tree and select the RAID group where the new Lun001 locates.
2. Choose **Configuration** > **Create LUN** from the main menu. The **Create LUN Step 5-1: RAID Group Information** dialog box will be displayed.



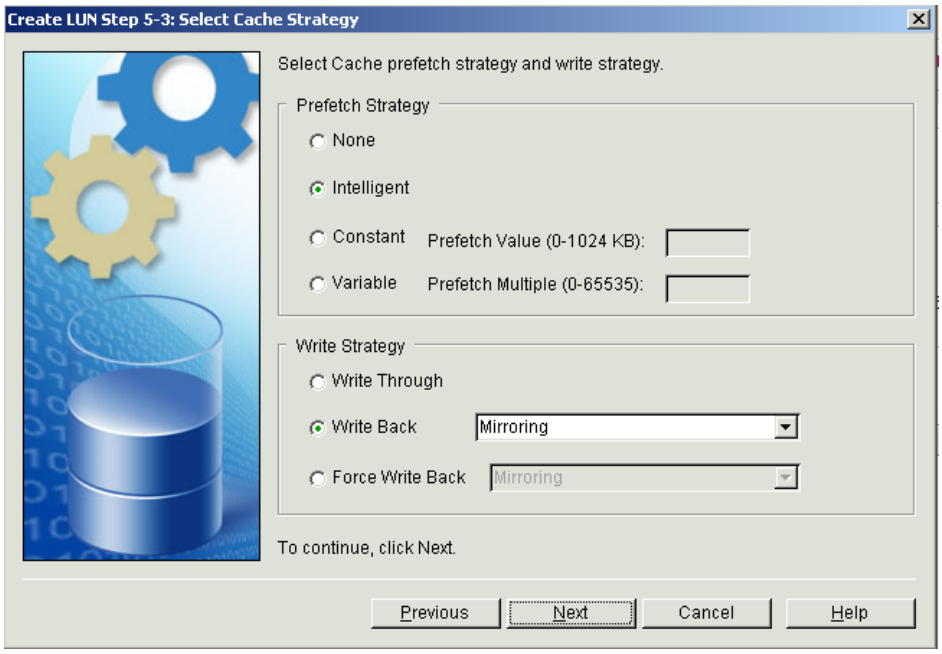
3. Click **Next**. The **Create LUN Step 5-2: Type LUN Information** dialog box will be displayed.

   Configure the settings as shown in the following figure.



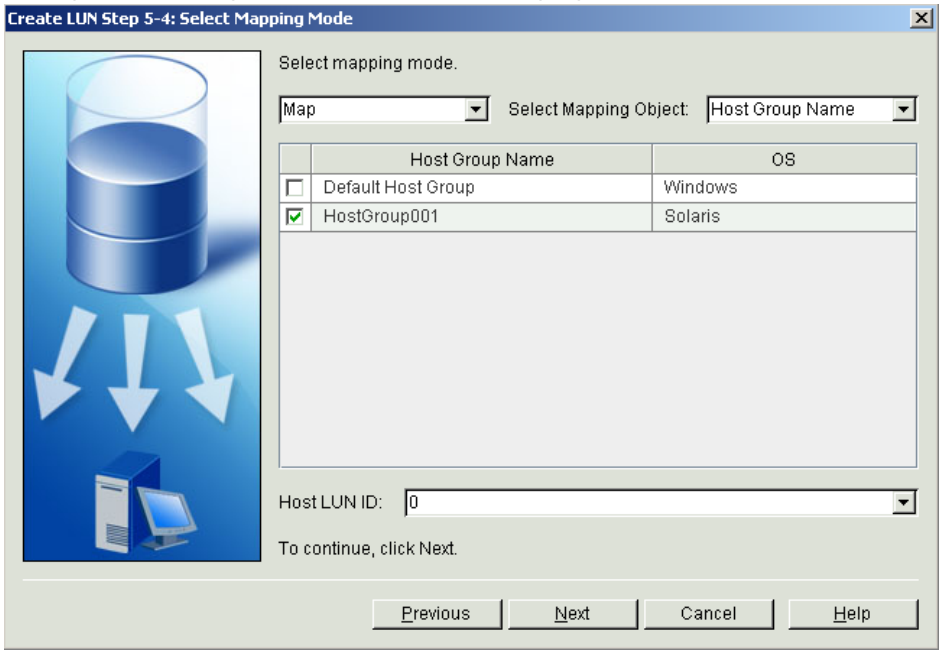
4. Click **Next**. The **Create LUN Step 5-3: Select Cache Strategy** dialog box will be displayed.

   Configure the settings as shown in the following figure.



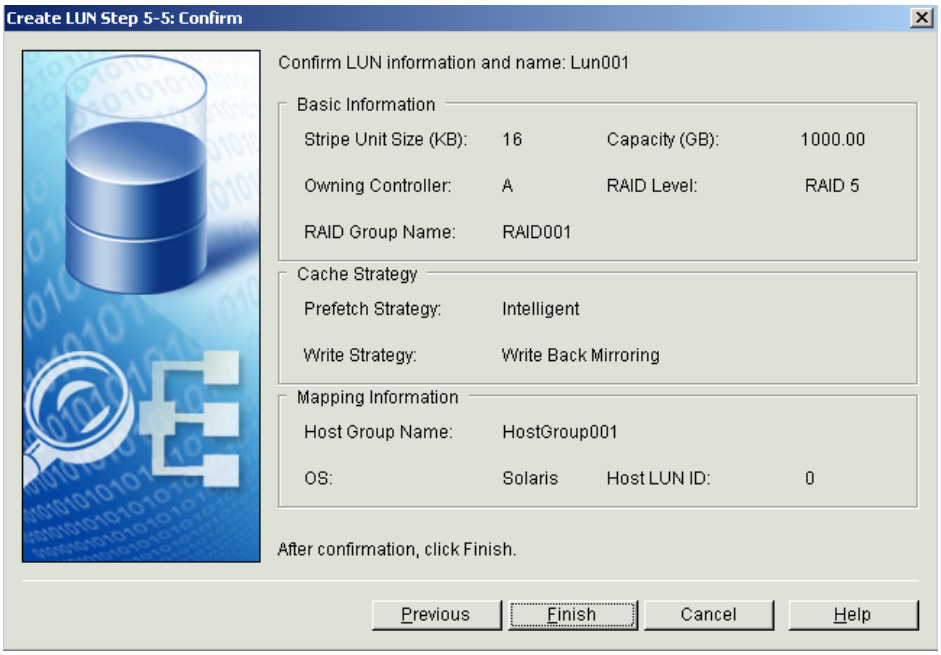
5. Click **Next**. The **Create LUN Step 5-4: Select Mapping Mode** dialog box will be displayed.

   Configure the settings as shown in the following figure.



6. Click **Next**. The **Create LUN Step 5-5: Confirm** dialog box will be displayed.

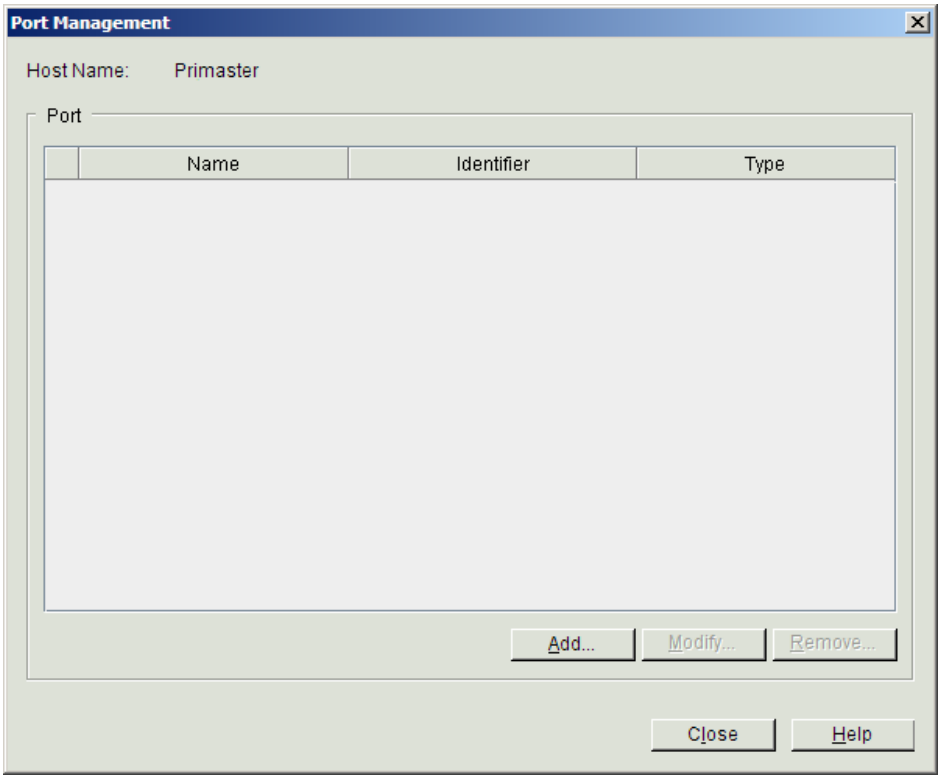
   Configure the settings as shown in the following figure.



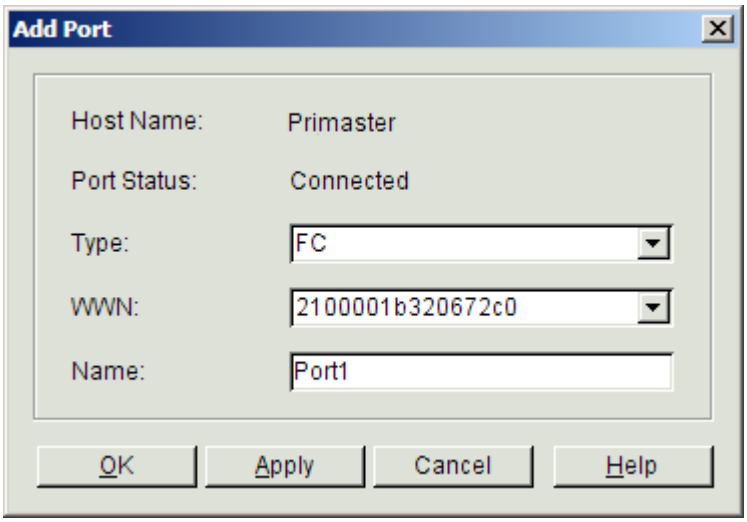
7. Click **Finish**. The **Info** dialog box will be displayed indicating that the operation was completed.
8. Click **OK**. Creation of Lun001 is complete.

8 Add a port.

1. Choose **Host** from the navigation tree, and then choose **Configuration** > **Host Port Management** from the main menu. The **Port Management** dialog box will be displayed.



2. Click **Add**. The **Add Port** dialog box will be displayed.



3. Select the first available option from the **WWN** drop-down list, enter **port1** in **Name**, and then click **Apply**. In the dialog box that will be displayed, click **OK**.
4. Click **Add** again. The **Add Port** dialog box will be displayed.
5. Enter **port2** in the **Name** text box, and click **OK**. In the dialog box that will be displayed, click **OK**.

9 Check the connection of the fiber card.

1. Log in to the server OS as user **root**.
2. Run the following command to check the connection status of the port on the fiber card:
   ```
   # luxadm -e port
   ```

   NOTE

   In the preceding command, *port ID* indicates the ports through which the disk array connects to the server.

   You can run the **lssci** command to query port IDs. the first column in the returned message displays the port IDs of the fiber card. For example, run the following command:

   The following message will be displayed:

   ```
   [0:0:0:0]    disk    IBM-ESXS  CBRBA146C3ETSO  N   C49B  -
   [0:0:1:0]    disk    IBM-ESXS  CBRBA146C3ETSO  N   C49B  -
   [0:1:0:0]    disk    LSTLOGIC  Logical Volume      3000  /dev/sda
   [3:0:0:0]    disk    HUAWEI    S2600               1     /dev/sdb
   [4:0:0:0]    disk    HUAWEI    S2600               1     /dev/sdc
   ```

   Find the last two lines containing **S2600** in the fourth column. Information in the first columns (**[3:0:0:0]** and **[4:0:0:0]**) indicates that the S2600 disk array connects to the server through port 3 and port 4.

   The following message will be displayed:

   ```
   /devices/pci@0,600000/pci@0/pci@8/pci@0,1/SUNW,qlc@1/fp@0,0:devctl  CONNECTED
   /devices/pci@0,600000/pci@0/pci@8/pci@0,1/SUNW,qlc@1,1/fp@0,0:devctl
   CONNECTED
   ```

   NOTE

   If the fiber card is not in the **CONNECTED** state, check and ensure the following aspect:

   - The fiber is properly connected to the optical module.
   - There is not any damage to the fiber.
   - The optical module is properly connected to the fiber card.
   - The indicator of the fiber card is functioning properly.

3. Run the following commands to restart the OS of the server and refresh the disk status:
```
# sync;sync;sync;sync
# shutdown -y -g0 -i6
```
4. Run the following command to scan the LUN that maps the OceanStor S2600 disk array:
```
# format
```
The following message will be displayed:
```
Searching for disks...done

c1t2200662233556653d0: configured with capacity of 999.97GB
c2t2210662233556653d0: configured with capacity of 999.97GB


AVAILABLE DISK SELECTIONS:
       0. c0t0d0 <SUN72G cyl 14087 alt 2 hd 24 sec 424>
          /pci@0,600000/pci@0/pci@8/pci@0/scsi@1/sd@0,0
       1. c0t1d0 <SEAGATE-ST973402SSUN72G-0400 cyl 14087 alt 2 hd 24 sec 424>
          /pci@0,600000/pci@0/pci@8/pci@0/scsi@1/sd@1,0
       2. c1t2200662233556653d0 <HUAWEI-S2600-1 cyl 19198 alt 2 hd 64 sec 256>
          /pci@0,600000/pci@0/pci@8/pci@0,1/SUNW,qlc@1/fp@0,0/
ssd@w2200662233556653,0
       3. c2t2210662233556653d0 <HUAWEI-S2600-1 cyl 19198 alt 2 hd 64 sec 256>
          /pci@0,600000/pci@0/pci@8/pci@0,1/SUNW,qlc@1,1/fp@0,0/
ssd@w2210662233556653,0
Specify disk (enter its number):
```

NOTE

- The displayed disk size varies according to the actual size of the disk.
- The disk identified with `< HUAWEI-S2600-1 .... >` indicates the LUN that maps the OceanStor S2600 disk array.
- The scanned number of disks is the product of: the number of local disks, the number of LUNs that map the OceanStor S2600 disk array, and the number of fiber paths. After the MPxIO multipathing is enabled, the number of disks scanned by the **format** command is equal to the number of LUNs that map the OceanStor S2600 disk array.
- If the disks that map the OceanStor S2600 disk array fail to be scanned, run the **devfsadm -C** command first and the **format** command to scan the required disks. If the disks still cannot be scanned, ensure that the fiber is properly connected.

----End

H.2 Configuring the StorageTek 2540 Disk Array Through the Web Browser

This topic describes how to configure the StorageTek 2540 disk array through the Web browser.

Prerequisite

- The cables between the server and the disk array are connected properly.
- The IP addresses for both controllers of the StorageTek 2540 disk array are configured.
- The OS of the server is installed.
- The U2000***version***_server_patch_solaris_SPARC_dvd3 or installation package U2000***version***_server_ospatch_solaris_SPARC.tar are on-hand. The DVD or installation package contains the StorageTek 2540 disk array manager.

  The installation software package must be uploaded to the **/tmp** path of the server in binary mode through FTP. Run the **tar xvf** *name_of_installation_software_package* command to decompress the installation package.

Context

The **/tmp** path is the temporary system path. After restart, the system will automatically clear the files in the **/tmp** path.

NOTE

Configure disk arrays separately at the primary and secondary sites. The following uses the configuration of the disk array at the primary site as an example.

The following table describes the configuration requirements on the StorageTek 2540 disk array.

Configure Item	Settings
RAID group	The first five disks serve as the RAID group named **RAID5**.
LUN	Configure one LUN and name it **disk1**; set the capacity to **1000** GB.
Hot-spare disk	The sixth disk is designated as the global hot-spare disk.

Procedure

1 Install the StorageTek 2540 disk array manager CAM on the server.

1. Log in to the OS of the server as user **root**.
2. To navigate to the directory of the installation files, perform the following operations:

   If the disk array manager was installed by using an installation DVD, perform the following operations:

   a. Insert U2000***version***_server_patch_solaris_SPARC_dvd3 into the DVD-ROM drive.

   b. Run the following command to navigate to the **/tmp** path:
   ```
   # cd /tmp
   ```

   c. Run the following command to copy the files from the **/cdrom/cdrom0/patches** directory to the **/tmp** path:
   ```
   # cp -r /cdrom/cdrom0/patches /tmp
   ```

   d. Run the following command to navigate to the **/tmp/patches/sun** directory where the installation files are saved:
   ```
   # cd /tmp/patches/sun
   ```

   If the disk array manager was installed by using an installation package, perform the following operations:

   a. Run the following command to navigate to the **/tmp** path:
   ```
   # cd /tmp
   ```

   b. Run the following **tar** command to decompress the installation package:
   ```
   # tar xvf U2000version_server_ospatch_solaris_SPARC.tar
   ```

   c. Run the following command to navigate to the **/tmp/patches/sun** directory where the installation files are saved:
   ```
   # cd /tmp/patches/sun
   ```

3. Run the following command to decompress the CAM installation file:
   ```
   # gzcat host_sw_solaris_6.6.0.11.tar.gz | tar xf -
   ```
4. Run the following commands to install the CAM software:

```
# cd /tmp/patches/sun/HostSoftwareCD_6.6.0.11
# ./RunMe.bin -c
```

Follow the screen prompts and proceed with the installation of the StorageTek 2540 disk array manager.

NOTE

- During the installation, enter **1** and select **I accept the terms of the license agreement** in the license agreement window, and press **Enter** in the other windows.
- During the CAM installation, some OS patches may fail to be installed, but the failure does not affect the use of the CAM software; therefore, you can ignore these occurrences.

5. Run the following commands to enable the Internet Explorer login rights of other IP addresses:

```
# svccfg -s svc:/system/webconsole:console setprop options/local=false
# svccfg -s svc:/system/webconsole setprop options/tcp_listen=true
# svcadm restart svc:/system/webconsole
```

NOTE

Run the **netstat -an | grep 6789** command to verify that the login rights of other IP addresses are enabled. Information similar to the following will be displayed if rights are enabled. If no, run the preceding commands again.

```
      *.6789               *.*                0      0 49152      0 LISTEN
```

2 Start the disk array manager.

1. Log in to the OS of the Windows management terminal as an administrator.
2. Open the IE, enter the local IP address of the management terminal in the **Address** bar, and then press **Enter**. The IP address is in an **https://127.0.0.1:6789/**.

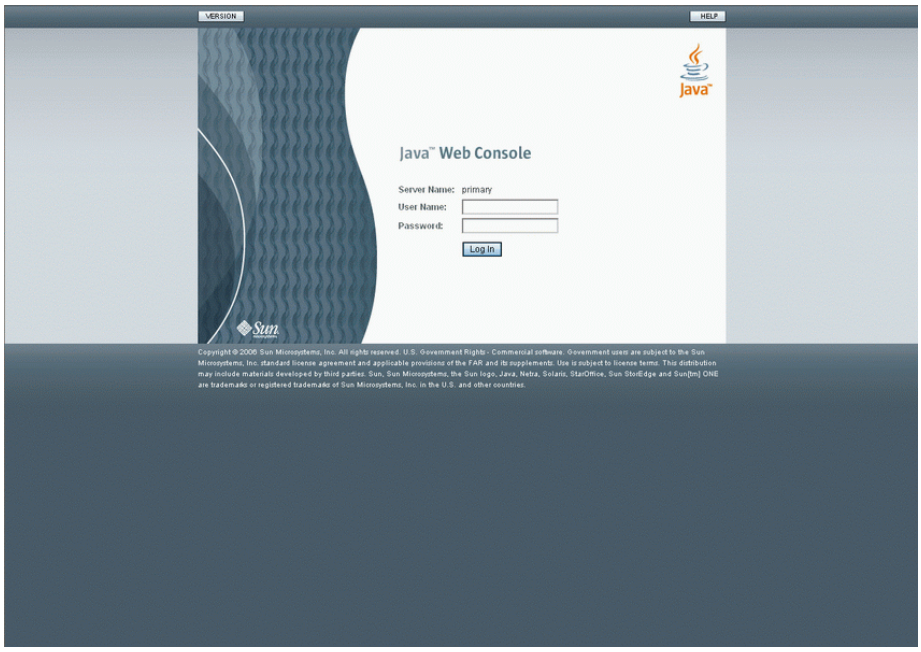
NOTE

You can also access the management terminal where the disk array manager is installed by using the IE on other Windows management terminals. In this scenario, enter the actual IP address of the management terminal where the disk array manager is installed.

3. The **Security Alert** dialog box is displayed. Click **Yes**.
4. In the login window, enter the user name and password, for example, **root**, and click **Log In**.

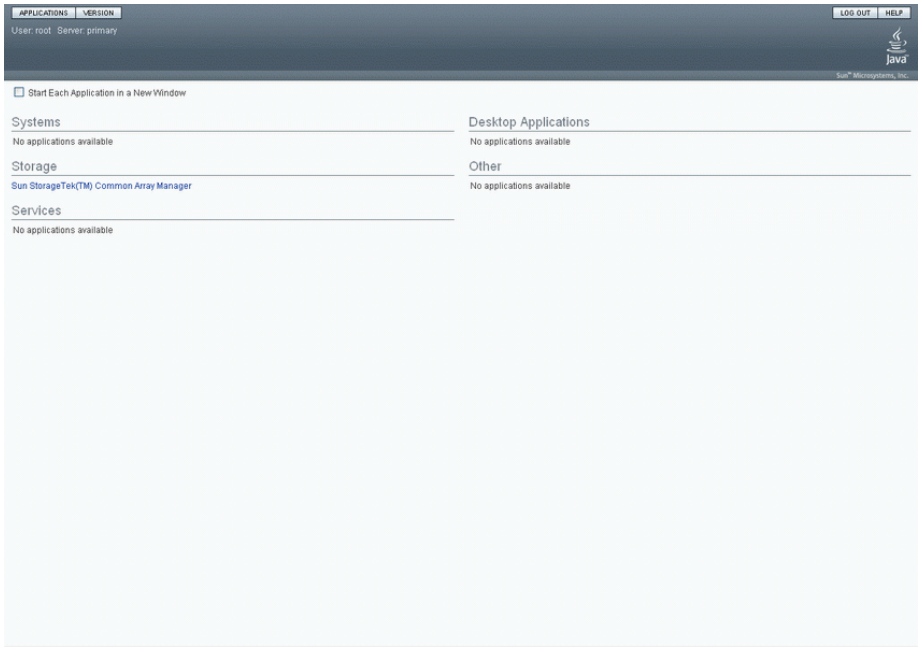
NOTE

If the security warning information is displayed, click **Confirm**.

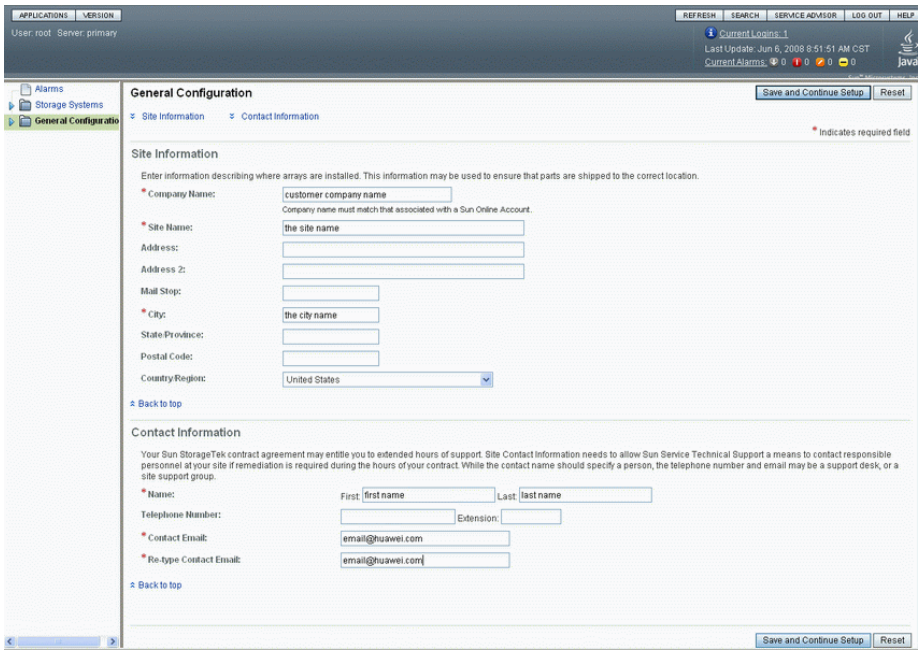


3 Configure the StorageTek 2540 disk array by using the disk array manager.

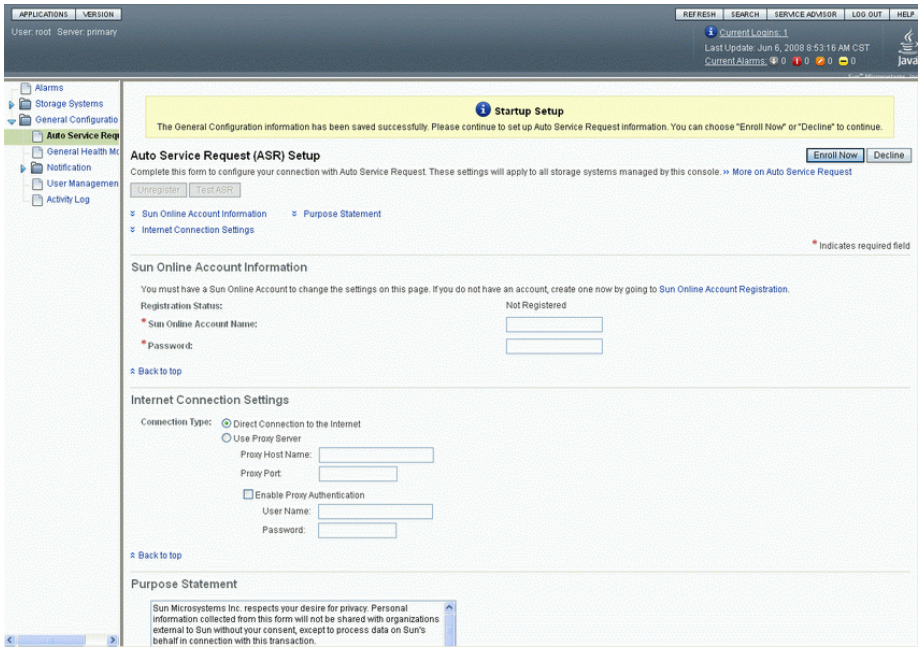
1. On Java Web console, click **Sun Storage Tek(TM) Common Array Manager** in **Storage**.



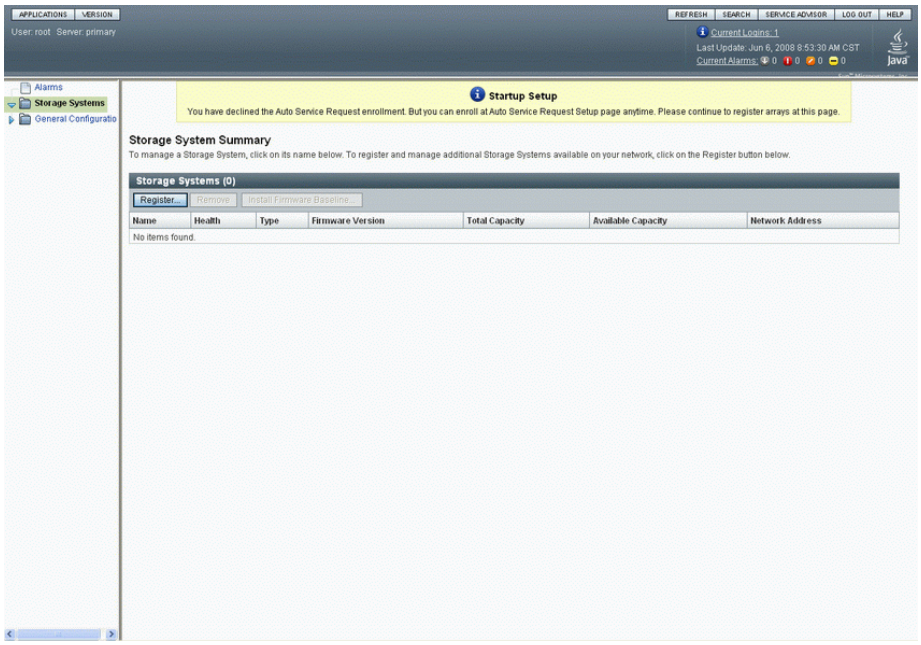
2. In the Common Array Manager, choose **General Configuration** from the navigation tree to set the station information. Then, click **Save and Continue Setup**.



3. Choose **General Configuration** > **Auto Service Request (ASR) Setup** from the navigation tree and click **Decline** in the **Auto Service Request (ASR) Setup** window.

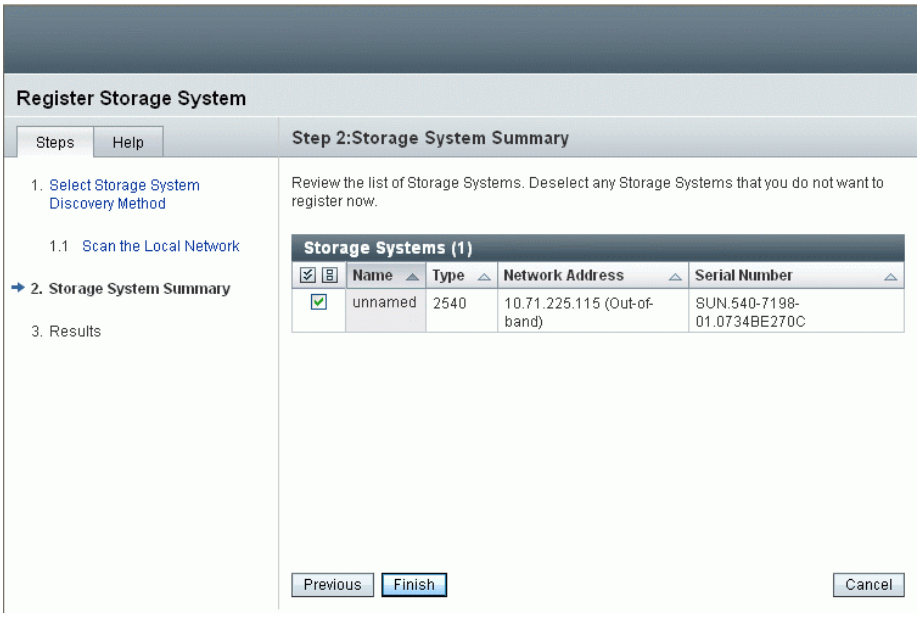


4. Choose **Storage Systems** from the navigation tree and click **Register**.

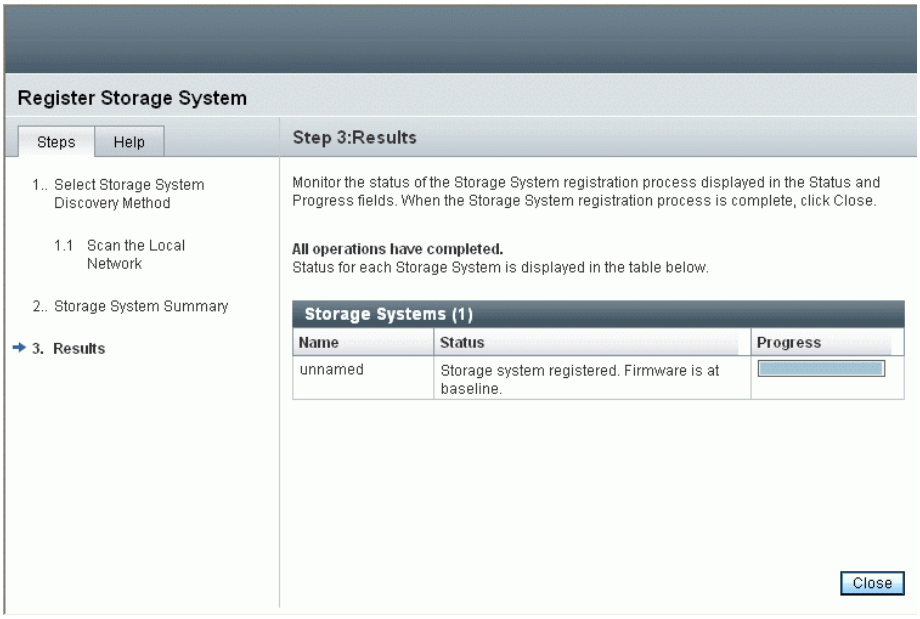


5. In the **Register Storage System** window, select **Enter IP address or hostname**, enter the IP address of disk array controller A in the address bar, and then click **Next**.

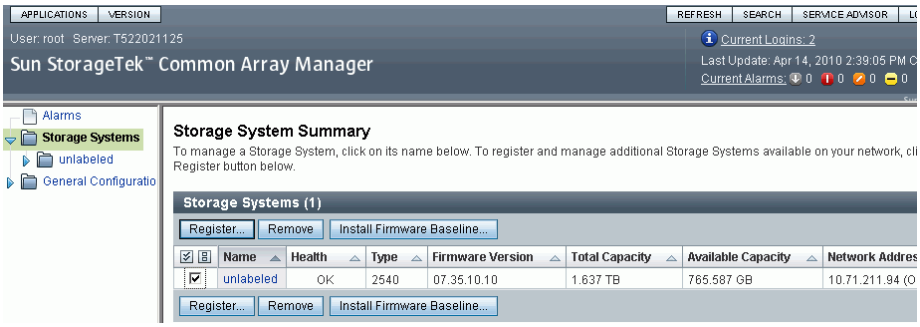
6. View the storage system list, select the system that you want to register right now, and click **Finish**.



7. The system will display a progress bar. After the registration is complete, click **Close**.



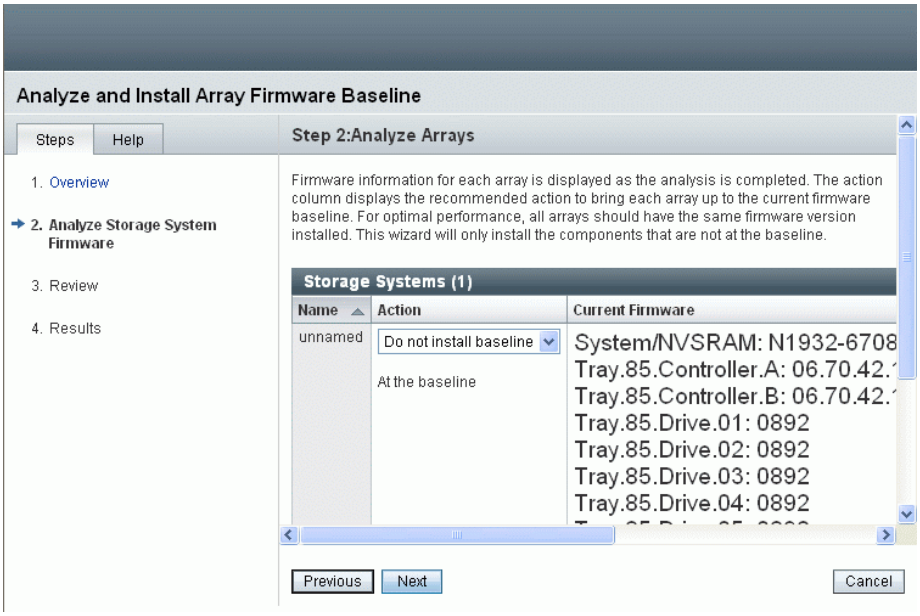
8. Under **Storage Systems** in the navigation tree, select the disk system to be configured and click **Install Firmware Baseline**.



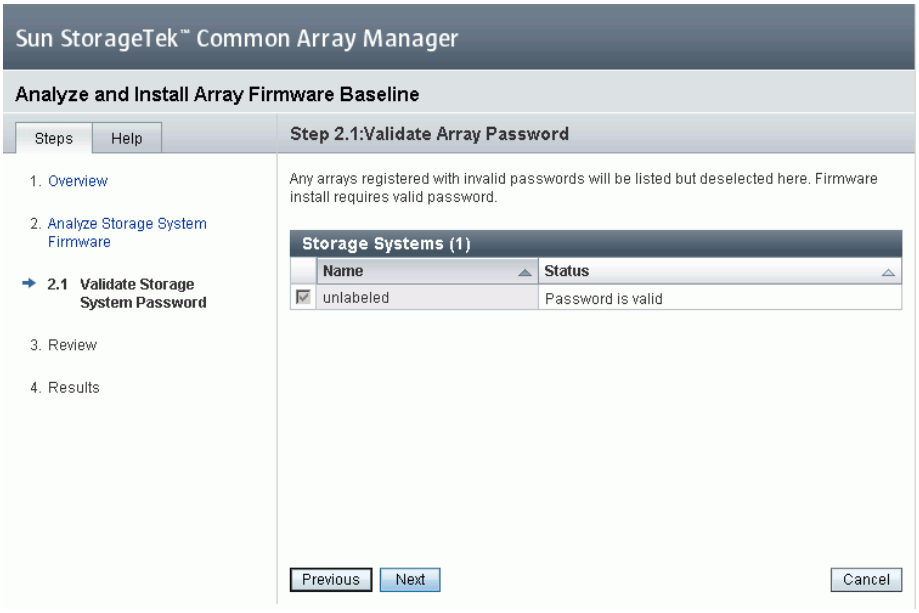
9. In the **Analyze and Install Array Firmware Baseline** window, click **Next**.
10. Analyze the firmware of the storage system and click **Next**.

NOTE

- If the components are not at the baseline (**Health** is displayed as **Degraded**), select **Install baseline, All** in **Storage Systems (1)**.
- If the components are at the baseline (**Health** is displayed as **OK**), select **Do not install baseline** in **Storage Systems (1)**.
- Options vary with CAM software versions. Select the appropriate option according to the conditions at your site.



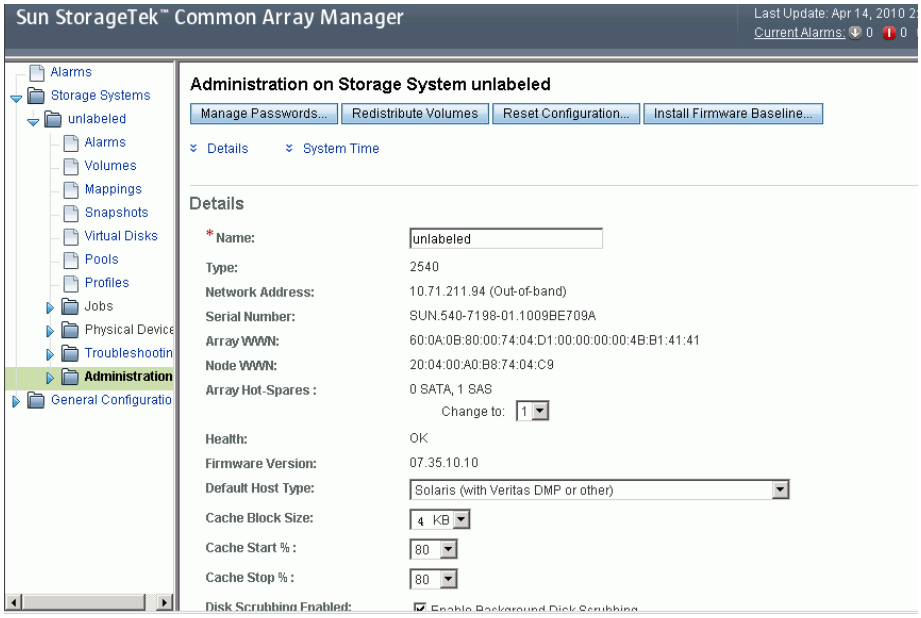
11. Verify the array password and click **Next**.



12. View the current selection and click **Finish** to install the specified firmware. After the installation is complete, click **Close**.
13. Select the storage system to be set from the navigation tree and set the detailed information in **Administration**. Then, click **Save**.

NOTE

- Set **Array Hot-Spares** to **1**.
- Set **Default Host Type** to **Solaris (with Veritas DMP or other)**.
- Use default values for other parameters.



14. In the storage system to be configured, choose **unamed** > **Physical Device** > **Disks**. Then, on the **Disk Summary on Storage System unlabeled** tab page, click the name of the last disk.
15. On the **Disk Details** tab page, click **Assign Hot-Standby Disk**. The **Succeeded in operating the hot-standby disk** message will be displayed.
16. In the storage system to be set, choose **Physical Device** > **Disks** from the navigation tree. In the **Role** column, ensure that the disk for hot backup has been allocated.

    NOTE

    Repeat **3.14** to **3.15** to set and save the information again if a disk for hot backup has not been allocated.

Disk Summary on Storage System unlabeled

Disks (6)

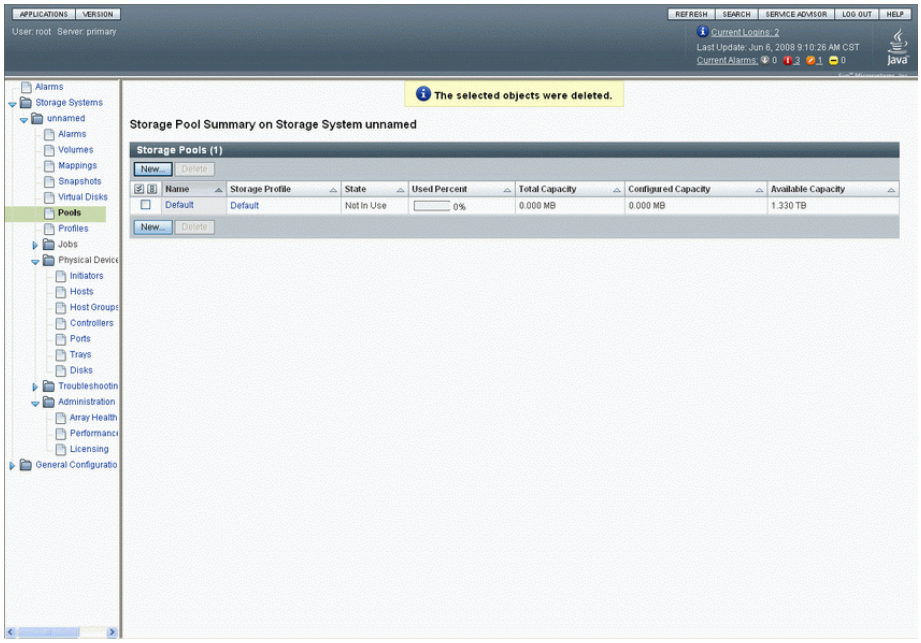
Name	Array Name	Array Type	Tray	Role	State	Status	Capacity	Type	Firmware
t85d01		2540	85	Data Disk	Enabled	Optimal	279.396 GB	SAS	SA04
t85d02		2540	85	Data Disk	Enabled	Optimal	279.396 GB	SAS	SA04
t85d03		2540	85	Data Disk	Enabled	Optimal	279.396 GB	SAS	SA04
t85d04		2540	85	Data Disk	Enabled	Optimal	279.396 GB	SAS	SA04
t85d05		2540	85	Data Disk	Enabled	Optimal	279.396 GB	SAS	0605
t85d06		2540	85	Array Spare	Enabled	Optimal	279.396 GB	SAS	SA04

17. Delete the default mapping. In the navigation tree on the left, choose **Storage Systems** > **unnamed** > **Mappings**. Select the existing mapping **Access** and click **Delete**.
18. In the storage system to be configured, choose **Profiles** and click **New**.
19. Configure the configuration file and click **Confirm**.

NOTE

- Set **Storage Profile** to **NMS_Profile**.
- Set **Raid Level** to **Raid5**.
- Set **Segment Size** to **512KB**.
- Set **No. of Disks** to **5**.
- Set **Disk Type** to **SAS**.

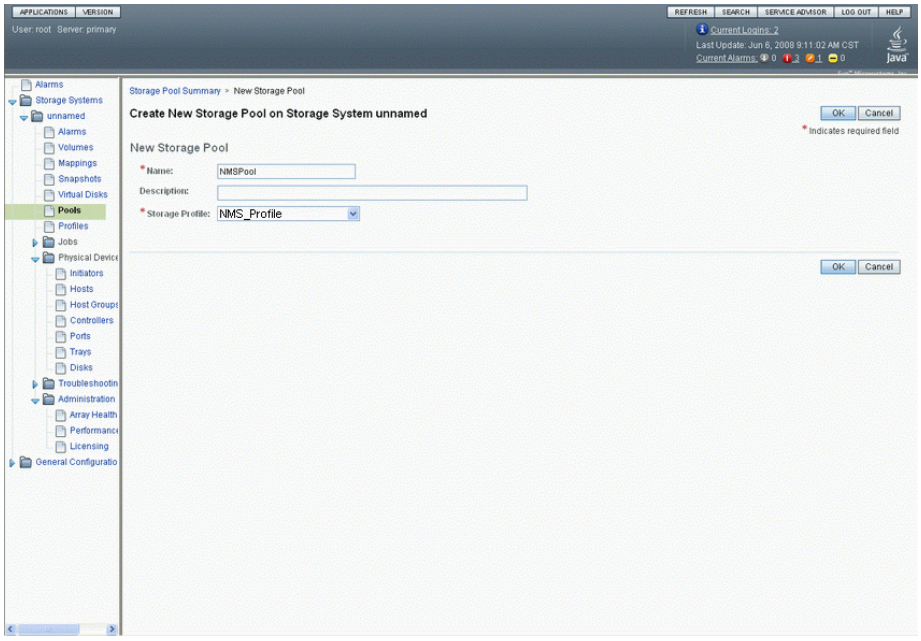
20. In the storage system to be set, choose **Pools** from the navigation tree and click **New**.



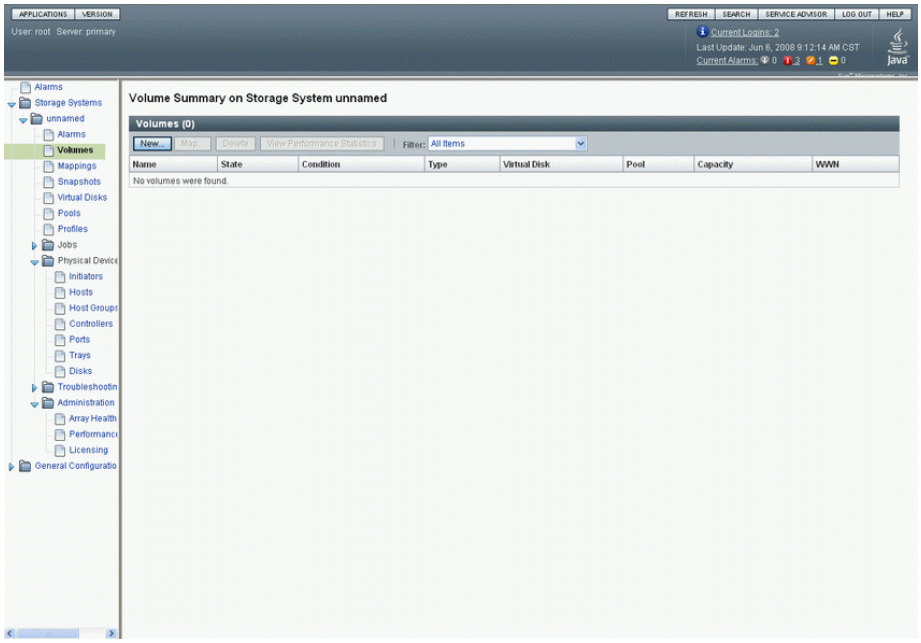
21. Set the storage pool and click **OK** to complete the settings.

NOTE

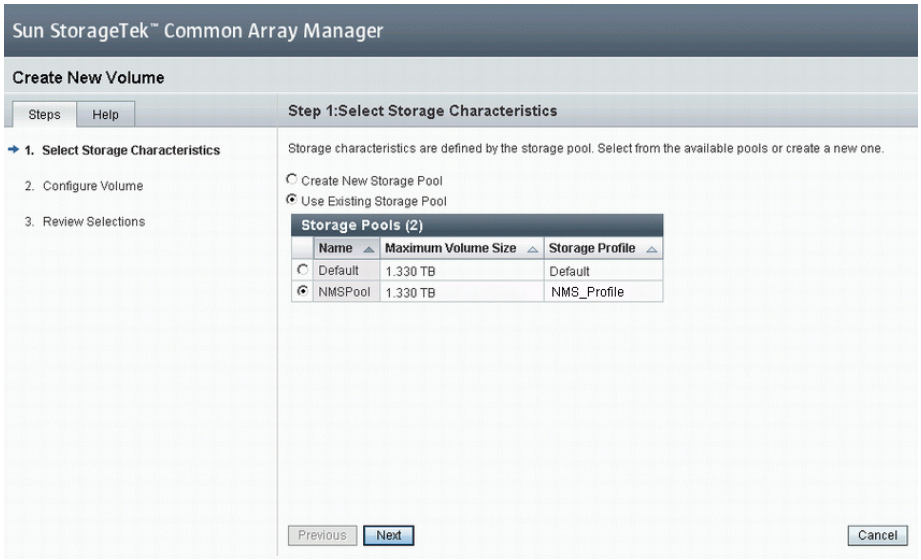
- Set **Name** to **NMSPool**.
- Set **Storage Profile** to **NMS_Profile**.



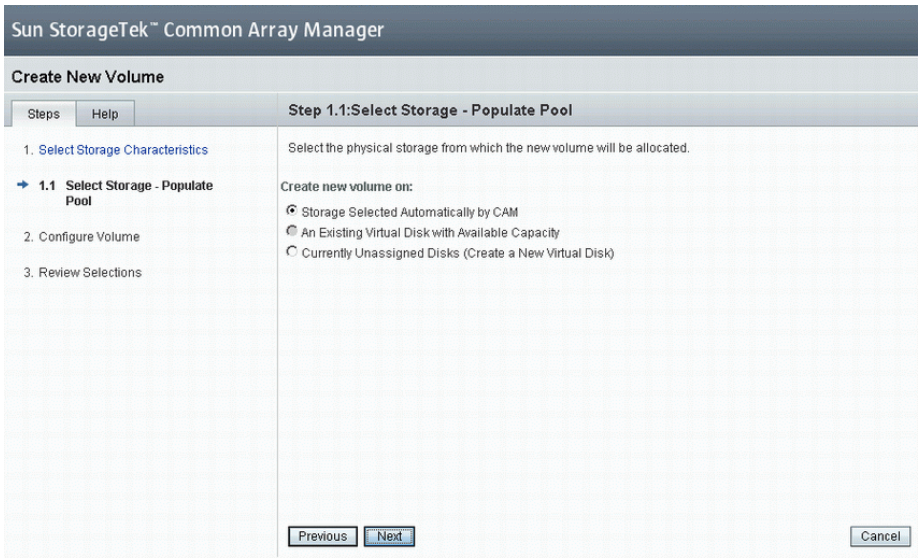
22. Create a volume. In the storage system to be set, choose **Volumes** from the navigation tree and click **New**.



23. Select **Use Existing Storage Pool**, select the storage pool **NMSPool**, and then click **Next**.



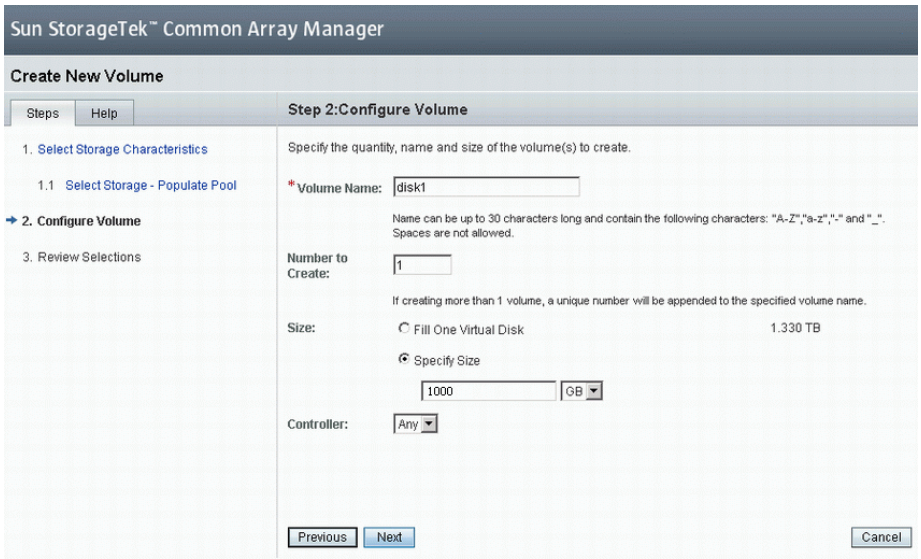
24. Set the storage characteristics. Specifically, select **Storage Selected Automatically by CAM** and click **Next**.



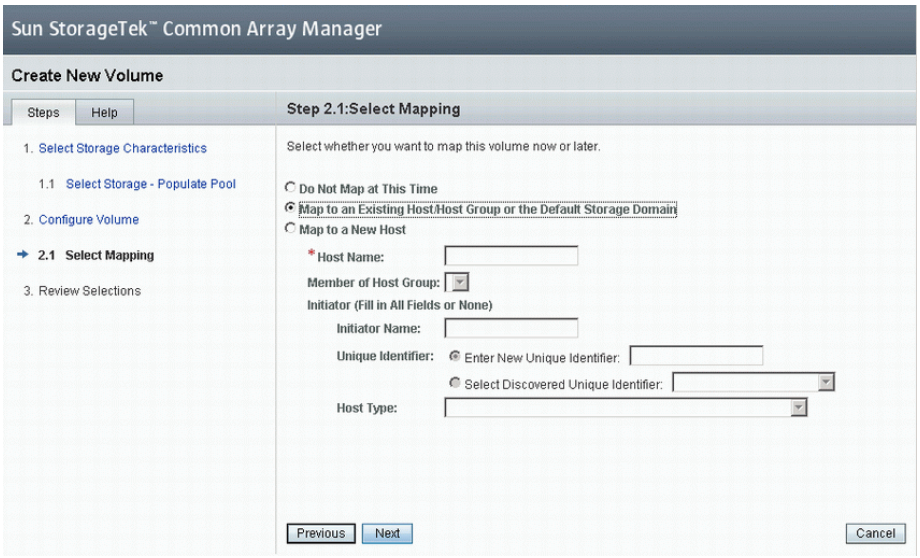
25. Configure the volume.

    NOTE

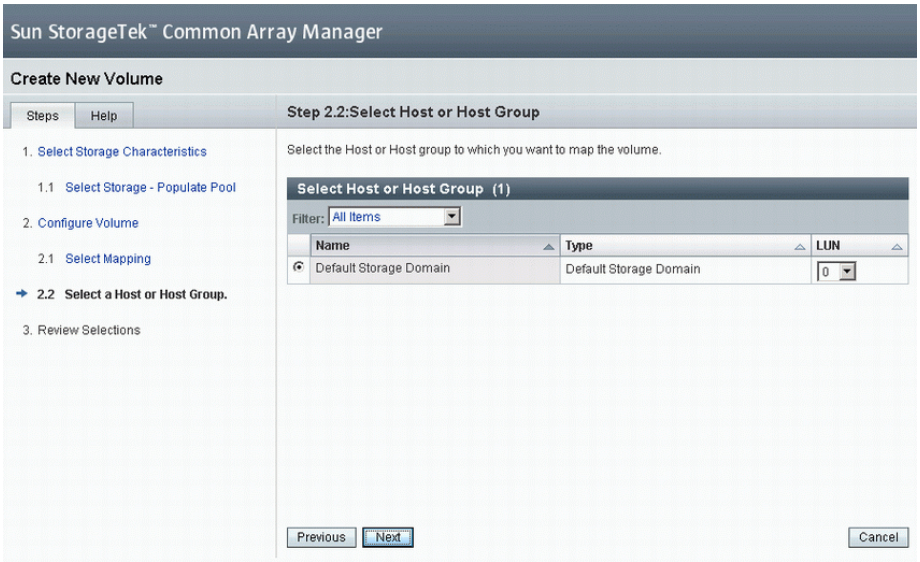
    - Set the volume name to **disk1**.
    - Set the number of volumes to be created to **1**.
    - Set the size of the volume to 1000 GB.
    - Set the controller to **Any**.



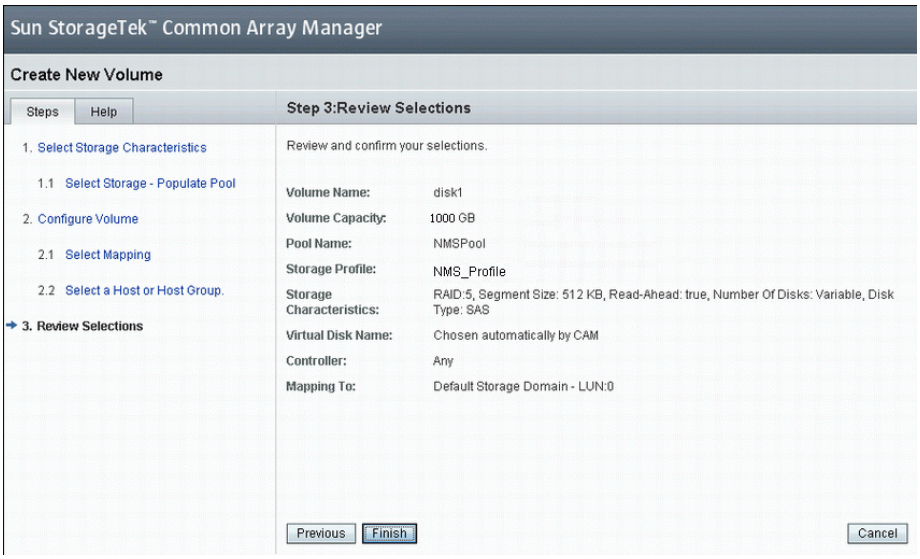
26. Select mapping. Specifically, select **Map to an Existing Host/Host Group or the Default Storage Domain** and click **Next**.



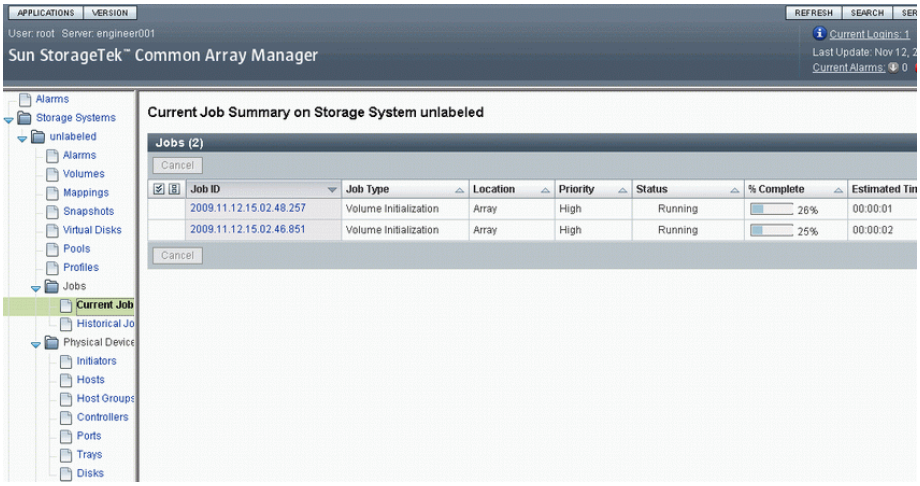
27. Select the host or host group. Specifically, select **Default Storage Domain** and click **Next**.



28. Check the settings and click **Finish**.



29. View the progress of the current job. Specifically, choose **Jobs** > **Current Job** to view the progress of the current job and wait until it is completed.



4 Update disk information.

1. Run the following command to view connections to the ports of the fiber cards:
   ```
   # luxadm -e port
   ```
   The following message will be displayed:
   ```
   /devices/pci@0,600000/pci@0/pci@8/pci@0,1/SUNW,qlc@1/fp@0,0:devctl   CONNECTED
   /devices/pci@0,600000/pci@0/pci@8/pci@0,1/SUNW,qlc@1,1/fp@0,0:devctl
   CONNECTED
   ```
   NOTE
   If the fiber card is not in the **CONNECTED** state, check and ensure the following items:
   - The fiber is properly connected to the optical module.
   - There is not any damage to the fiber.
   - The optical module is properly connected to the fiber card.
   - The indicator of the fiber card is functioning properly.
2. Run the following commands to update the disk information:
   ```
   # devfsadm -C
   # devfsadm
   ```
3. Run the following command to check the disk information:
   ```
   # format
   ```

The following message will be displayed:

```
Searching for disks...done

c3t2d0: configured with capacity of 999.99GB
c3t2d1: configured with capacity of 999.99GB


AVAILABLE DISK SELECTIONS:
       0. c0t0d0 <SUN72G cyl 14087 alt 2 hd 24 sec 424>
          /pci@0,600000/pci@0/pci@8/pci@0/scsi@1/sd@0,0
       1. c0t1d0 <SEAGATE-ST973402SSUN72G-0400 cyl 14087 alt 2 hd 24 sec 424>
          /pci@0,600000/pci@0/pci@8/pci@0/scsi@1/sd@1,0
       2. c3t2d0 <SUN-LCSM100_F-0670 cyl 38398 alt 2 hd 128 sec 64>
          /pci@0,600000/pci@0/pci@8/pci@0,1/SUNW,qlc@1/fp@0,0/
ssd@w202300a0b85a4d21,0
       3. c3t2d1 <SUN-LCSM100_F-0670 cyl 38398 alt 2 hd 128 sec 64>
          /pci@0,600000/pci@0/pci@8/pci@0,1/SUNW,qlc@1/fp@0,0/
ssd@w202300a0b85a4d21,1
Specify disk (enter its number):
```

NOTE

- **SUN-LCSM100_F** indicates the new volumes that are configured for the StorageTek 2540 disk array.
- If two controllers are properly connected to the server, the information about the volumes of the two StorageTek 2540 disk arrays will be displayed. Otherwise, check the connections of the disk arrays and run the **reboot -- -r** command to restart the server.

5 Label the unlabeled disks.

1. Select the disk to be labeled.

   The following message will be displayed:

   ```
   selecting c1t600A0B80005A4D2100000E6D4AFB1E2Cd0
   [disk formatted]
   Disk not labeled.  Label it now?
   ```

2. Enter **y** to label the disk.

   The following message will be displayed:

   ```
   FORMAT MENU:
           disk       - select a disk
           type       - select (define) a disk type
           partition  - select (define) a partition table
           current    - describe the current disk
           format     - format and analyze the disk
           repair     - repair a defective sector
           label      - write label to the disk
           analyze    - surface analysis
           defect     - defect list management
           backup     - search for backup labels
           verify     - read and display labels
           save       - save new disk/partition definitions
           inquiry    - show vendor, product and revision
           volname    - set 8-character volume name
           !<cmd>     - execute <cmd>, then return
           quit
   format>
   ```

3. Enter **disk**.

   The following message will be displayed:

   ```
   AVAILABLE DISK SELECTIONS:
          0. c0t0d0 <SUN72G cyl 14087 alt 2 hd 24 sec 424>
             /pci@0,600000/pci@0/pci@8/pci@0/scsi@1/sd@0,0
          1. c0t1d0 <SEAGATE-ST973402SSUN72G-0400 cyl 14087 alt 2 hd 24 sec 424>
             /pci@0,600000/pci@0/pci@8/pci@0/scsi@1/sd@1,0
          2. c1t600A0B80005A4D2100000E6D4AFB1E2Cd0 <SUN-LCSM100_F-0670 cyl 38398
   ```

```
alt 2 hd 128 sec 64>
          /scsi_vhci/ssd@g600a0b80005a4d2100000e6d4afb1e2c
Specify disk (enter its number):
```

4. Repeat **5.1** to **5.3** for the other unlabeled disks.
5. Press **Ctrl**+**D** to exit.

----End

H.3 Configuring the OceanStor S3100 Disk Array

This topic describes how to configure the OceanStor S3100 disk array.

H.3.1 Configuring the SC IP Address of the OceanStor S3100 Disk Array
This topic describes how to configure the SC IP address of the OceanStor S3100 disk array.

H.3.2 Using the Manager Suite to Configure the OceanStor S3100 Disk Array
This topic describes how to use the Manager Suite to configure the OceanStor S3100 disk array.

H.3.1 Configuring the SC IP Address of the OceanStor S3100 Disk Array

This topic describes how to configure the SC IP address of the OceanStor S3100 disk array.

Prerequisite

- The controller IP addresses are obtained.
- The power cable of the disk array is connected.

Context

Each disk array OceanStor S3100 has two controllers that need to be configured separately.

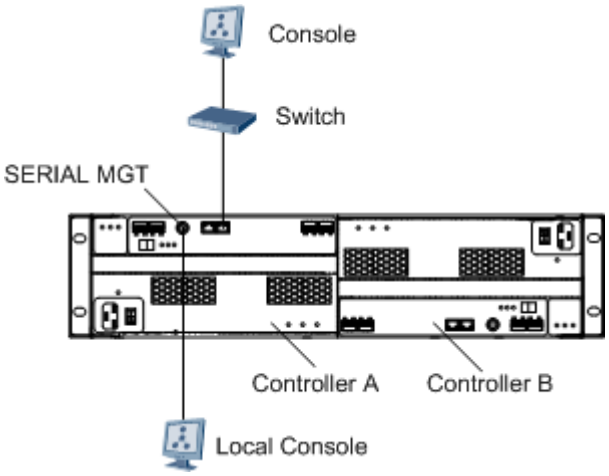
Procedure

1 Connect the computer and controller A of the disk array physically.

Use a serial port cable (DB9-PS/2) to connect the serial port of the local controller to the serial port of the disk array (SERIAL MGT).

Use an PS/2 connector at one end of the serial port cable to connect to the serial port of the disk array (SERIAL MGT) and a DB-9 connector at the other end of the cable to connect to the serial port of the computer (COM1 or COM2).

Figure H-1 Connections between the controllers of the OceanStor S3100 disk array



2 Set up a logical connection between the computer and controller A.

1. Start the computer and enter Windows OS.
2. Choose **start** > **Programs (P)** > **Accessories** > **Communications** > **HyperTerminal**.
3. In the **Connection Description** dialog box, enter the name of the new connection, such as **NMS**, and click **OK**.
4. In the dialog box that is displayed, select the serial port of the computer that is used to connect to the disk array, such as COM1, and click **OK**.
5. In the dialog box that is displayed, set the attributes of the serial port as follows:
   - Bits per second: 9600 bps
   - Data bit: 8 bit
   - Parity check: none
   - Stop bit: 1 bit
   - Data flow control: none
6. Click **OK**.

3 Configure the IP address of the network interface of controller A of the disk array on the local console.

NOTE

One OceanStor S3100 disk array has two controllers. You need to configure them separately.

1. Send a break signal from the computer by pressing **Ctrl+Pause Break**.
2. Press **ESC** within five seconds according to the prompt to access the shell login window.
3. Enter **infiniti** as the password and press **Enter**. If a dialog box shown in the following figure is displayed, it indicates that the login to the configuration shell of the controller succeeds.

```
Press within 5 seconds: <S> for Service Interface, <BREAK> for baud rate *** Exp
ired

Press within 5 seconds: <S> for Service Interface, <BREAK> for baud rate


Current date: 07/11/07  time: 06:25:12

Enter password to access shell:
LSI Logic RAID Controller
Copyright 2004-2006 LSI Logic Corporation. All Rights Reserved.
Copyright Wind River Systems, Inc., 1984-2003
VxWorks: VxWorks5.5.1   Kernel: WIND version 2.6
Model: 3994    Firmware version: 06.19.15.00



-> _
```

4. At the prompt, enter **netCfgShow** and press **Enter**. The information about the configuration network interface of the controller that you have logged in to is displayed.

```
->
-> netCfgShow

==== CURRENT NETWORK CONFIGURATION ====
My Host Name          :
Interface Name    if0 :  esmc0
MAC Address       if0 :  00:a0:b8:2a:3f:6c
IP Address        if0 :  10.78.111.101
Subnet Mask       if0 :  255.255.255.0
Interface Name    if1 :  esmc1
MAC Address       if1 :  00:a0:b8:2a:3f:6d
IP Address        if1 :  192.168.129.101
Subnet Mask       if1 :  255.255.255.0
Server Host Name      :
Server IP Address     :  0.0.0.0
Gateway IP Address    :  10.78.111.1
Network Init Flags    :  0xA0
User Name             :
User Password         :
value = 24 = 0x18
-> _
```

5. At the prompt, enter **netCfgSet**.

   The following message will be displayed:

```
->
-> netCfgSet


    '.' = clear field;  '-' = to previous field;
     ^D = quit (keep changes)

==== CURRENT NETWORK CONFIGURATION ====
My Host Name          :
IP Address if0        :  10.78.111.101            10.78.111.56
```

NOTE

There are three subcolumns in the **CURRENT NETWORK CONFIGURATION** column.

- The first subcolumn displays the name of the information about this row.
- The second subcolumn displays the current values.
- The third subcolumn displays a flashing cursor.

6. Enter information about the network card to be modified at the flashing cursor, which includes the IP address, gateway, and subnet mask of the network card.

   NOTE

   - Select a network interface of the controller for configuration according to the actual connection condition. The following takes the configuration of if0 as an example.
   - If there is no special requirement, keep the default settings of the other network interface of the controller unchanged.
   - If you press **Enter**, the current values in the second subcolumn remain unchanged. If you enter the desired characters and then press **Enter**, the values in the second subcolumn are changed to the new values.
   - If you need to restore a value to the default factory setting, enter **.**.
   - if0 indicates to network interface 1 of the disk array; if1 indicates network interface 2 of the disk array. Generally, it is recommended that you use network interface 1. You need to set only **IP Address if0**, **Subnet Mask if0**, and **Gateway IP Address** rather than **My Host Name**, **Server Host Name**, **Server IP Address**, **Network Init Flags**, **User Name**, and **User Password**.

   The following message will be displayed:

```
-> netCfgSet


    '.' = clear field;  '-' = to previous field;
      ^D = quit (keep changes)

==== CURRENT NETWORK CONFIGURATION ====
My Host Name          :
IP Address if0        :  10.78.111.101            10.78.111.56
Subnet Mask if0       :  255.255.255.0
IP Address if1        :  192.168.129.101
Subnet Mask if1       :  255.255.255.0
Server Host Name      :
Server IP Address     :
Gateway IP Address    :  10.78.111.1
Network Init Flags    :  0xA0
User Name             :
User Password         :

Network Configuration successfully written to NVSRAM.
value = 0 = 0x0
->
```

   NOTE

   Here, **Network Configuration successfully written to NVSRAM** indicates that the modification is successful.

4 Disconnect the serial port cable from controller A.

1. On the computer, exit the HyperTerminal software.
2. Remove the serial port cable on the disk array.

5 Repeat Step 1 to Step 4 to configure the network port of controller B.

1. Establish a physical connection between the computer and controller B.
2. Establish a logical connection between the computer and controller B.
3. Configure the IP address of the network interface of controller B on the local console.
4. Disconnect the serial port from controller B.

----End

H.3.2 Using the Manager Suite to Configure the OceanStor S3100 Disk Array

This topic describes how to use the Manager Suite to configure the OceanStor S3100 disk array.

Prerequisite

- The cables between the server and the disk array are connected properly.
- The IP addresses for both controllers of the OceanStor S3100 disk array are configured.
- The OS of the server is installed.
- Before installing the Manager Suite, ensure that there is at least 140 MB of remaining hard disk space for full installation.

Context

NOTE

Configure disk arrays separately at the primary and secondary sites. The following uses the configuration of the disk array at the primary site as an example.

The following table describes the configuration requirements on the OceanStor S3100 disk array.

Configure Item	Settings
RAID group	The first five disks serve as the RAID group named **RAID5**.
LUN	Configure one LUN and name it **disk1**; set the capacity to **500** GB.
Hot-spare disk	The sixth disk is designated as the global hot-spare disk.

Procedure

1 Install the Manager Suite.

1. Log in to the server as user **root**.
2. Insert the **OceanStor Manager Suite 9.19 for S3000/S6000** installation DVD or prepare the **SMruntime-SOL.pkg**, **SMclient-SOL.pkg**, and **SMutil-SOL.pkg** installation packages.

   NOTE

   When uploading the installation packages by means of FTP, run the following commands to enable the FTP rights of user **root**:
   ```
   # sed "/^root/s//#root/g" /etc/ftpd/ftpusers > /tmp/ftpusers
   # cp /tmp/ftpusers /etc/ftpd/ftpusers
   ```
   Upload the installation packages to the **/tmp** path in binary mode.
3. In the terminal window, run the following command to go to the destination directory:
   ```
   # cd /cdrom/cdrom0/Solaris/native
   ```

   NOTE

   When installing from the hard disk, run the following command to go to the destination directory:
   ```
   # cd /tmp
   ```

4. Run the following commands to install the Manager Suite. Follow the screen prompts and determine the appropriate action specific to site scenarios:

```
# pkgadd -d /tmp/SMruntime-SOL.pkg SMruntime
# pkgadd -d /tmp/SMutil-SOL.pkg SMutil
# pkgadd -d /tmp/SMclient-SOL.pkg SMclient
```

   Installation of the Manager Suite is complete.

5. Run the following commands to check the installation of the Manager Suite:

```
# pkginfo -l SMruntime
# pkginfo -l SMutil
# pkginfo -l SMclient
```

   The Manager Suite was successfully installed if the information about the corresponding installation package is displayed after each command is run. Otherwise, perform the following to reinstall the Manager Suite:

   a. Uninstall the Manager Suite.

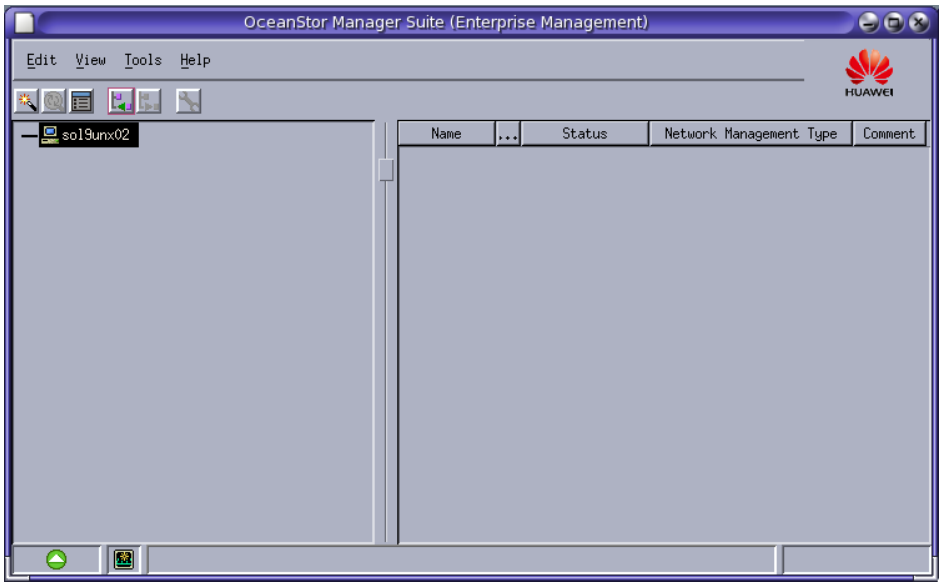
      1) Run the following command:
         ```
         # pkgrm SMutil
         ```
      2) Enter **y**.
      3) Run the following command:
         ```
         # pkgrm SMclient
         ```
      4) Enter **y**.
      5) Enter **y**.
      6) Run the following command:
         ```
         # pkgrm SMruntime
         ```
      7) Enter **y**.

   b. Reinstall the Manager Suite.

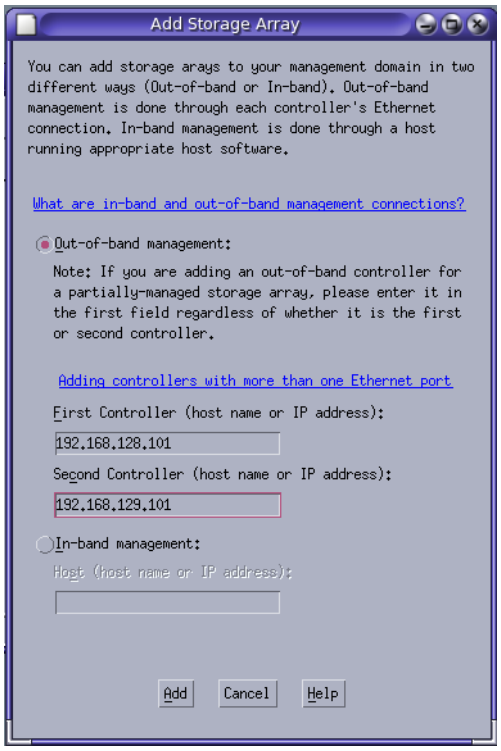
2 Log in to the server as user **root** through the GUI.

3 Use the Manager Suite to configure the OceanStor S3100 disk array.

1. In the terminal window, enter **SMclient** to start the Manager Suite.

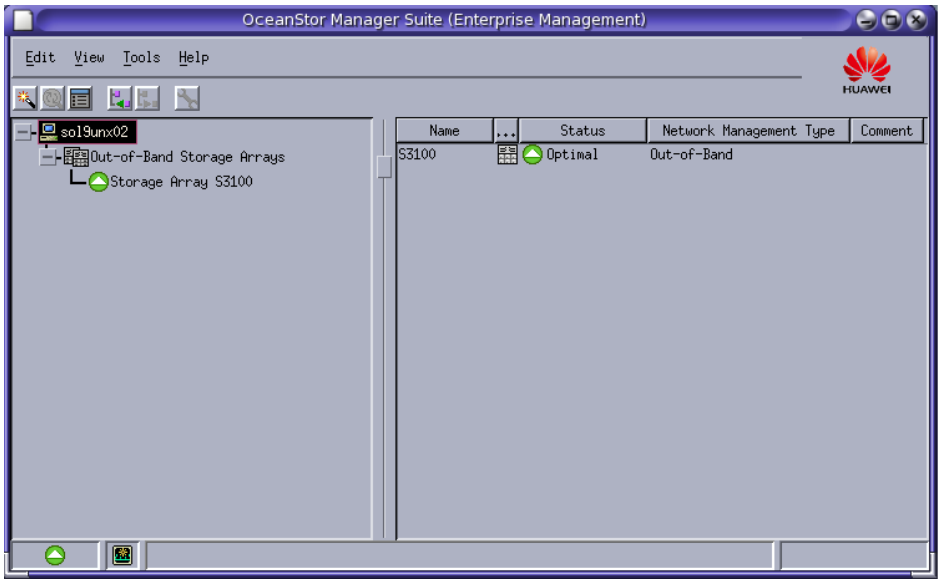


2. Click  . In the dialog box that is displayed, enter the IP addresses of controller A and controller B to log in to the local console.

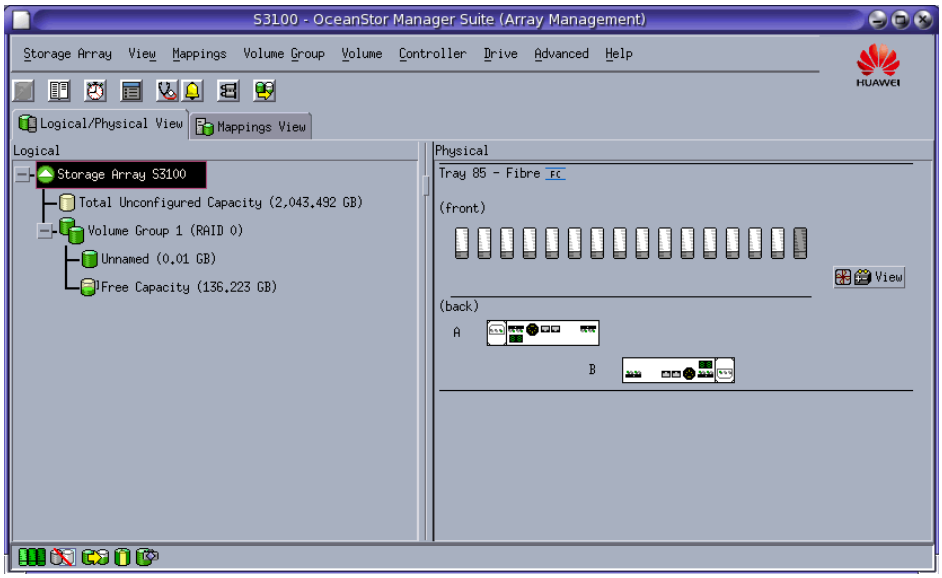


NOTE

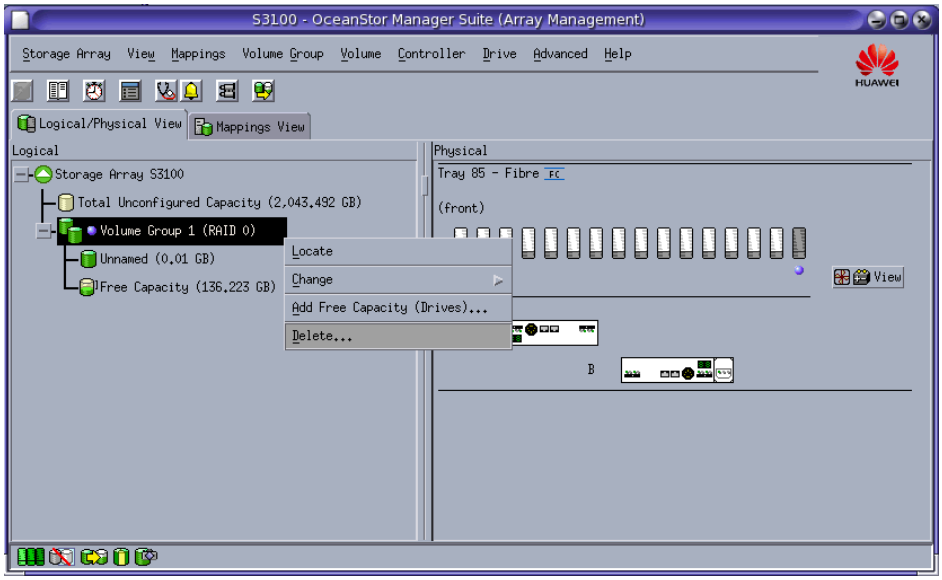
The IP addresses in the preceding figure are used as examples. Enter an appropriate IP address according to the conditions at your site. Before entering the IP addresses, ensure that you can ping through the IP addresses. Enter the IP addresses and click **Add** to add the disk array to the Manager Suite.

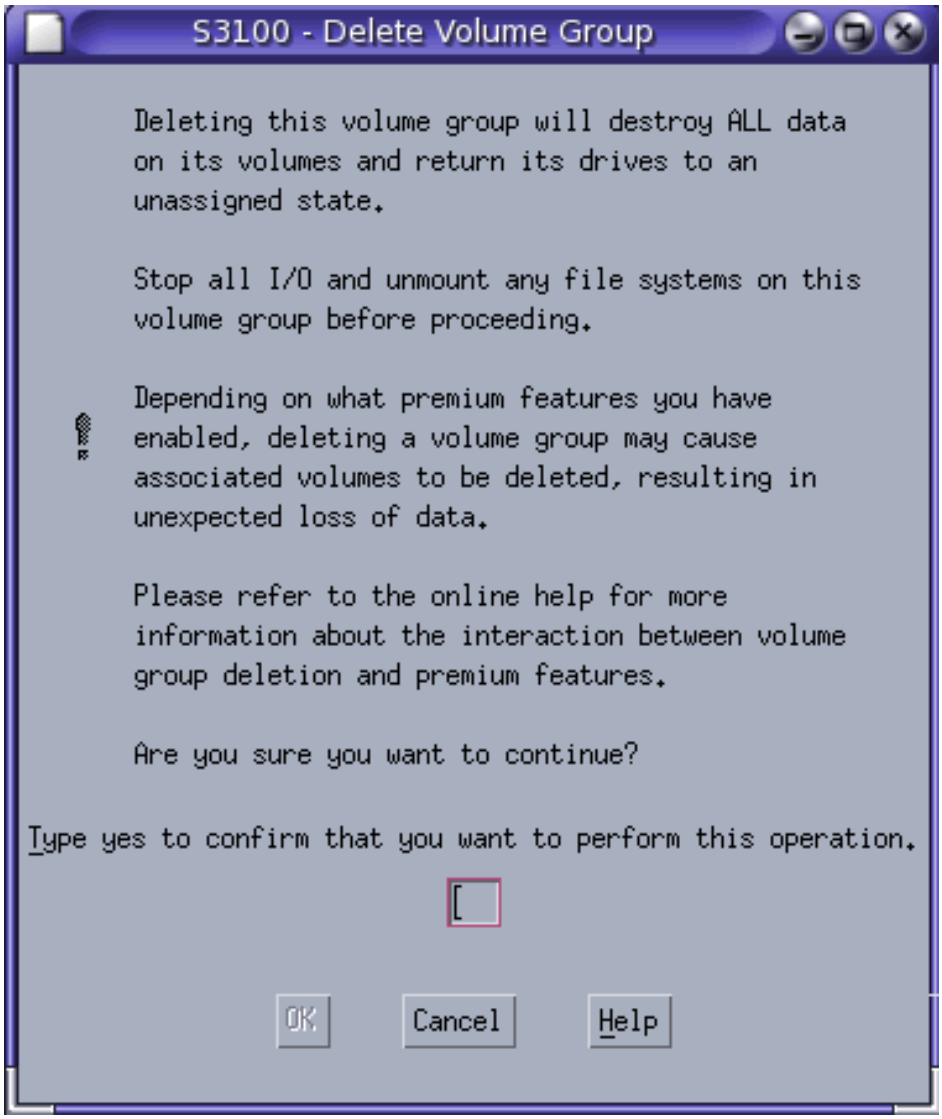


3. Double-click the storage equipment. The storage equipment management window will be displayed.

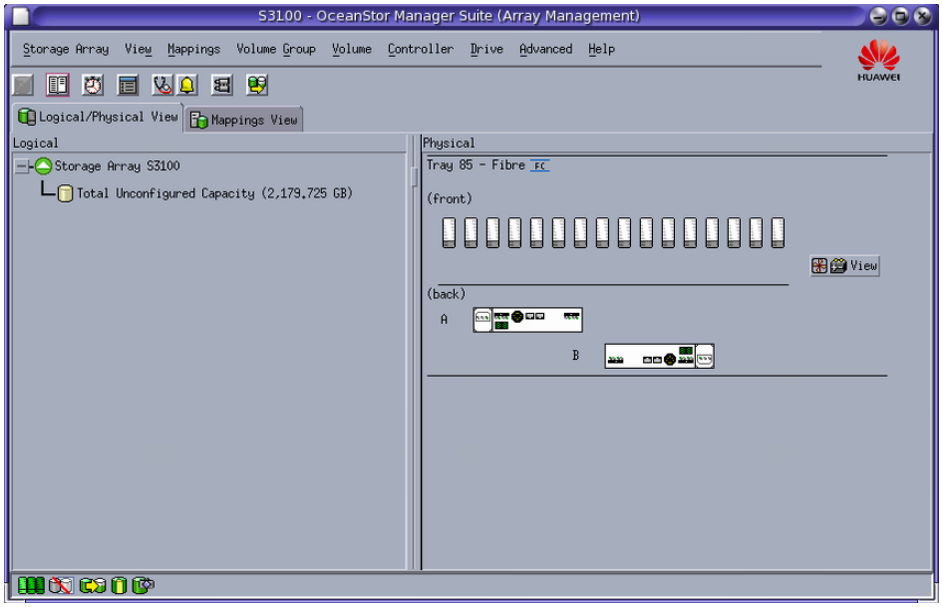


4. Usually, a new disk array has disk RAID0. The system automatically creates disk RAID0 by using a hard disk. Disk RAID0 has a volume of 0.01 GB. Right-click the volume group and choose **Delete** from the shortcut menu.

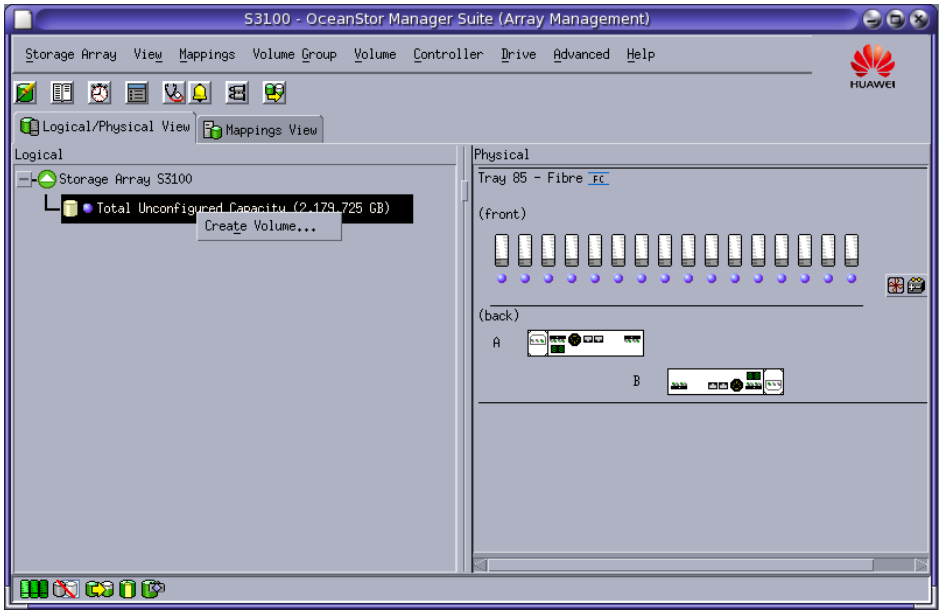


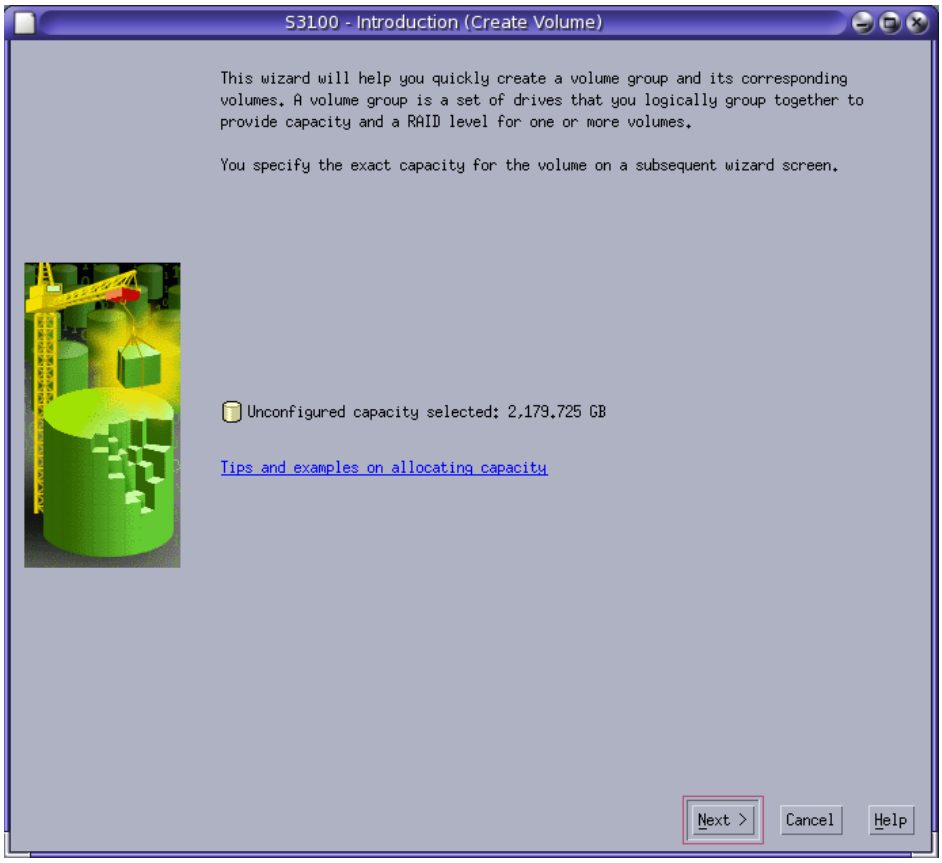


5. Enter **yes** and click **OK** to delete the volume group.

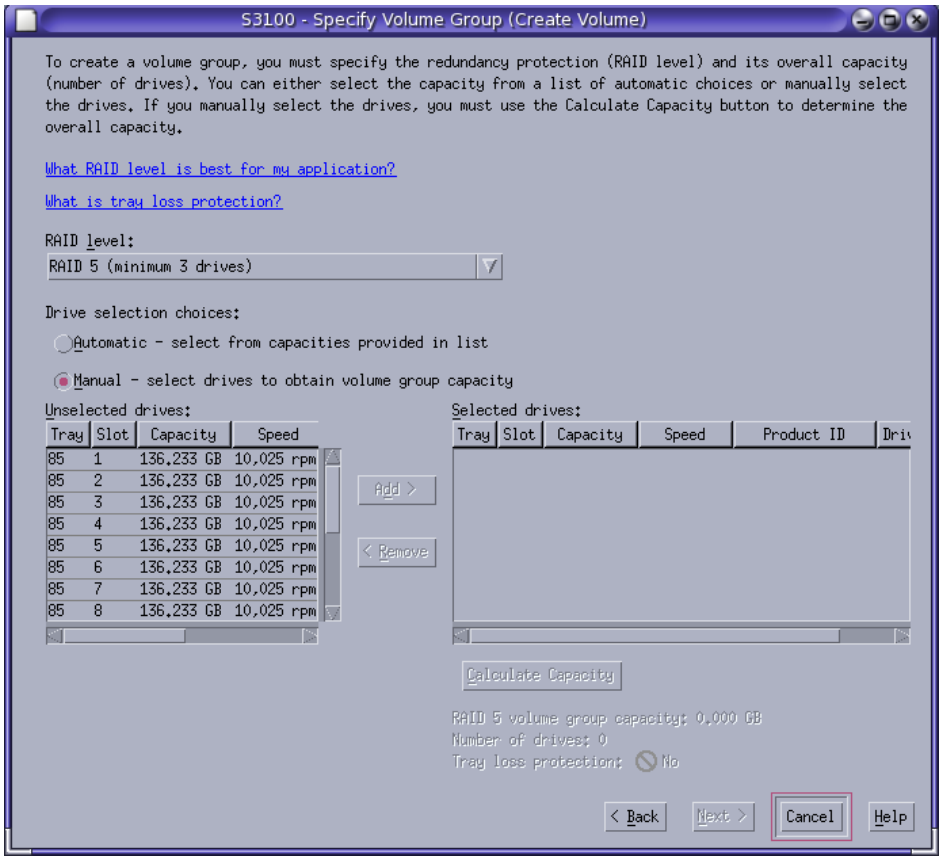


6. Right-click **Total Unconfigured Capacity** and choose **Create Volume** from the shortcut menu.

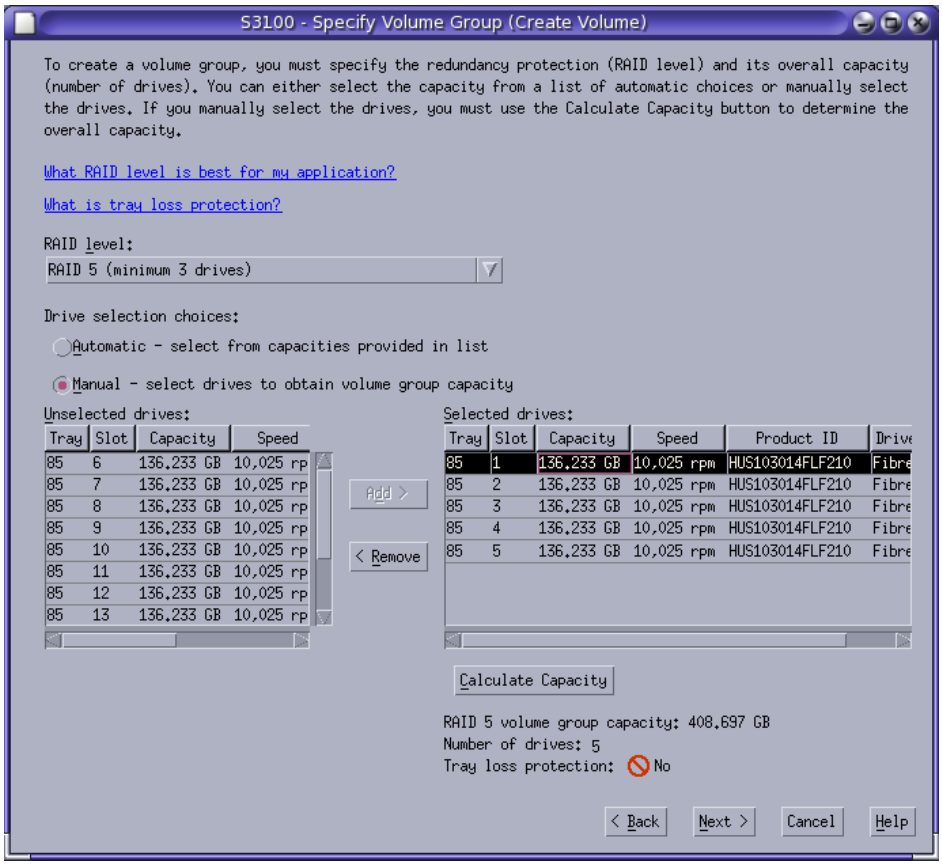




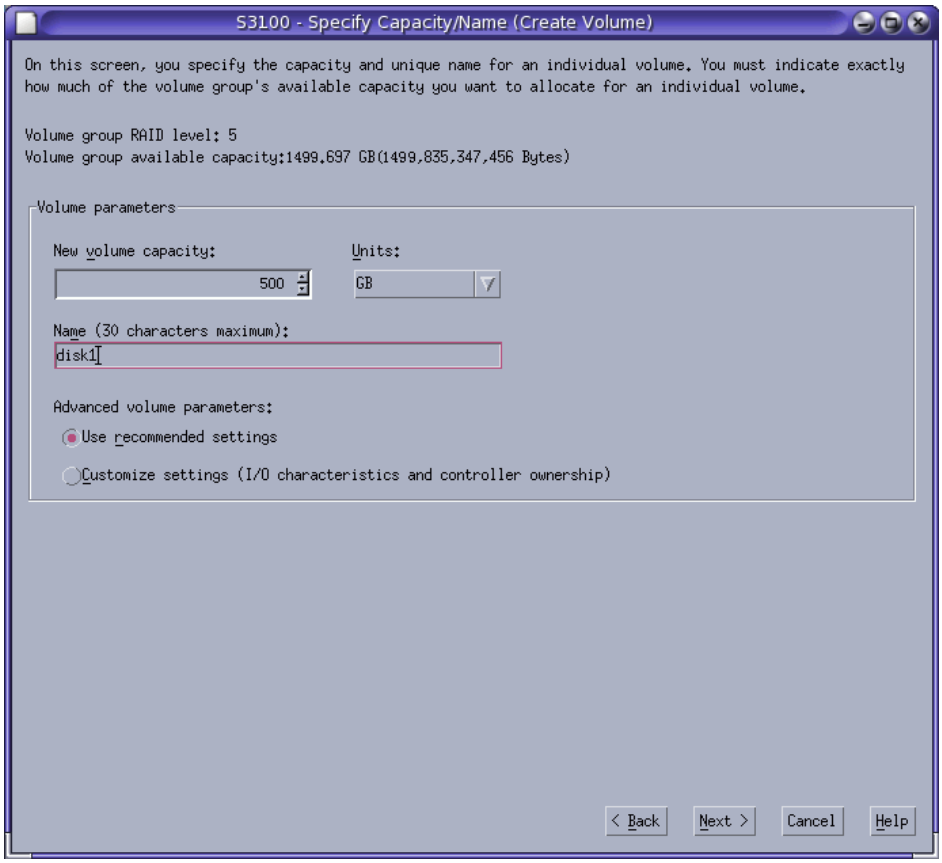
7. Click **Next** to open the dialog box for creating the volume group. Set the parameters as follows:
   - RAID level: **RAID 5 (minimum 3 drives)**
   - Drives selection choices: **Manual-select drives to obtain volume group capacity**



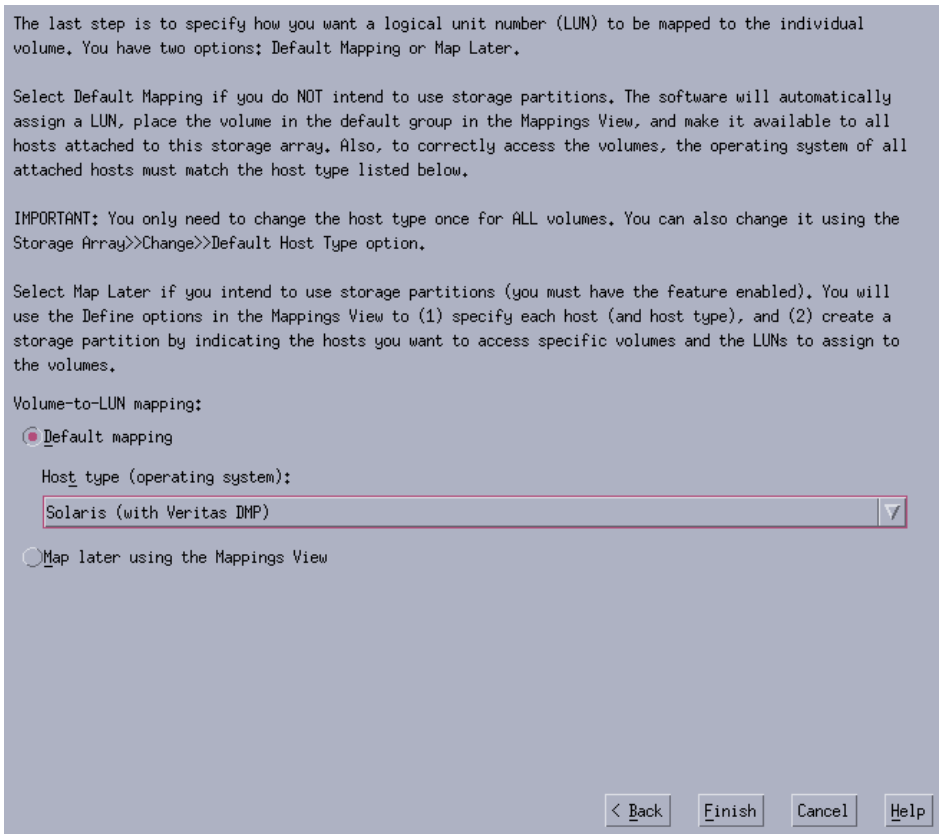
8. Select five disks from **Unselection drives** in the left pane and add them to **Selection drives** in the right pane, as shown in the following figure.



9. Click **Calculate Capacity**.
10. Click **Next>**. In the confirmation dialog box, click **OK**.
11. Set the volume as follows:
    - New volume capacity: **500 GB**
    - Name (30 characters maximum): **disk1**
    - Advanced volume parameters: **Use recommended settings**

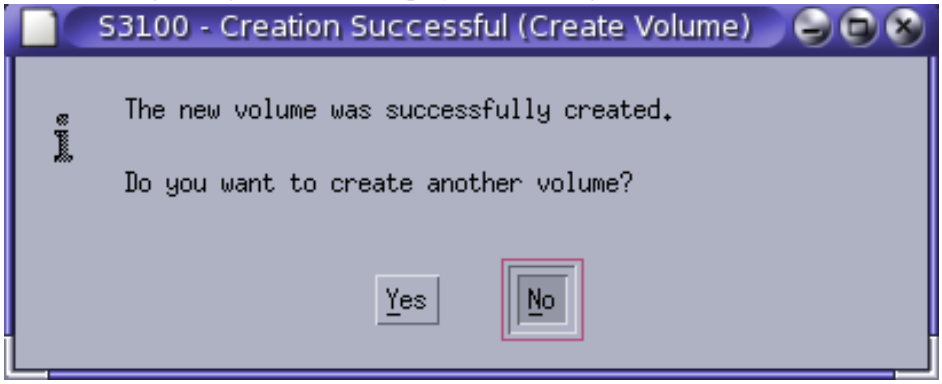


12. Click **Next**.
13. Click the **Default mapping** option button and set **Host type (operating system)** to **solaris (with Veritas DMP)**.



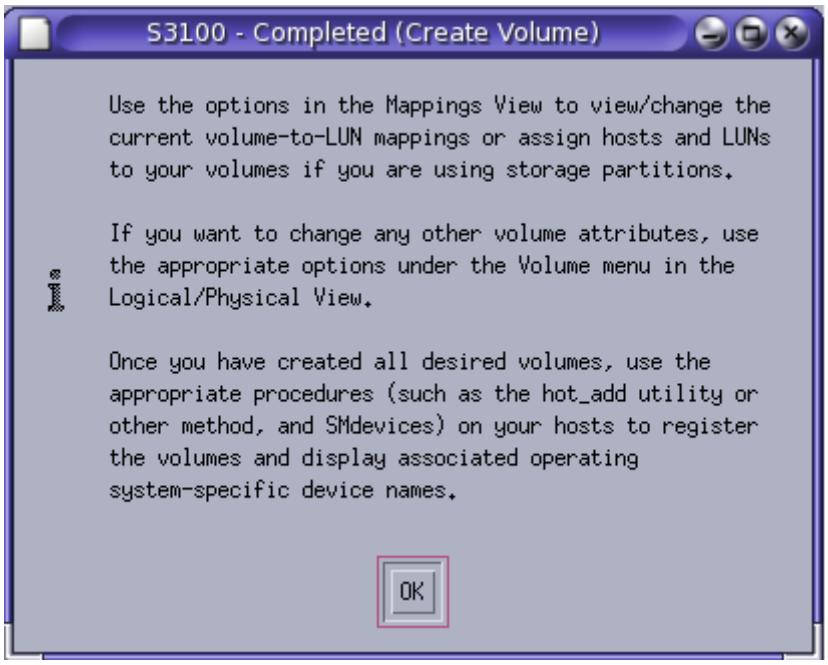
14. Click **Finish**.

    The following dialog box will be displayed indicating that volume disk 1 has been created.

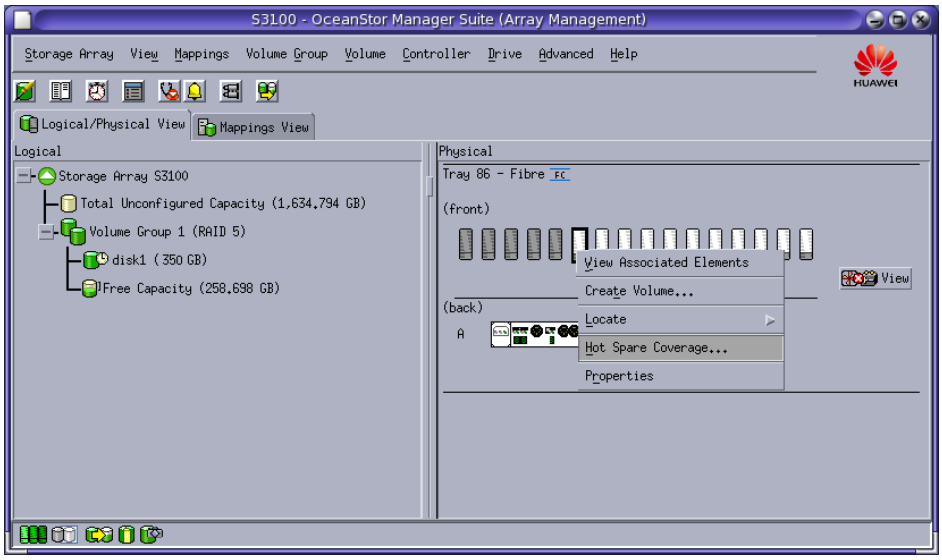


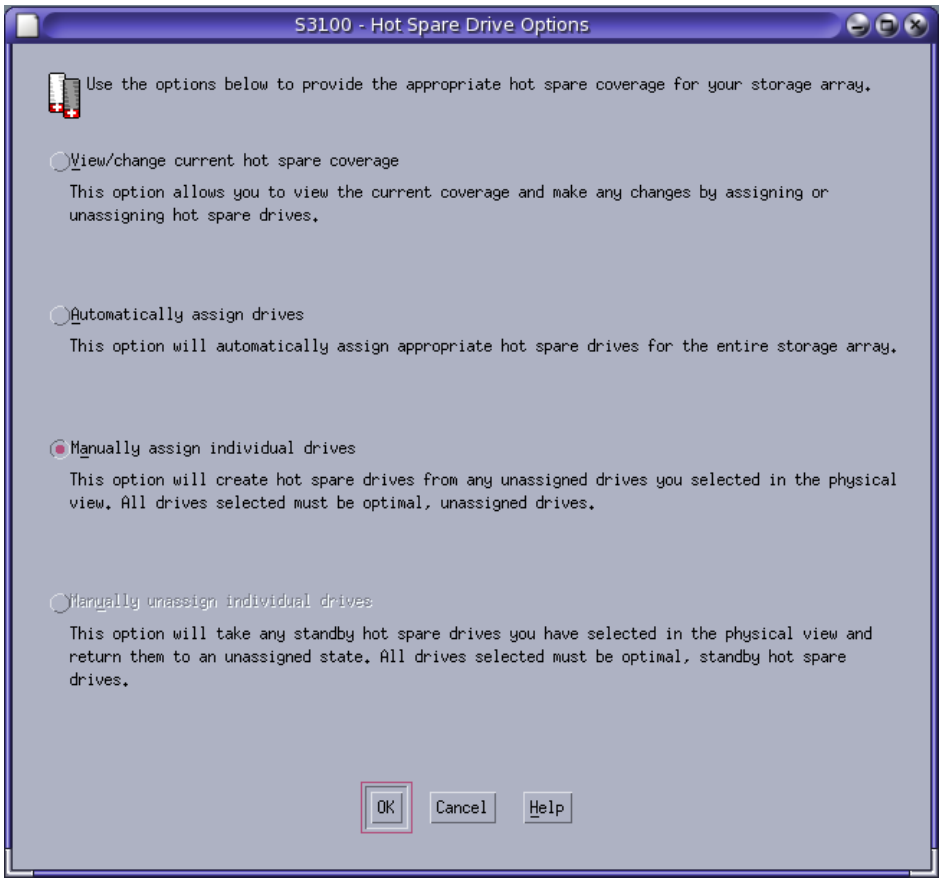
15. Click **No**.

    The **S3100 - Completed (Create Volume)** dialog box will be displayed.



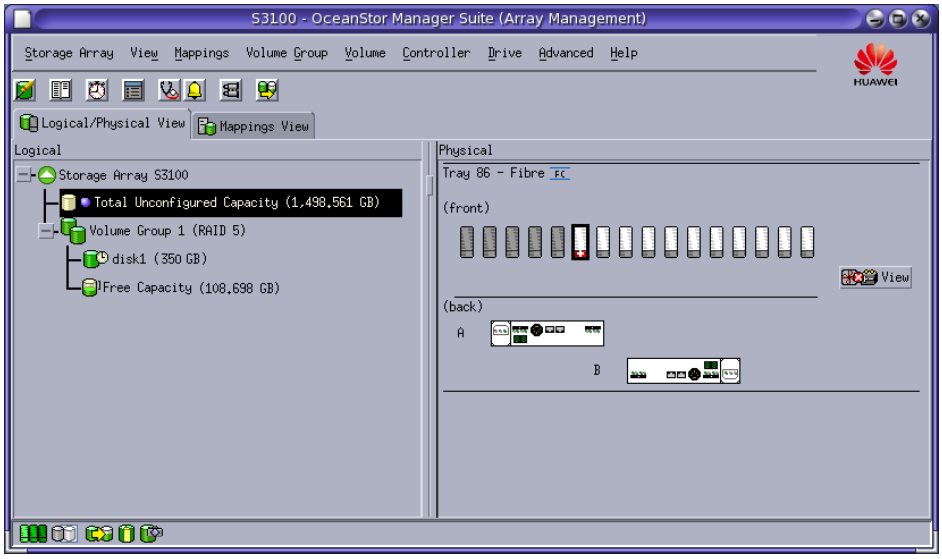
16. Click **OK**.
17. Right-click the sixth disk and choose **Hot Spare Coverage** from the shortcut menu, as shown in the following figure.



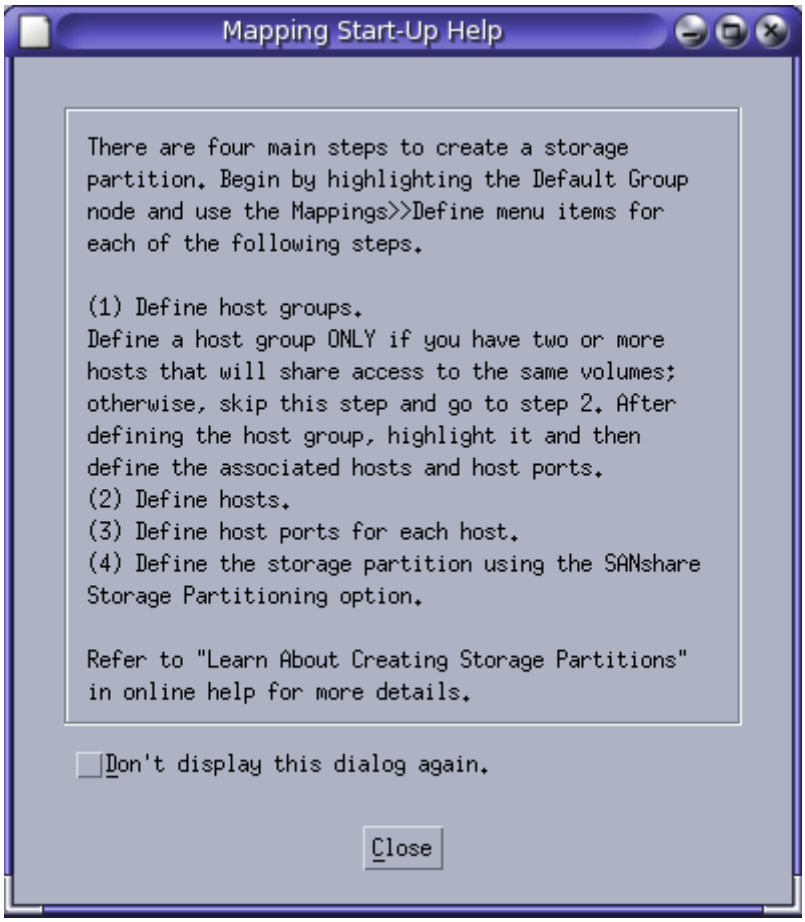


18. Click the **Manually assign individual drives** option button, and click **OK**.

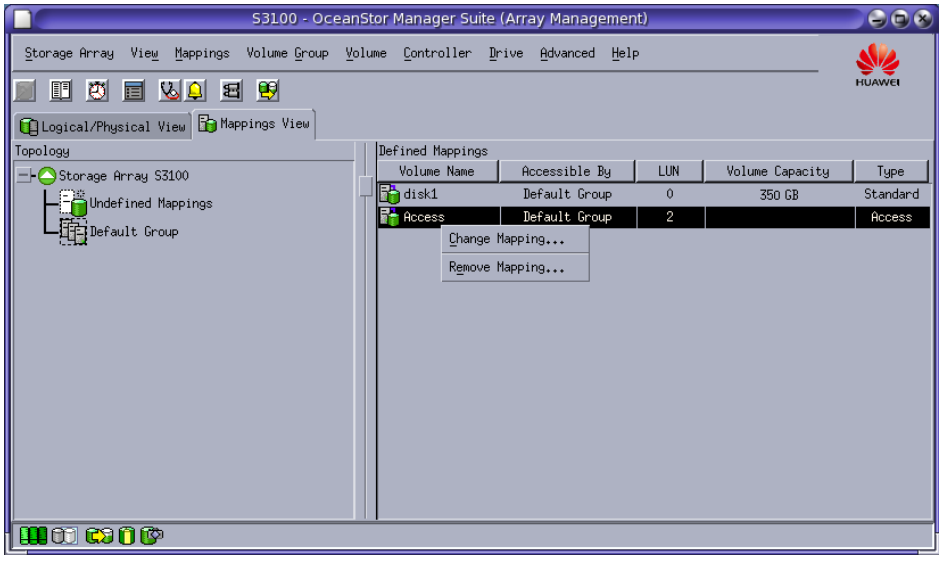
    Configuring the hot-spare disk was successful if a red cross is displayed below the hard disk icon.



19. Click the **Mappings View** tab.



20. In the **Mapping start-up Help** dialog box, click **Close**.
21. **Optional:** If there is a volume named **Access** in the right pane, right-click the volume and choose **Remove Mapping** from the shortcut menu to delete the volume. The configuration is complete.



4 Configure the LUN that maps disk array S3100 on the server.

1. Check the connection of the HBA card.

a. Run the following command to check the connection of the port on the HBA card:
```
# luxadm -e port
```
The following message will be displayed:
```
/devices/pci@0,600000/pci@0/pci@8/pci@0,1/SUNW,qlc@1/fp@0,0:devctl
CONNECTED
/devices/pci@0,600000/pci@0/pci@8/pci@0,1/SUNW,qlc@1,1/fp@0,0:devctl
CONNECTED
```
NOTE

If the HBA card does not work in the connected state, check and ensure the following items:
- The fiber is properly connected to the optical module.
- There is not any damage to the fiber.
- The optical module is properly connected to the HBA card.
- The indicator of the HBA card is functioning properly.

b. Run the following commands to restart the OS of the server and refresh the disk status:
```
# sync;sync;sync;sync
# shutdown -y -g0 -i6
```

c. Run the following command to scan the LUNs that map the S3100 disk array:
```
# format
```
The following message will be displayed:
```
Searching for disks...done

c2t5d0: configured with capacity of 349.99GB
c2t5d1: configured with capacity of 349.99GB

AVAILABLE DISK SELECTIONS:
       0. c1t0d0 <SUN146G cyl 14087 alt 2 hd 24 sec 848>
          /pci@0/pci@0/pci@2/scsi@0/sd@0,0
       1. c1t1d0 <SUN146G cyl 14087 alt 2 hd 24 sec 848>
          /pci@0/pci@0/pci@2/scsi@0/sd@1,0
       2. c1t2d0 <SUN146G cyl 14087 alt 2 hd 24 sec 848>
          /pci@0/pci@0/pci@2/scsi@0/sd@2,0
       3. c1t3d0 <SUN146G cyl 14087 alt 2 hd 24 sec 848>
          /pci@0/pci@0/pci@2/scsi@0/sd@3,0
       4. c2t5d0 <ENGENIO-INF-01-00-0619 cyl 51198 alt 2 hd 128 sec 64>
          /pci@0/pci@0/pci@8/pci@0/pci@9/SUNW,qlc@0/fp@0,0/
ssd@w200500a0b8423e19,0
       5. c2t5d1 <ENGENIO-INF-01-00-0619 cyl 51198 alt 2 hd 128 sec 64>
          /pci@0/pci@0/pci@8/pci@0/pci@9/SUNW,qlc@0/fp@0,0/
ssd@w200500a0b8423e19,1
       6. c3t1d0 <ENGENIO-INF-01-00-0619 cyl 51198 alt 2 hd 128 sec 64>
          /pci@0/pci@0/pci@8/pci@0/pci@a/SUNW,qlc@0/fp@0,0/
ssd@w200400a0b8423e19,0
       7. c3t1d1 <ENGENIO-INF-01-00-0619 cyl 51198 alt 2 hd 128 sec 64>
          /pci@0/pci@0/pci@8/pci@0/pci@a/SUNW,qlc@0/fp@0,0/
ssd@w200400a0b8423e19,1
Specify disk (enter its number):
```

NOTE

- The displayed disk size varies according to the actual size of the disk.
- The disks identified with **<ENGENIO-INF-01-00-0619 .... >** are the LUNs that map the S3100 disk array.
- The scanned number of disks is the product of: the number of local disks, the number of LUNs that map the S3100 disk array, and the number of fiber paths. After the MPxIO multipathing is enabled, the number of disks scanned by the **format** command is equal to the number of LUNs that map the S3100 disk array.
- If the disks that map the S3100 disk array fail to be scanned, run the **devfsadm -C** command first, and the **format** command to scan the required disks. If the disks still cannot be scanned, ensure that the fiber is properly connected.
- Press **Ctrl**+**D** to exit.

5 Label the required disks.

1. Select the disk to be labeled.

   NOTE

   The disk is not labeled if the message "Searching for disks...done" is displayed. In this case, enter the corresponding disk number. For example, enter **4** when the c2t5d0 disk needs to be labeled. The following uses the c2t5d0 disk as an example.

   ```
   c2t5d0: configured with capacity of 349.99GB
   c2t5d1: configured with capacity of 349.99GB
   ```

   The following message will be displayed:

   ```
   Specify disk (enter its number): 4
   selecting c2t5d0
   [disk formatted]
   Disk not labeled.  Label it now?
   ```

2. Enter **y** to label the disk.

   The following message will be displayed:

   ```
   FORMAT MENU:
           disk       - select a disk
           type       - select (define) a disk type
           partition  - select (define) a partition table
           current    - describe the current disk
           format     - format and analyze the disk
           repair     - repair a defective sector
           label      - write label to the disk
           analyze    - surface analysis
           defect     - defect list management
           backup     - search for backup labels
           verify     - read and display labels
           save       - save new disk/partition definitions
           inquiry    - show vendor, product and revision
           volname    - set 8-character volume name
           !<cmd>     - execute <cmd>, then return
           quit
   format>
   ```

3. Enter **disk**.

   The following message will be displayed:

   ```
   AVAILABLE DISK SELECTIONS:
          0. c1t0d0 <SUN146G cyl 14087 alt 2 hd 24 sec 848>
             /pci@0/pci@0/pci@2/scsi@0/sd@0,0
          1. c1t1d0 <SUN146G cyl 14087 alt 2 hd 24 sec 848>
             /pci@0/pci@0/pci@2/scsi@0/sd@1,0
          2. c1t2d0 <SUN146G cyl 14087 alt 2 hd 24 sec 848>
             /pci@0/pci@0/pci@2/scsi@0/sd@2,0
          3. c1t3d0 <SUN146G cyl 14087 alt 2 hd 24 sec 848>
   ```

```
          /pci@0/pci@0/pci@2/scsi@0/sd@3,0
       4. c2t5d0 <ENGENIO-INF-01-00-0619 cyl 51198 alt 2 hd 128 sec 64>
          /pci@0/pci@0/pci@8/pci@0/pci@9/SUNW,qlc@0/fp@0,0/
ssd@w200500a0b8423e19,0
       5. c2t5d1 <ENGENIO-INF-01-00-0619 cyl 51198 alt 2 hd 128 sec 64>
          /pci@0/pci@0/pci@8/pci@0/pci@9/SUNW,qlc@0/fp@0,0/
ssd@w200500a0b8423e19,1
       6. c3t1d0 <ENGENIO-INF-01-00-0619 cyl 51198 alt 2 hd 128 sec 64>
          /pci@0/pci@0/pci@8/pci@0/pci@a/SUNW,qlc@0/fp@0,0/
ssd@w200400a0b8423e19,0
       7. c3t1d1 <ENGENIO-INF-01-00-0619 cyl 51198 alt 2 hd 128 sec 64>
          /pci@0/pci@0/pci@8/pci@0/pci@a/SUNW,qlc@0/fp@0,0/
ssd@w200400a0b8423e19,1
Specify disk (enter its number):
```

4. Perform **5.1** to **5.3** to label the rest of the disks.
5. Press **Ctrl**+**D** to exit.

----End

I Acronyms

A	
ACL	Access Control List
ASCII	American Standard Code for Information Interchange
C	
CD-ROM	Compact Disc-Read Only Memory
CPU	Central Processing Unit
D	
DC	Data Center
DCN	Data Communication Network
DHCP	Dynamic Host Configuration Protocol
E	
ESN	Equipment Serial Number
F	
FTP	File Transfer Protocol
I	
ID	Identity
iMAP	Integrated Management Application Platform
IP	Internet Protocol

IPMP	IP Network Multipathing
K	
KVMS	Keyboard, video, mouse (KVM) switch
L	
LCT	Local Craft Terminal
LAN	Local Area Network
M	
MML	Human-Machine Language (formerly Man-Machine Language)
MPLS	MultiProtocol Label Switching
MA	Media Service Access
MAC	Media Access Control
MAN	Metropolitan Area Network
MAU	Medium Attachment Unit
N	
NBI	Northbound Interface
NE	Network Element
NIC	Network Information Center
NMS	Network Management System
NTP	Network Time Protocol
O	
OEM	Original Equipment Manufacturer
OS	Operation System
OSS	Operation Support System
P	
PPP	Peer-Peer Protocol
PSTN	Public Switched Telephone Network

PVC	Permanent Virtual Circuit
R	
RAID	Redundant Array of Independent Disks
S	
SCSI	Small Computer Systems Interface
SDH	Synchronous Digital Hierarchy
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSH	Secure Shell
T	
TCP	Transport Control Protocol
TFTP	Trivial File Transfer Protocol
U	
UDP	User Datagram Protocol
UPS	Uninterrupted Power Supply
X	
XML	Extensible Markup Language