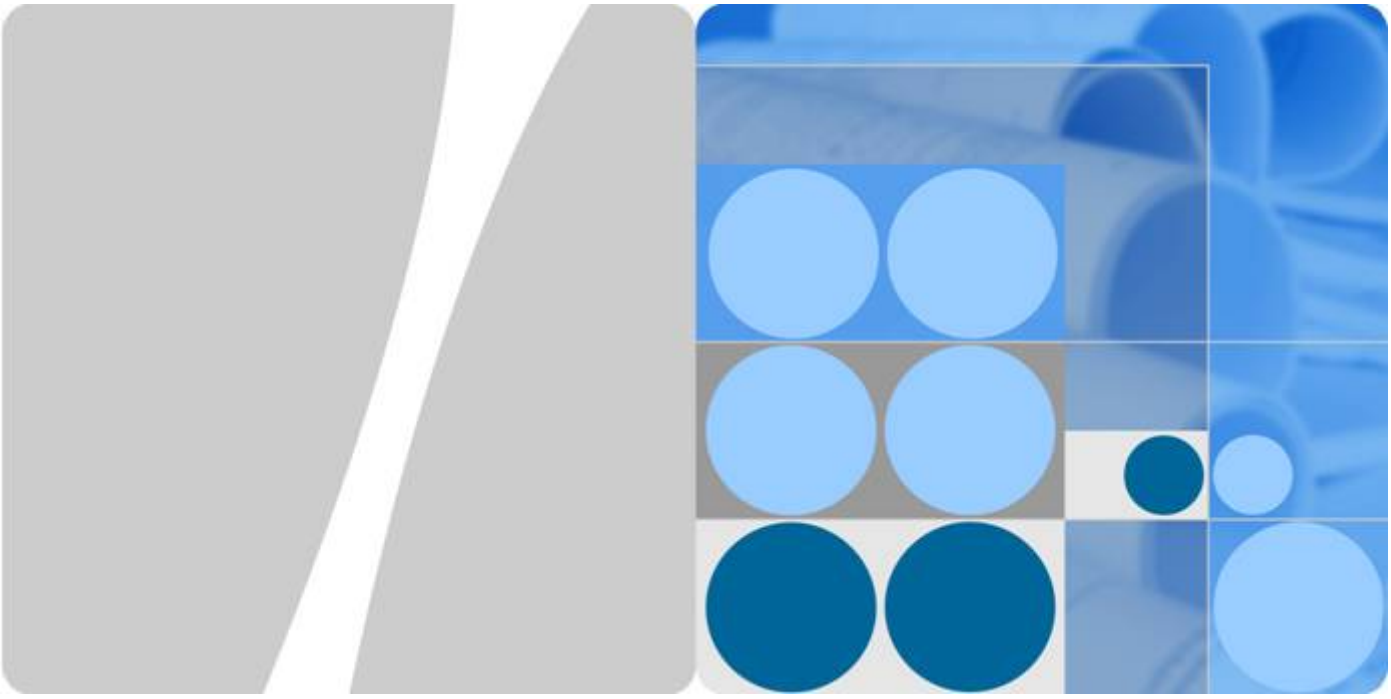


iManager U2000 Unified Network Management System

V100R002C01

# High Availability System (Veritas) Software Installation Guide (SUSE Linux)

Issue 05

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 SUSE Linux 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 05 (2010-11-19)

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 SUSE Linux operating system (OS).

**CAUTION**

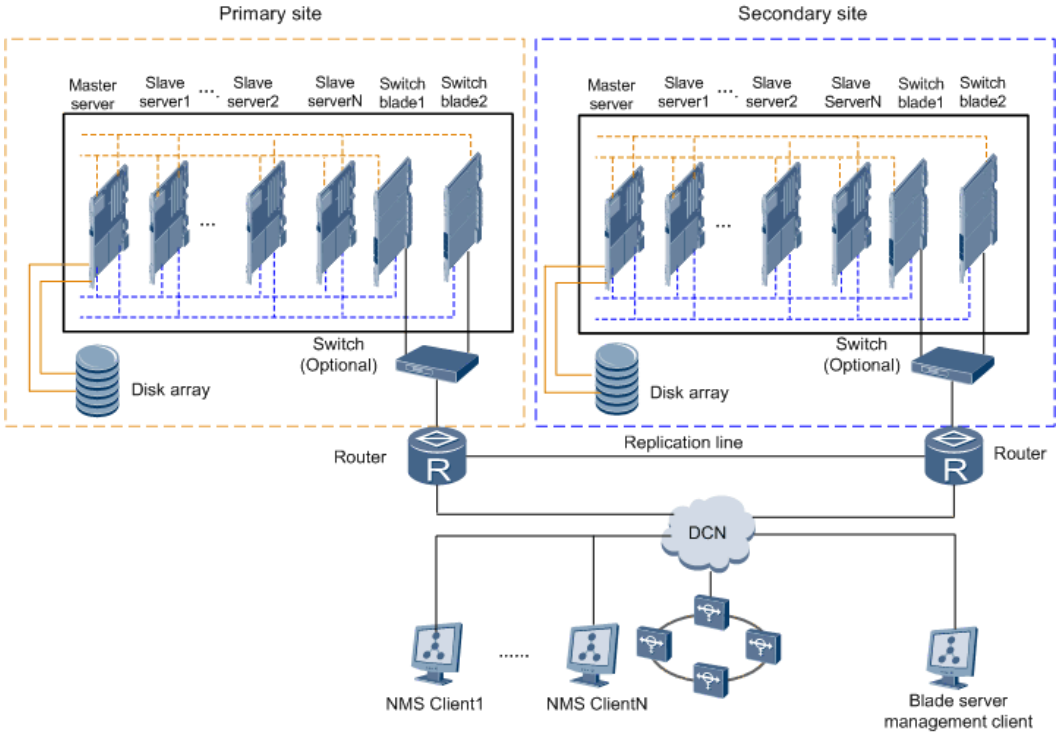
Servers are pre-installed with software from Huawei and can be commissioned immediately. For more information, see the *iManager U2000 Commissioning Guide*. If servers are purchased from other suppliers, install software according to the U2000 deployment.

Definitions for terms as used in this document before introducing the 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 SUSE Linux 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.
- Master server: A master server refers to the server where the core processes of the U2000 and database service are installed and deployed.

- Slave server: It is used for a distributed system. A slave server is used to share the load of the master server. It is placed at the same site of the master server and mounted to the master server of the distributed system.
- Distributed system: The distributed system includes the master server and slave server. The master server and slave server constitute a site that takes on the functions of the U2000 server. The master server is the core of the distributed system. The database server and the core components of the U2000 run on the master server. The non-core components of the U2000 are running on the slave server, with the purpose of reducing the CPU usage and memory usage of the master server so that the load on the master and slave servers can be balanced. If the blade server has only one blade, the Slave server is not available.

**Figure 1-1** Networking diagram of the high availability system (SUSE Linux-distributed)




- 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.

  In a distributed system, the deployment packages of a component may be deployed on different computers.

  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 the process of installing a high availability system (Veritas hot standby) of the U2000 that is deployed in distributed mode.

Before installing a U2000 high availability system (Veritas hot standby), you must install the primary and secondary sites, and then connect the primary site and secondary site to form a high availability system. Assume that the on-site server has been preinstalled before delivery, you need to perform only the relevant commissioning operations (for example, changing the IP address and time zone) according to planning, and then connect the primary site and secondary site if the network between the primary and secondary sites is normal.

**Table 2-1** lists the topics that you can refer to at each installation stage as well as the time required for each stage.

**CAUTION**

The OSs of the master server and slave server on the primary and secondary sites can be installed and configured at the same time.

If the blade server has only one blade, skip the operation for the slave server.

**Table 2-1** Description of the process of installing a HA system (Veritas hot standby) of the U2000 that is deployed in distributed mode

| Stage | Description | Reference Topics | Time Required (Minutes) |
|---|---|---|---|
| 1 | Prepare for the installation. | **3 Installation Preparations** | 30 |
| 2 | Configure server hardware. | **4 Configuring Hardware** | 60 |
| 3 | Power on the system. | **5 Powering On a Server** | 20 |

| Stage | Description | Reference Topics | Time Required (Minutes) |
|---|---|---|---|
| 4 | Install SUSE Linux OSs on the primary and secondary sites. | **6 Installing the SUSE Linux OS and Its Patches by Using the Quick Installation CD-ROM** | 100 |
| 5 | Install the U2000 on the primary and secondary sites. | **7 Installing U2000 Software** | 230 |
| 6 | Connect the primary site and secondary site. | **8 Connecting the Primary and Secondary Sites** | 20 |
| 7 | (Optional) Install a 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 the high availability system (SUSE Linux-distributed), ensure that associated software and hardware are ready and the environment is normal.

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 (SUSE Linux-distributed).

## Requirements for Hardware Configuration

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

**Table 3-1** Configuration requirements on server hardware

| Hardware | Description |
|---|---|
| Blade server | ATAE-T8223 cabinet + BH23C server blade (CPU: 2 x Intel Xeon Quad Core 2.13 GHz, memory: 16 GB, disk: 2 x 146 GB, network port: 4 or more) |
| | Blade center E cabinet + IBM HS22 (CPU: 2 x Intel Xeon Quad Core 2.4 GHz or greater, memory: 16 GB, disk: 2 x 146 GB, network port: 4 or more) |
| | Blade center E cabinet + IBM HS21 (CPU: 2 x Intel Xeon Quad Core 2.5 GHz, memory: 16 GB, disk: 2 x 146 GB, network port: 4 or more) |
| Disk array | OceanStor S2600: 6 x 300 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 (SUSE Linux-distributed).

## Requirements for Software Configuration

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

**Table 3-2** Configuration requirements on the server software

| Software | Description |
|---|---|
| OS | SUSE Linux Enterprise Server 10 with SP3 |
| Veritas software | Recommended configurations: Veritas 5.1 |
| Database | Oracle 11g Enterprise Edition Release 11.1.0.7 |
| NMS software | U2000 software<br>**NOTE**<br>The U2000 software can be installed on the OS with either the English version or simplified Chinese version. |

**NOTE**

The Veritas software can be installed only on the master server of the primary and secondary sites.

# 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

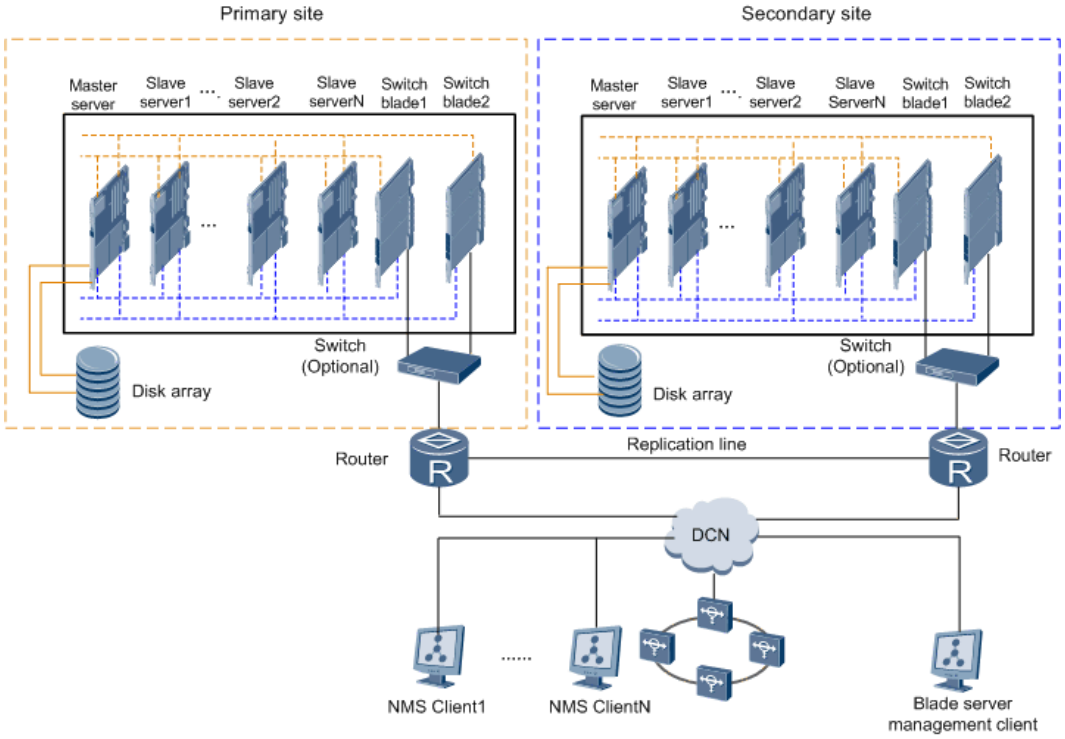
| Check Item | Requirement |
| --- | --- |
| Temperature | The required temperature range must be from 15°C to 30°C for long-term working conditions and from 0°C to 45°C for short-term working conditions |
| Humidity | The required humidity range must be from 40% to 65% in long-term working conditions 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. |
| 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 (SUSE Linux-distributed). Before installing a high availability system (SUSE Linux-distributed), you must get familiar with the networking structure of the high availability system (SUSE Linux-distributed).

The following figure shows the networking structure of a high availability system (SUSE Linux-distributed).

**Figure 3-1** Networking structure of the high availability system (SUSE Linux-distributed)




## Networking Description of the high availability system (SUSE Linux-distributed)

A high availability system (SUSE Linux-distributed) is network management system featuring high reliability and is composed of primary and secondary sites. Integrating the Veritas remote hot standby and switching technologies on the basis of a U2000 single-server system, a high availability system (SUSE Linux-distributed) achieves real-time data backup and dynamically monitors the running status of the peer site. If the primary site becomes faulty, the high availability system (SUSE Linux-distributed) can automatically switch to the secondary site, thereby ensuring the uninterrupted network monitoring by the U2000.

The communication bandwidth between the primary and secondary sites must be no less than 2 Mbit/s for networking.

- In actual networking, the cables indicated by dotted lines in the preceding figure do not need to be connected manually, and the connection is implemented inside the server chassis. Details about the structure of a blade server chassis and the communications between a public network and private network are as follows:
  - Two switching planes are inside the chassis of an ATAE blade server: base plane and fabric plane. The ATAE blade server is connected to a public network by the base plane. The fabric plane is used for internal communications inside a distributed system.
  - Four modules are inside the chassis of an IBM blade server: I/O module 1, I/O module 2, I/O module 3, and I/O module 4. The IBM blade server is connected to a public network by I/O module 1 and I/O module 2. I/O module 3 and I/O module 4 are used for communications inside a distributed system.
- The network interfaces for the private network configuration and those for the public network configuration must be connected to different switches.

- A single site is composed of one master server, multiple slave servers, and disk arrays. The number of slave servers is no more than five. Each server corresponds to one blade server in the shelf.
- The disk array is mandatory and used to store database data to improve database performance.
- The high availability system (SUSE Linux-distributed) communicates with the external, such as clients and equipment, using a public network.

### Description About Communications in a high availability system (SUSE Linux-distributed)

- The primary and secondary sites communicate with each other using a DCN.
- The master server and slave server communicate with each other using a private network. By default, the private network is configured with bond to ensure that the master server and slave server communicate with each other properly in the case of an NIC fault.
- A U2000 client and the network management system maintenance suite client communicate with the master server using a DCN. You must select the public IP address of the master server when logging in to a U2000 client or the network management system maintenance suite client. Bond is configured for the public network by default to ensure the normal communication between the master server and slave server on the active site when the NIC is faulty, on the master and slave servers, bond is configured for the public network by default.
- NEs and the upper-layer NMS (OSS) communicate with the primary and secondary sites, including the master server and slave server, using a DCN.

## 3.4 Collecting Installation Information

This topic describes how to collect installation information. Before installing a high availability system (SUSE Linux-distributed), 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 | master server | Primaster | |
| | | slave server | PrislaveN | |
| Secondary Site | Host name | master server | Secmaster | |
| | | slave server | SecslaveN | |

**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
```

**NOTE**

- The preceding planned host names are examples only. You need to plan host names based on the actual conditions and customer preference.
- N in the preceding table represents the serial number of the slave server. The host names of the slave servers can be increased in sequence along with the increase of the number of slave servers. For example, Prislave 1. The number of slave servers is equal to or less than five.

**Table 3-5** shows the sample planning of the IP addresses of control cards on the equipment.

**NOTE**

The IP address is in the **IP address/subnet mask/gateway** format.

**Table 3-5** Controller IP address list

| Site | Item | | Example | Plan |
|---|---|---|---|---|
| Primary Site | Blade server | IP address for the network interface on the SMM | ● ATAE blade server: 129.9.1.102/255.255.255.0/129.9.1.254<br>● IBM blade server: 192.168.70.125/255.255.255.0/192.168.70.1 | |
| | Disk array | Primary controller IP address | 129.9.1.103/255.255.255.0/129.9.1.254 | |
| | | Secondary controller IP address | 129.9.1.104/255.255.255.0/129.9.1.254 | |
| Secondary Site | Blade server | IP address for the network interface on the SMM | ● ATAE blade server: 129.9.1.105/255.255.255.0/129.9.1.254<br>● IBM blade server: 192.168.70.126/255.255.255.0/192.168.70.1 | |
| | Disk array | Primary controller IP address | 129.9.1.106/255.255.255.0/129.9.1.254 | |
| | | Secondary controller IP address | 129.9.1.107/255.255.255.0/129.9.1.254 | |

Table 3-6 shows the planning of system IP addresses of the master and slave servers on the primary and secondary sites.

**Table 3-6** Planning of system IP addresses of the master and slave server

| Site | Item | Example | Plan |
|---|---|---|---|
| Primary Site | System network interface | eth0 | |
| | System IP address | ● master server: 129.9.1.30/255.255.255.0/129.9.1.254<br>● slave server: 129.9.1.31/255.255.255.0/129.9.1.254 | |
| | Private network segment | 192.168.100.0 | |
| Secondary Site | System network interface | eth0 | |
| | System IP address | ● master server: 129.9.1.40/255.255.255.0/129.9.1.254<br>● slave server: 129.9.1.41/255.255.255.0/129.9.1.254 | |
| | Private network segment | 192.168.101.0 | |

**CAUTION**

If multiple distributed NMSs are installed in a shelf, ensure that the private network segments of the distributed NMSs are different from one another.

**Table 3-7** Route list

| Item | Example | Plan |
|---|---|---|
| Routing network segment 1 | 129.9.10.0\255.255.255.0 | |

| Item | Example | Plan |
| --- | --- | --- |
| 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 3-8** Time zone and time list

| Item | Example | Plan |
| --- | --- | --- |
| Time zone | **Asia** > **Shanghai** | |
| Time | 14:00 | |

**Table 3-9** User and password list

| User | Example | Plan |
| --- | --- | --- |
| Password for the **root** user for the ATAE blade server management board | huaweiosta | |
| **USERID** for the user for the IBM blade server management board | changeme | |
| OS user **root** | root | |
| OS user **oracle** | oracle | |
| Database superuser (sa) | changeme | |
| Database user | NMSuser | |
| U2000 user **admin** | admin123 | |
| network management system maintenance suite user **admin** | admin | |
| VCS Client User **admin** | password | |

NOTE

No database user is available for a slave server.

If multiple U2000s are installed in a subrack, setting different passwords for database users is recommended.

**Table 3-10** Quantity list of configured components and instances

| Example | Plan |
| --- | --- |
| ● One instance for SDH NE management<br>● One instance for PTN NE management<br>● One instance for router NE management<br>● ... | |

**Table 3-11** Installation path list

| Item | Installation Path |
| --- | --- |
| NMS software | /opt/U2000 |
| Oracle database software | /opt/oracle |

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 **I Planning Disk Partitions**.

# 3.5 Checking Required Software

This topic describes how to verify that the software meets U2000 installation requirements.

The U2000 can be installed by using software packages or DVDs, as follows:

- 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 SUSE Linux OS installation DVD and software packages are on-hand.

**Perform the following operations:**

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 you use the download tool (for example, Flashget). If you use Windows Internet Explorer, some software packages may be renamed automatically after being downloaded to the local computer. In this case, you must manually 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.4.13 How to Check Downloaded Software Packages by Using MD5 Software**.
5. Use the WinRAR to decompress the U2000*Version*_server_db_sles_x64.part1.rar and U2000*Version*_server_db_sles_x64.part2.rar software packages. The filename after decompression is U2000***version***_server_db_sles_x64.tar.

**NOTE**

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

**Table 3-12** Software package list

| Software | Medium Name | Description |
|---|---|---|
| SUSE Linux OS installation DVD | Install the SUSE Linux OS by using the quick installation DVD or the standard installation DVD.<br>● Quick installation DVD: U2000***version***_ server_os_sles_x64_dvd1<br>● Standard installation DVD: SUSE Linux 10 Enterprise Server 10 SP3 | **It must be available.** It is used to install the SUSE Linux OS. |
| Database software package | Database software package:U2000***version***_ server_db_sles_x64.tar<br>**NOTE**<br>Because the database software package is too large, it is decompressed and divided into the following two packages:<br>1. U2000*Version*_ server_db_sles_x64.part1.rar<br>2. U2000*Version*_ server_db_sles_x64.part2.rar | **It must be available.** It is used to install the database. |

| Software | Medium Name | Description |
| --- | --- | --- |
| Veritas software | 1. Veritas software installation package: veritas5.1_sles_x64.tar.gz<br>2. Veritas patch package:U2000***version***_ server_veritas5-1_patch_sles_x64.tar | **It must be available.** It is used to install the Veritas. |
| U2000 server software | Basic component:U2000***version***_ server_nmsbase_sles_x64.tar | **It must be available.** It is used to install the U2000. |
| | Core component:U2000***version***_ server_nmscore_sles_x64.tar | **It must be available.** It is used to install the U2000. **It must be available.** |
| | Transport component:U2000***version***_ server_nmstrans_sles_x64.tar | **It is required only if the U2000 needs to manage Huawei transport equipment**. Huawei transport equipment includes:<br>● MSTP equipment<br>● WDM equipment<br>● NA WDM equipment<br>● Submarine equipment<br>● RTN equipment<br>● PTN equipment |
| | IP component:U2000***version***_ server_nmsip_sles_x64.tar | **It is required only if the U2000 needs to manage Huawei IP equipment**. Huawei IP equipment includes:<br>● Routers<br>● Switches<br>● Metro service equipment<br>● Broadband access equipment<br>● VoIP gateways<br>● Firewalls<br>● Service inspection gateway<br>● SVN equipment |
| | Access component:U2000***version***_ server_nmsaccess_sles_x64.tar | **It is required only if the U2000 needs to manage Huawei access equipment**. Huawei access equipment includes:<br>● FTTx equipment<br>● MSAN equipment<br>● DSLAM equipment |

## Using DVDs

Before installing the U2000 by using DVDs, ensure that the following DVDs are available.

**Table 3-13** DVD list

| Software | DVD Name |
| --- | --- |
| SUSE Linux OS installation DVD | Install the SUSE Linux OS by using the quick installation DVD or the standard installation DVD.<br>● Quick installation DVD: U2000***version***_server_os_sles_x64_dvd1<br>● Standard installation DVD: SUSE Linux 10 Enterprise Server 10 SP3 |
| Database software DVD | U2000***version***_server_db_sles_x64_dvd3 |
| Veritas software DVD | 1. Veritas software installation DVD: Storage Foundation and HA Solutions 5.1 for SuSE Linux<br>2. Veritas patch DVD: U2000***version***_server_patch_sles_x64_dvd2 |
| U2000 server software DVD | U2000***version***_server_nms_sles_x64_dvd4 |

# 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

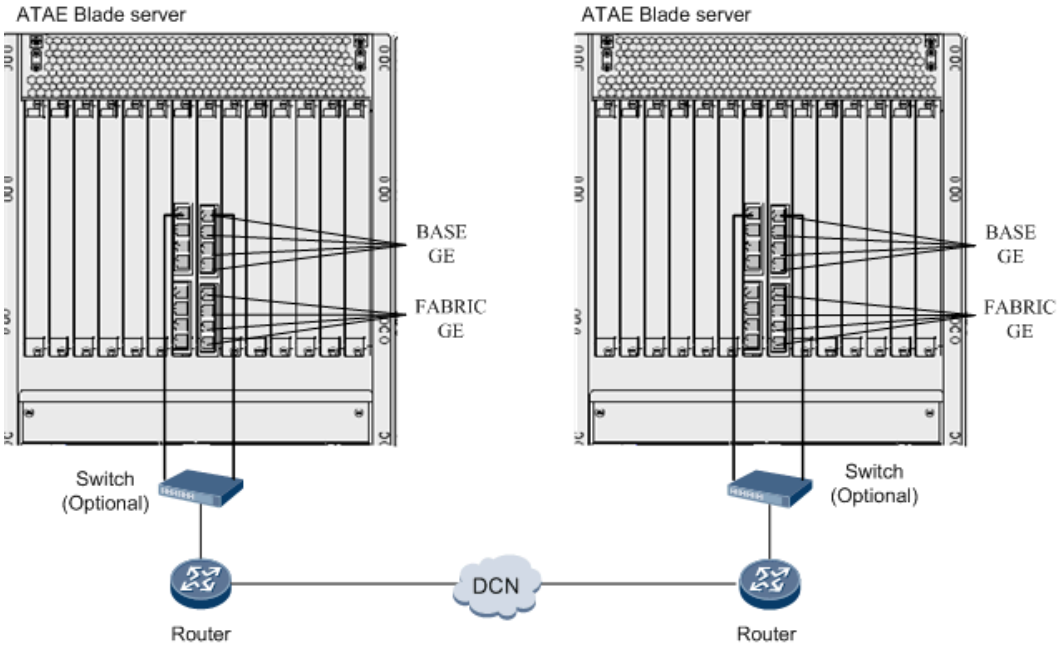
1. Ensure that the power cables and ground wires for all components are tightly connected and in good contact and that the polarities are properly placed.
2. Ensure that all cables are bundled and free of visible damage.
3. Check whether the label (slot x, shelf x) of the associated slot is available on the card.
   If not, attach a label (slot x, shelf x) to the card.

   **NOTE**

   Labels are used to identify the mappings between cards and slots after U2000 installation.
4. Check hardware connections and network cable connections according to the hardware connection diagram.

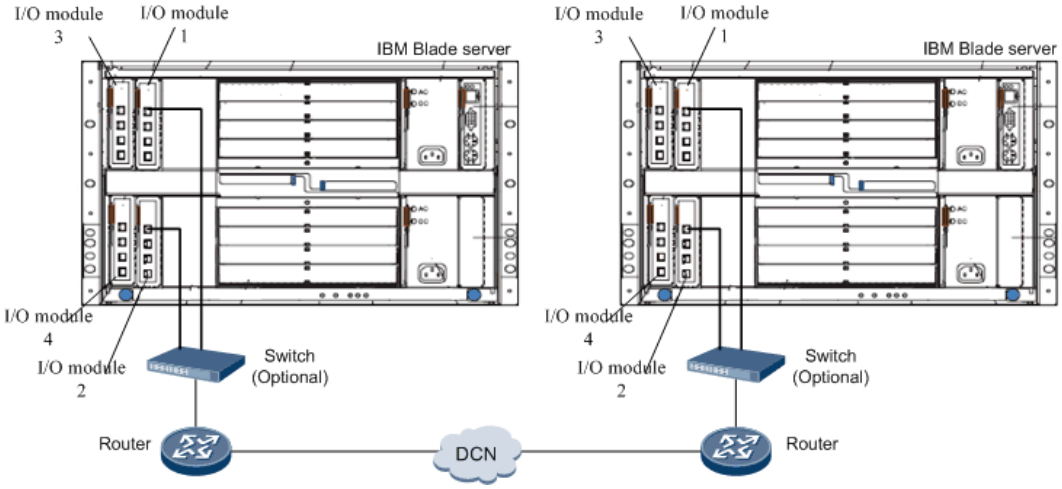
- The ATAE blade server is connected to the external network through the base plane of the switching board. The following figure shows how to connect the cables.

**Figure 3-2** Connecting the ATAE blade server to the public network through the switching board




- The IBM blade server is connected to the external network through I/O module 1 or I/O module 2. The following figure shows how to connect the cables.

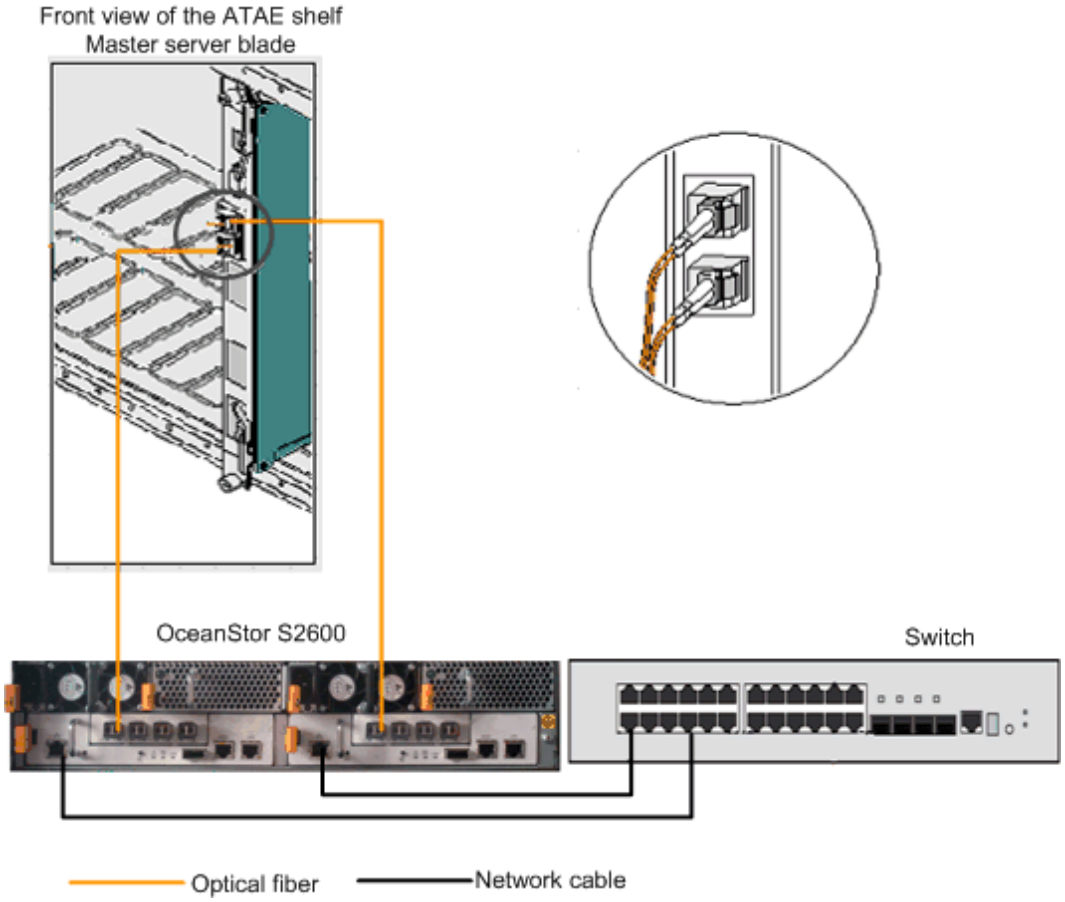
**Figure 3-3** Connecting the IBM blade server to the public network through the switching board




5 Check the connection cables of blade server and the disk array against the hardware connection diagram.

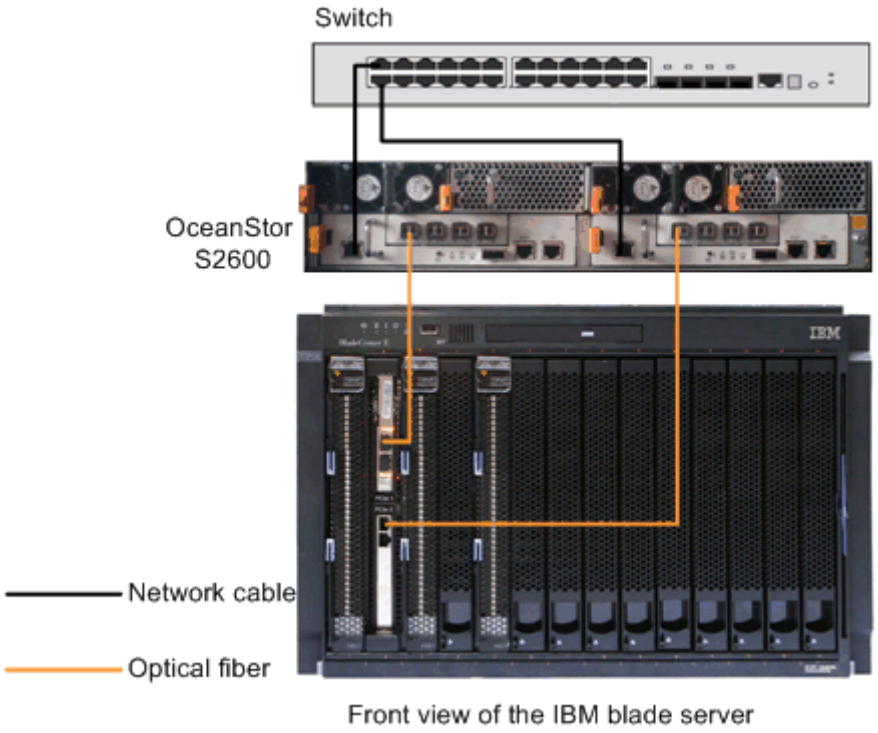
- The ATAE blade server is connected to a disk array using fibers, as shown in the following figure.

**Figure 3-4** Diagram of the connection between the ATAE blade server and a disk array




- The IBM blade server is connected to a disk array using fibers, as shown in the following figure.

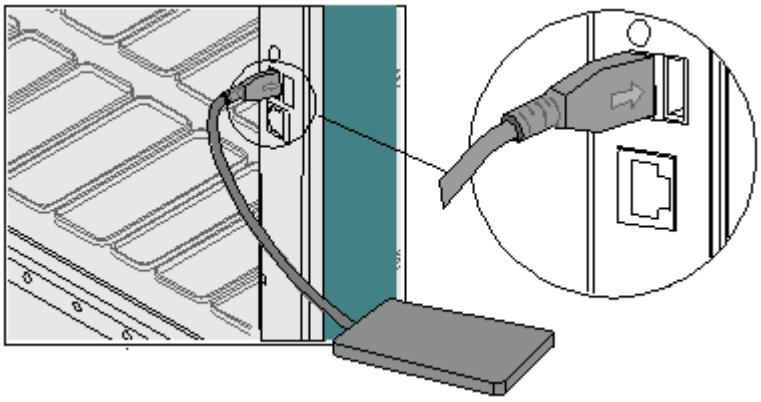
**Figure 3-5** Diagram of the connection between the IBM blade server and a disk array




6 **Optional:** If the blade server is the ATAE blade server, check the connection between the ATAE blade server card and the USB drive.

The following figure shows the connection between the ATAE server card and the USB drive. After the card and the USB drive are connected, insert a disk to check the disk reading indicator. If the indicator is green and flashes, the drive works properly.

**Figure 3-6** Diagram of the connection between the ATAE server card and the USB drive



7 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.

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

**9** 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 the U2000 installation DVD. Contact Huawei engineers for the application of the U2000 license according to the contract number and ESNs of the master servers 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 use the same U2000 license. When applying for a license, you must save the ESNs of the master servers on the primary and secondary sites separately.

## Procedure

**1** Obtain the contract number.

**2** View the ESNs of the master servers on the primary and secondary sites by using the ESN tool.

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

**NOTE**

Make the following preparations:

- Obtain the ESN tool software package named U2000***version***_ESN_sles_x64.tar.
- Copy the ESN tool software package to a PC.

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 master server 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 ESNs of the master servers on 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 Hardware

## About This Chapter

This topic describes how to configure hardware. Before installing the U2000, you must set IP addresses for the remote management console and the disk array controller on the blade server.

# 4.1 Configuring the Remote Management Console of an IBM Blade Server

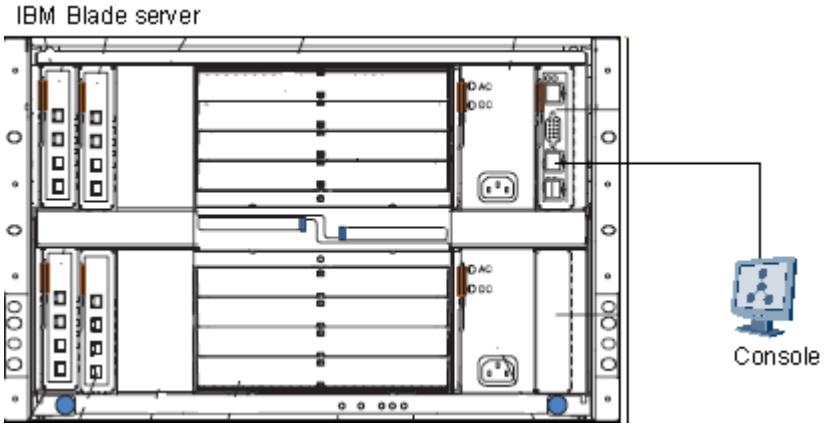
This topic describes how to configure the remote management console of an IBM blade server. After that, you can remotely maintain and manage the IBM blade server through the Internet Explorer.

## Prerequisite

The PC where the Windows OS, and JRE1.4.2_08 or later are installed must be available.

## Procedure

1. Connect the control network port of the management module of the IBM blade server to the network port on the PC with a network cable, as shown in the following figure.

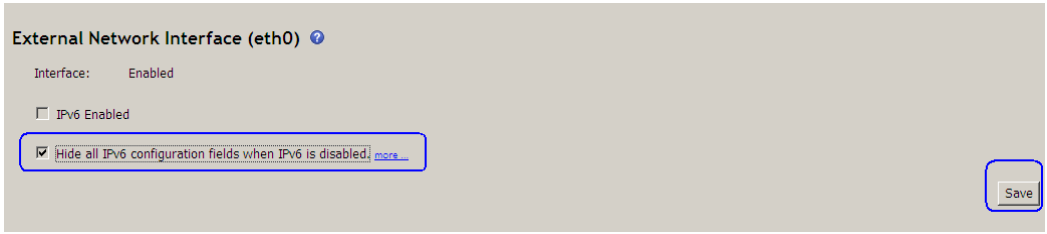



2. On the PC, modify the IP address and subnet mask of the network adapter that is connected to the network port of the management module of the IBM blade server. Modify the IP address to *192.168.70.xx*, for example, *192.168.70.100*, and modify the subnet mask to *255.255.255.0*.
3. Open an Internet Explorer window. In the address bar, enter the IP address **http://192.168.70.125**. Then, the login web page of the IBM management module is displayed.
4. Enter the default user name **USERID** and initial password **PASSW0RD**, and click **Log In**.

**CAUTION**

When you enter the initial password, note that the character after letter "W" is a number "0", but not a letter "O".

5. Click **Exit Wizard** in the **Advanced Management Module Configuration Wizard** dialog box, and the click **OK** and the management page is displayed.
6. Choose **MM Control** > **Network Interfaces**. The configuration page is displayed.
   1. Select **Hide all IPv6 configuration fields when IPv6 is disabled**.
   2. After you set the parameters, click **Save** to save the settings.




7 Set the parameters by referring to **Table 4-1**. After you set the parameters, click **Save** to save the settings.

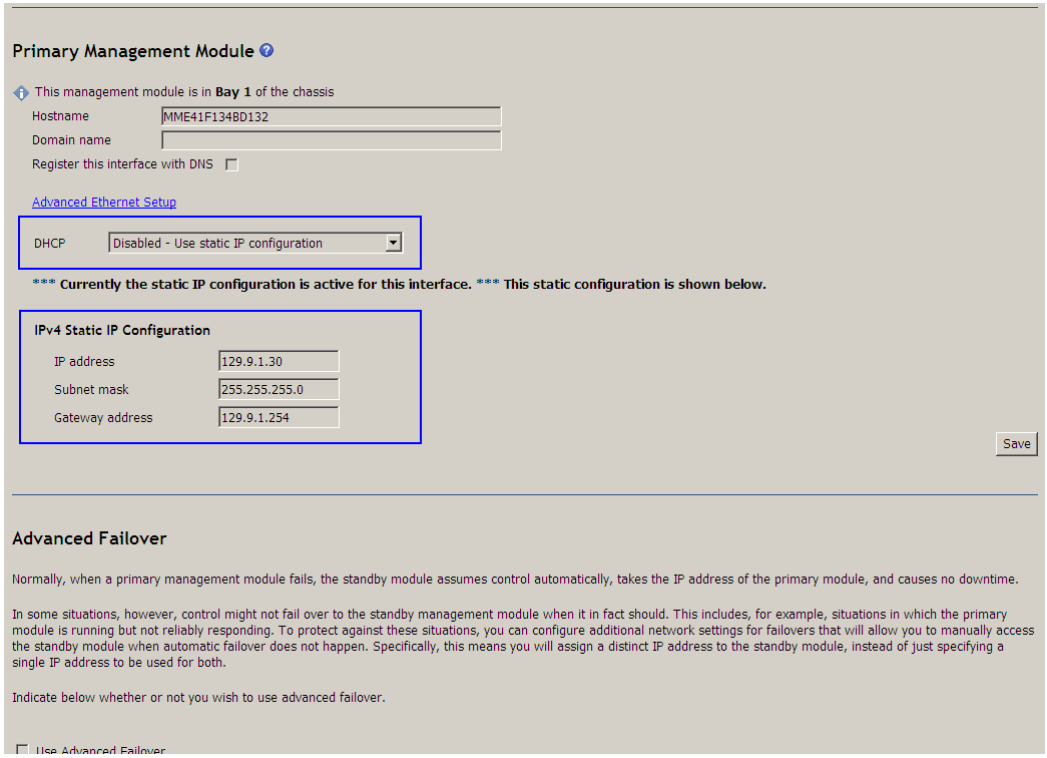



**Table 4-1** Parameter settings

| Item | Parameter | Description |
|---|---|---|
| External Network Interface (eth0) | DHCP | Sets this parameter to **Disabled - Use static IP configuration**. |
| Primary Management Module | IP address | Enters the planned IP address of the management module, such as *129.9.1.30*.<br>Enters the subnet mask of the management module. |
| | Subnet mask | Enters the planned subnet mask of the management module, such as *255.255.255.0*. |

| Item | Parameter | Description |
| --- | --- | --- |
| | Gateway address | Enters the planned route address of the management module, such as *129.9.1.254*. |

8 Choose **MM Control** > **Restart MM**. Then, click **Restart**.

9 Click **OK** in the confirmation dialog box. Then, the management module restarts.

10 Remove the network cable from the control network port of the management module of the IBM blade server, and insert the network cable that is connected to an external network.

**----End**

# 4.2 Configuring the Remote Management Console of an ATAE Blade Server

You can configure the IP address of the network port on the SMM board on an ATAE blade server through a serial port. This facilitates the access to the ATAE blade server management software through the Internet Explorer, thus to manage the ATAE blade server.

## Prerequisite

A Windows-based management terminal must be available.

## Procedure

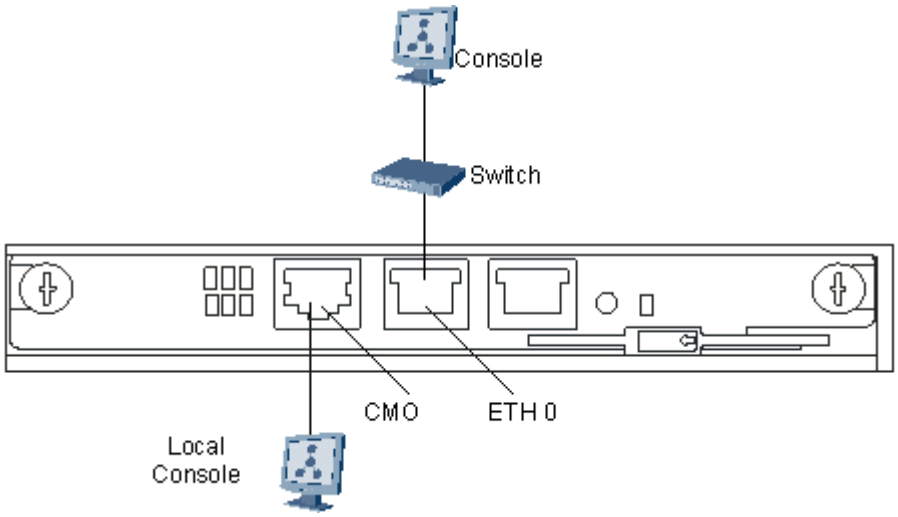
1 Set up the physical connection between the PC and the server.

1. Connect the serial port of the local console and the network port on the SMM board (COM) with a serial port cable (DB9-RJ45) to set up the physical connection between the PC and the server.

   As shown in the following figure, the RJ-45 connector of the serial port cable is plugged into the network port on the SMM board (COM) the DB-9 connector of the cable is plugged into the serial port (COM1 or COM2) of the PC.

2. Connect the network interface (Net Mgt port) of the system controller and the switch with a network cable to set up the physical connection between the system controller and the network.

**Figure 4-1** Diagram of the connection between the SMM board and the controller




2 Set up the logical connection between the PC and the server.

1. Start the PC to enter the Windows OS.
2. Choose **Start** > **Programs (P)** > **Accessories** > **Communications** > **HyperTerminal**.
3. In the **Connection Description** dialog box, enter the name of the newly created connection, such as **NMS**. Then, click **OK**.
4. In the dialog box that is displayed, select the serial port of the PC that is used to connect to the server, such as COM1. Then, click **OK**.
5. In the dialog box that is displayed, set the parameters as follows: **Bit/Second**: 11520, **Data Bit**: 8, **Parity Check**: null, **Stop Bit**: 1, and **Data Flow Control**: null. Click **OK**.

   **NOTE**

   Set the parameters according to the preceding values. Otherwise, the communication may fail.
6. Click **OK**.

3 Enter the user name **root** and the password **huaweiosta**, and press **Enter**.

**NOTE**

If you change the initial password, enter the new password in this step.

4 To configure the IP address of the network port on the SMM board, run the following command:

```
# smmset -l smm -t eth0 -d staticip -v 129.9.1.102 255.255.255.0 129.9.1.254
```

**CAUTION**

It is recommended that you use the public network IP address as the IP address of the network port on the SMM board. Hence, you can manage the blade server remotely in an easy manner. Restrict the access to the IP address of the management unit (such as SMM) based on the actual situation for security purpose. For example, use the firewall to restrict the access.

**----End**

# 4.3 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

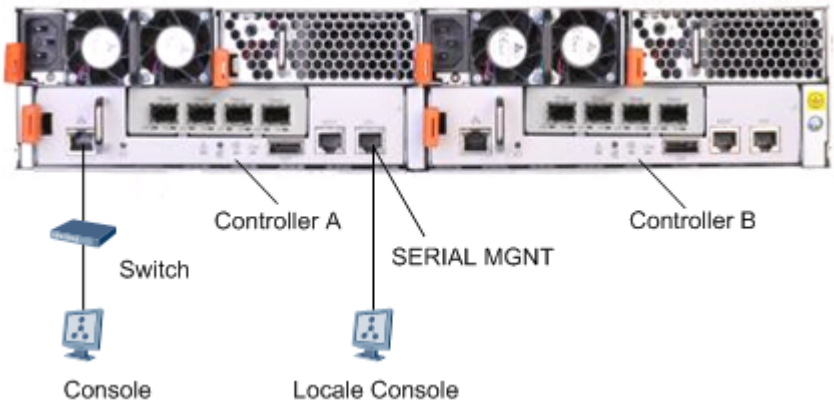
Each OceanStor S2600 disk array has two controllers that need to be configured with management interfaces separately.

## 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**.

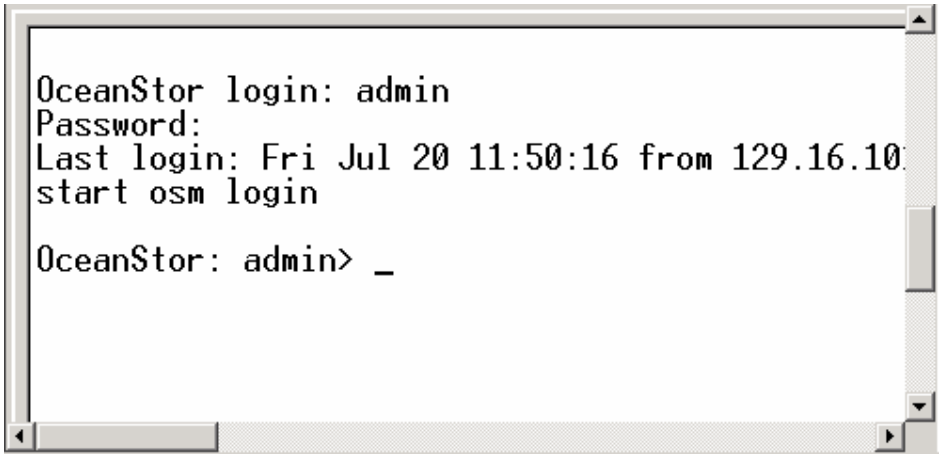
   The following message will be displayed on the Windows management terminal if the connection was established:

   ```
   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 4-2**.

**Table 4-2** 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.<br>● **-a** *IP address*: Indicates the IP address of the management network interface of the controller.<br>● **-s** *subnet mask*: Indicates the subnet mask.<br>● **-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 4-3 provides the format and parameter description of the **showctrlip** command.

**Table 4-3** 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**

# 5 Powering On a Server

This topic describes how to power on a blade server and disk array when the power supply is normal. Perform associated operations according to the server type and disk array type.

## Blade Server

**NOTE**

The following example describes how to power on an ATAE blade server.

1. Power on the cabinet if available.
2. Switch on the DC PDU in the ATAE blade server chassis.

   After the chassis is powered on, all fans work at constant speed rather than at full speed. The fans do not generate abnormal noise during rotation and blow strong air through the ventilation hole on the rear side of the chassis. The HEALTHY indicator on the fan frame is green and constantly on.
3. Raise the ejector lever of the SMM and power on the SMM.

   If the following conditions are met, the SMM is powered on properly:

   - The HEALTHY indicator on the active SMM is green and constantly on.
   - The HEALTHY indicator on the standby SMM is green and flashes with the frequency of 0.5 Hz.
4. Raise the ejector lever of the front panel of the switching network card and power on the switching network card.

   If the following conditions are met, the switching network card is powered on properly:

   - The HEALTHY indicators on the two switching network cards are green and constantly on.
   - The HOTSWAP indicator is off.
   - The OSS indicator is off.
5. Raise the ejector lever of the server card and power on the server card.

   If the following conditions are met, the server card is powered on properly:

   - The HEALTHY indicators on all server cards are green and constantly on.
   - The HOTSWAP indicator is off.
   - The OSS indicator is off.

## 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 the SUSE Linux OS and Its Patches by Using the Quick Installation CD-ROM

This topic describes how to install the SUSE Linux OS and the patches by using the quick installation CD-ROM.

## Prerequisite

- The MAC addresses of NICs through which blade servers are connected to the public network must be collected.
  - An ATAE blade server is connected to the public network through the base plane. For details about how to view the MAC address of the base plane of an ATAE blade server, see **G.5 How to View the MAC Address of the Base Plane of an ATAE Blade Server**.
  - An IBM blade server is connected to the public network through I/O module 1 and I/O module 2. The system IP address of the IBM blade server must be set on the external communication NIC. For details about how to view the MAC address of the external communication NIC of an IBM blade server, see **G.3 How to View the MAC Address of the External Communication NIC of an IBM Blade Server**.
- The installation CD-ROM must be available.
- For the ATAE server, if the USB drive is connected to the ATAE server card, the indicator of the USB drive is green and flashes.

## Context

You can use the quick installation CD-ROM to install the OS and its patches, and partition disks.

NOTE

If the quick installation CD-ROM is not available on the site, manually install the SUSE Linux OS by using the attached SUSE Linux installation CD-ROM. For details, refer to **F Manually Installing the SUSE Linux OS and Its Patches**.

## Procedure

1 **Optional:** In the case of the ATAE blade server, in BIOS, set the order for starting the OS so that the OS boots from the CD-ROM.

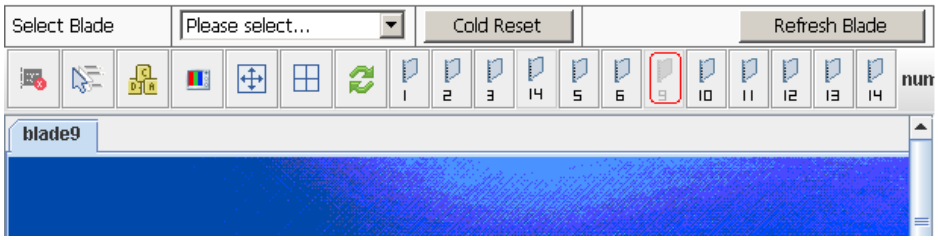
NOTE

This step is applicable only to the ATAE blade server. In the case of other servers, skip this step.

1. Insert the installation disk to the USB drive.
2. **Logging In to the Management Console of an ATAE Blade Server**.
3. In the Blade >> KVM panel, select the required board from **Select Blade**, and click **Cold Reset** to restart the blade server.

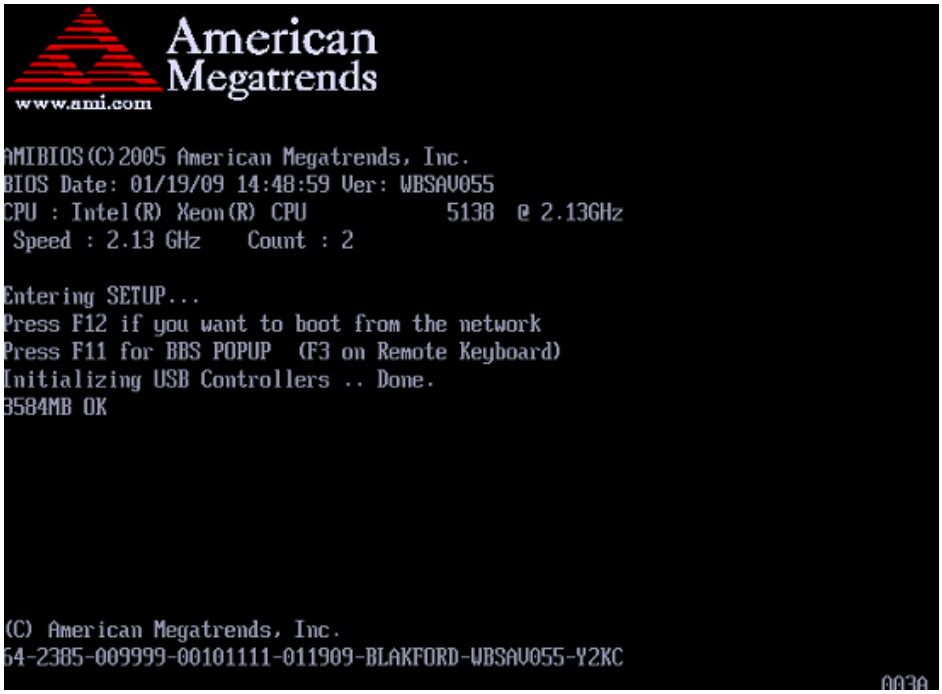
   On the toolbar of the Blade >> KVM panel, click the icon of the card to be operated to display the related tab page.

   Blade >> KVM

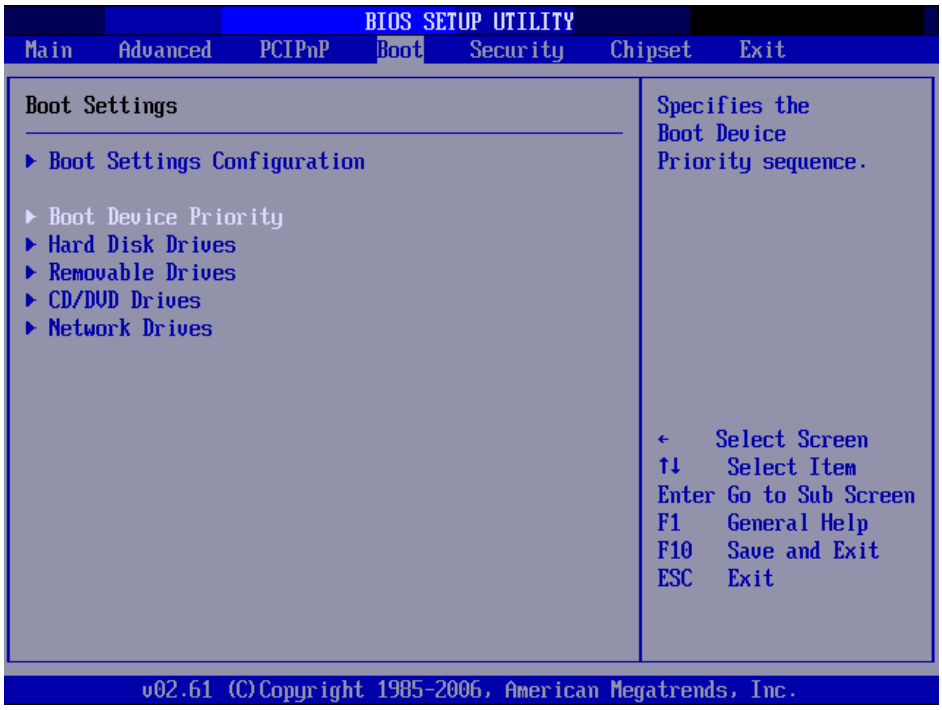
   
   

   **TIP**

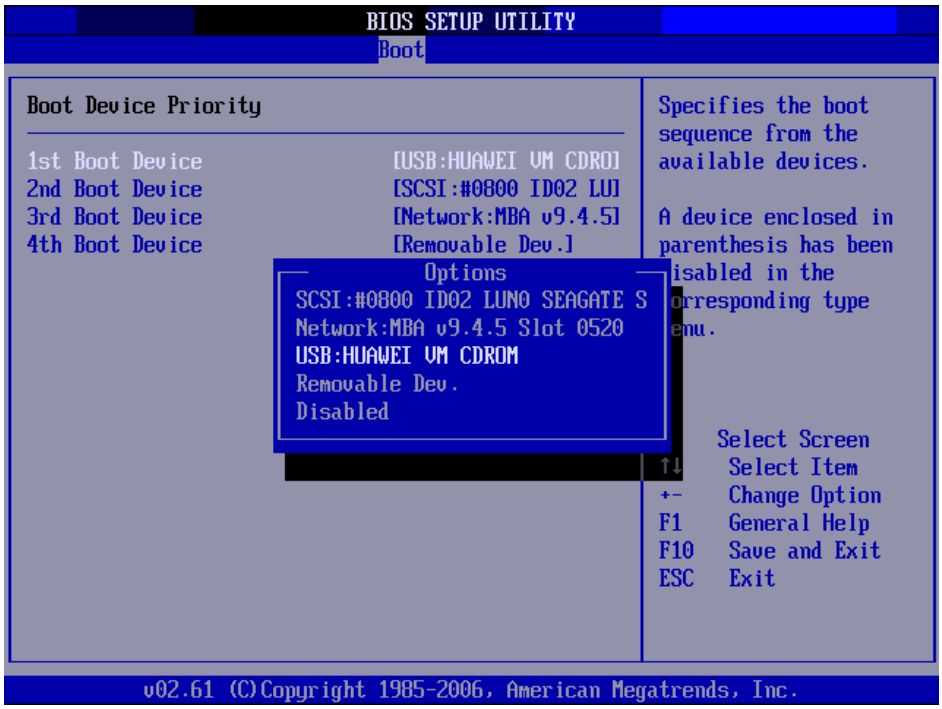
   - To enter the full screen mode, click  on the toolbar.
   - To restore from the full screen mode to window, move the mouse to upper middle of the screen, press **Ctrl+Shift+Alt** and click  in the upper portion of the screen.
4. In the process of restarting the blade server, when the **American Megatrends** window is displayed, press **Delete** to display the **BIOS SETUP UTILITY** window.

   
   
5. In the **BIOS SETUP UTILITY** window, use the left arrow and right arrow keys to choose **Boot** from the main menu.

   On the **Boot Settings** tab page, use the up arrow and down arrow keys to select **Boot Device Priority**. Then, press **Enter**.




6. In the **Boot Device Priority** pane, set the order for starting the OS of the blade server so that the OS boots from the USB disk drive.
   a. Select **1st Boot Device**, and then press **Enter**. The **Options** dialog box is displayed.
   b. Use the up arrow and down arrow keys to select **USB:HUAWEI VM CDROM**. Then, press **Enter**.




7. Press **F10** after the previous settings, the confirm dialog box is displayed.
8. Click **OK**, and then press **Enter** to save the settings and exit.

**2** **Optional:** In the case of the IBM HS22 blade server, in BIOS, set the order for starting the OS so that the OS boots from the CD-ROM.

**NOTE**

This step is applicable only to the IBM HS22 blade server. In the case of other servers, skip this step.

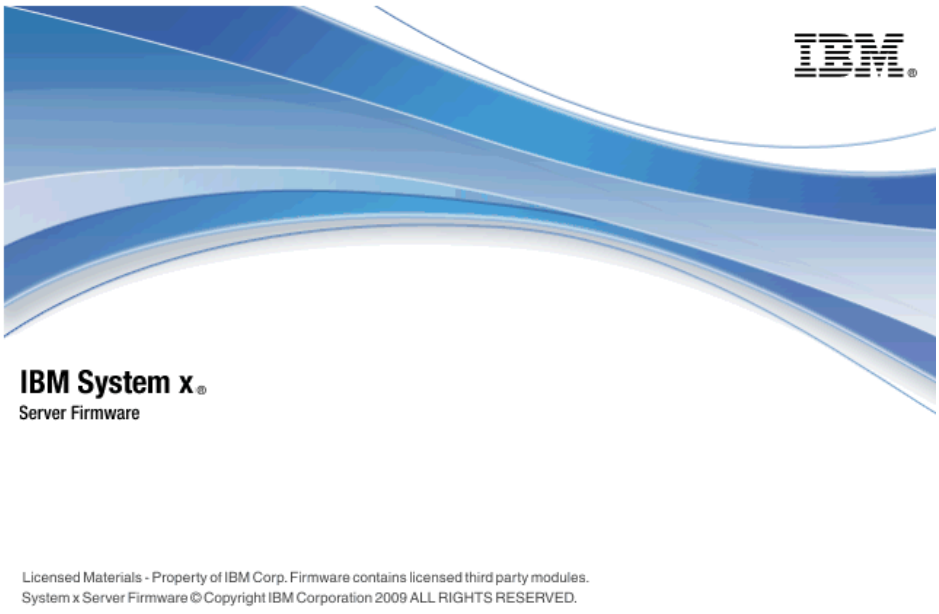
1. **Mount the virtual media of the IBM blade server**.

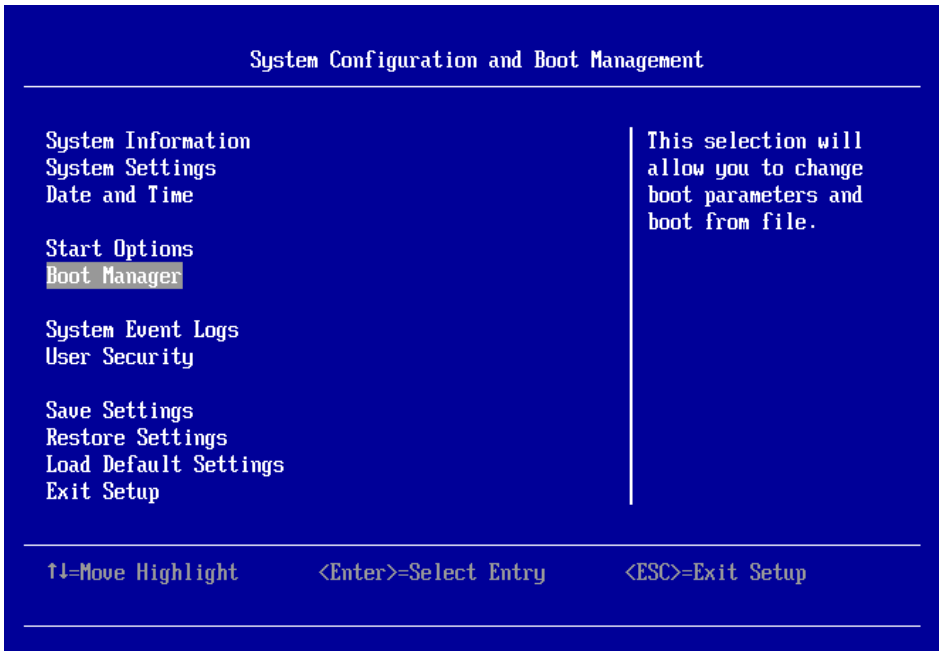
   **NOTE**

   - The purpose of mounting the virtual media of the IBM blade server is to mount the CD/DVD drive or ISO file of the PC where the Web console is installed to a blade server, thus implementing remote installation of the OS of the blade server. Alternatively, the default CD/DVD drive of the IBM BladeCenter E can be used to install the OS of the blade server.
   - To use the default CD/DVD drive of the IBM BladeCenter E to install an OS on a blade server, you need to insert the OS installation DVD into the default CD/DVD drive of the IBM BladeCenter E and then press **MT** at the middle of the blade server, If the **MT** indicator is on, it indicates that the blade server is connected to the default CD/DVD drive.

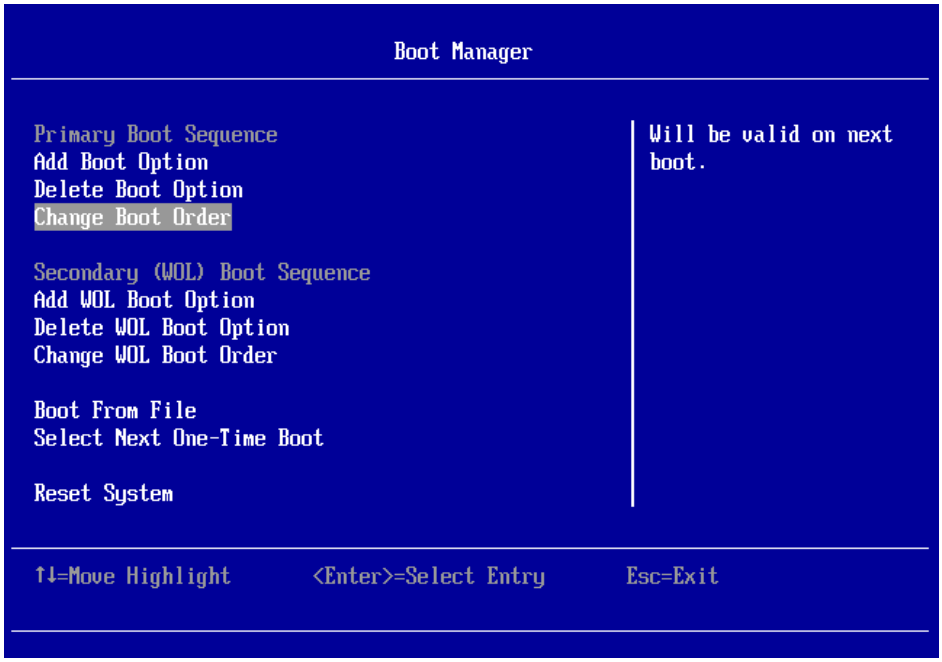
2. In the remote console window, click 

. Then, select the required card.
3. In the **Power Control** area, select **Restart** to restart the blade server.
4. In the process of restarting the blade server, when the **System x** window is displayed, press **F1** and the **System Configuration and Boot Management** window is displayed.

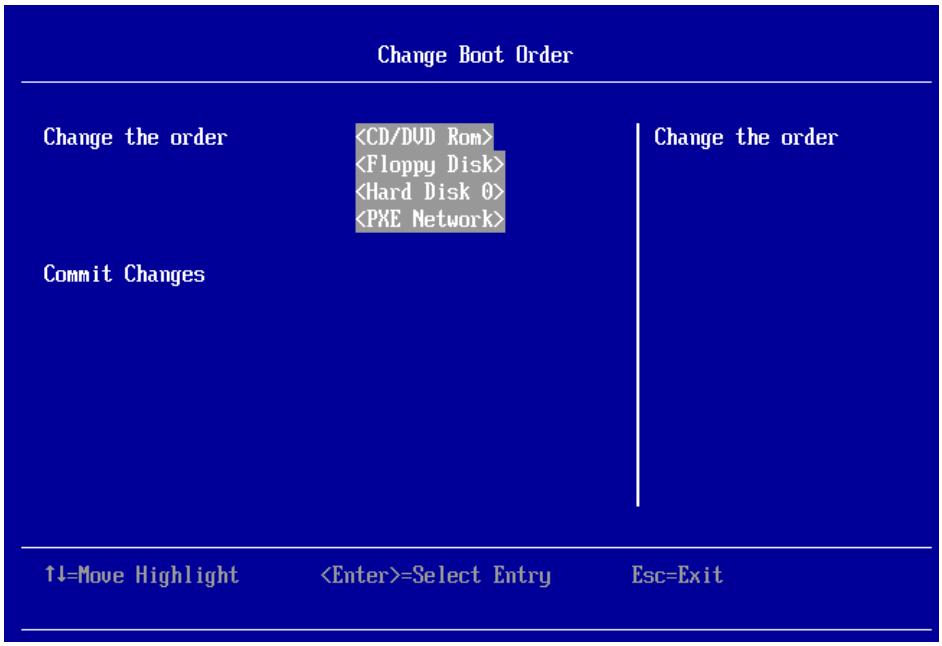





5. Press an arrow key to choose **Boot Manager** from the main menu. Press **Enter**.




6. Press an arrow key to choose **Change Boot Order** from the **Boot Manager**. Press **Enter**.




7. Press an arrow key to choose **CD/DVD Rom** from the **Change Boot Order**. Press **Enter**.
8. Choose **Save Settings** from the main menu. Press **Enter** twice to save the settings.
9. Choose **Exit Setup** and press **Enter** twice to exit BIOS setting.

**3 Optional:** In the case of the IBM HS21 blade server, in BIOS, set the order for starting the OS so that the OS boots from the CD-ROM.

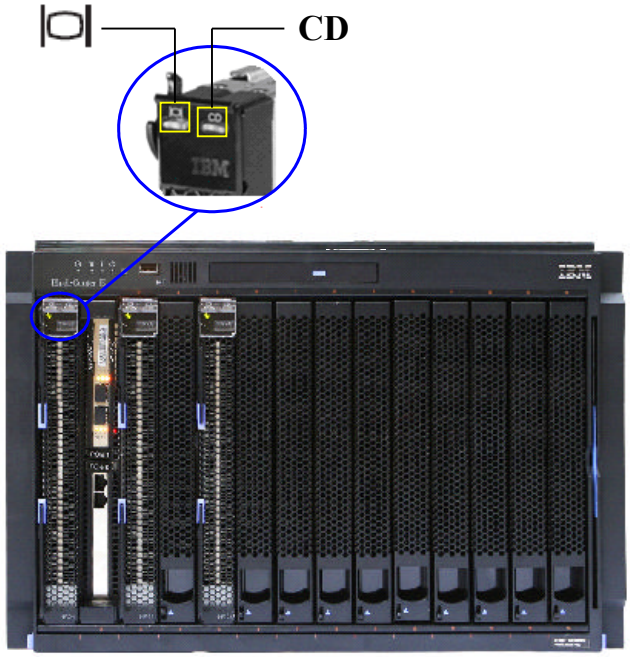
**NOTE**

This step is applicable only to the IBM HS21 blade server. In the case of other servers, skip this step.

1. **Mount the virtual media of the IBM blade server**.

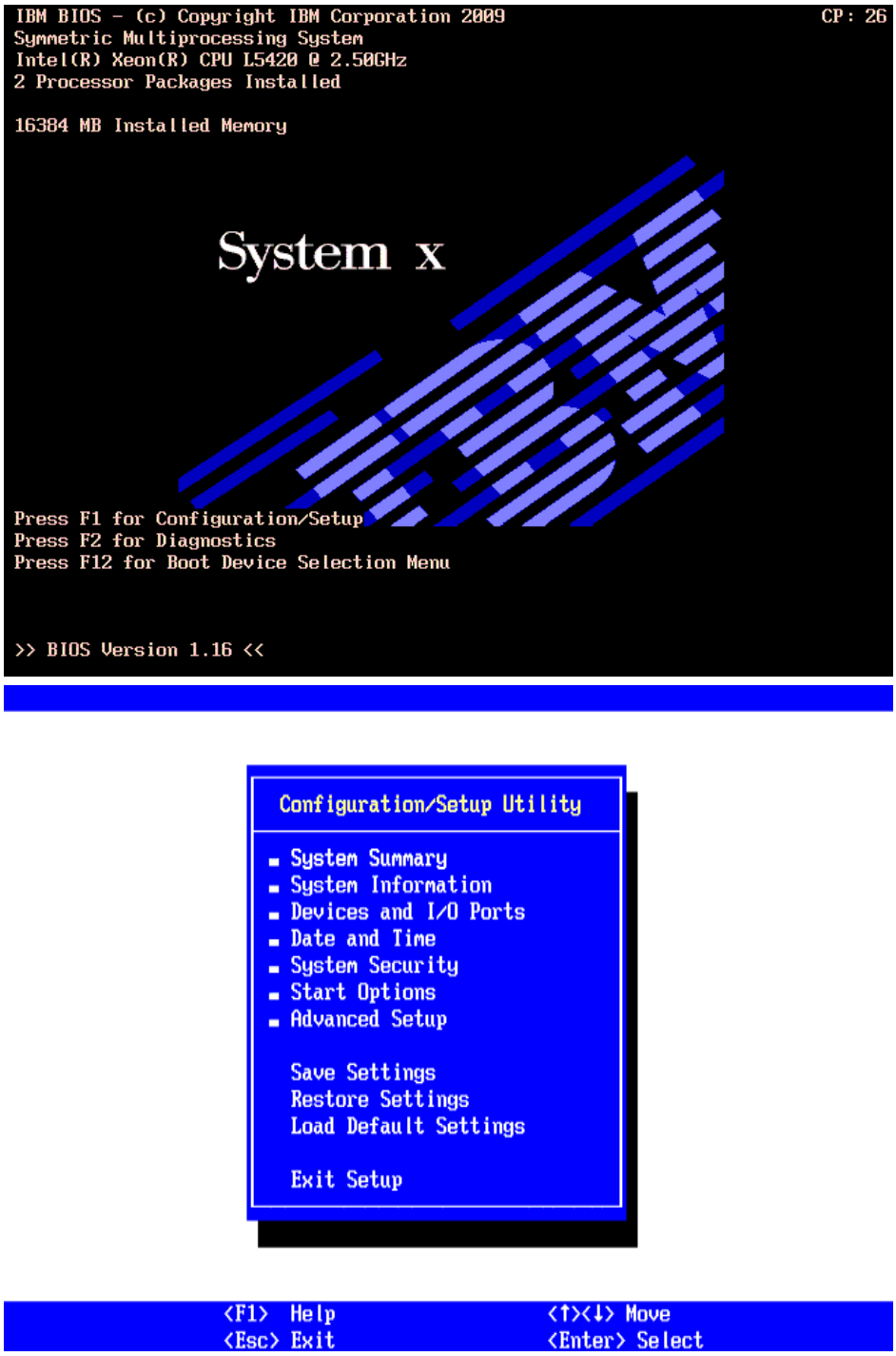
**NOTE**

- The purpose of mounting the virtual media of the IBM blade server is to mount the CD/DVD drive or ISO file of the PC where the Web console is installed to a blade server, thus implementing remote installation of the OS of the blade server. Alternatively, the default CD/DVD drive of the IBM BladeCenter E can be used to install the OS of the blade server.
- To use the default CD/DVD drive of the IBM BladeCenter E to install an OS on a blade server, you need to insert the OS installation DVD into the default CD/DVD drive of the IBM BladeCenter E and then press **CD** at the top of the blade server, as shown in the following figure. If the **CD** indicator is on, it indicates that the blade server is connected to the default CD/DVD drive.




2. In the remote console window, click 

. Then, select the required card.
3. In the **Power Control** area, select **Restart** to restart the blade server.
4. In the process of restarting the blade server, when the **System x** window is displayed, press **F1** and the **Configuration/Setup Utility** window is displayed.




5. Press an arrow key to choose **Start Options** > **Startup Sequence Options** from the main menu. Press **Enter**.
6. In the **Startup Sequence Options** window, do as follows:
   - Set **First Startup Device** to **CD ROM**.
   - Set **Second Startup Device** to **Diskette Drive 0**.
   - Set **Third Startup Device** to **Hard Disk 0**.


After you complete the settings, press **Esc** twice to return to the main menu.

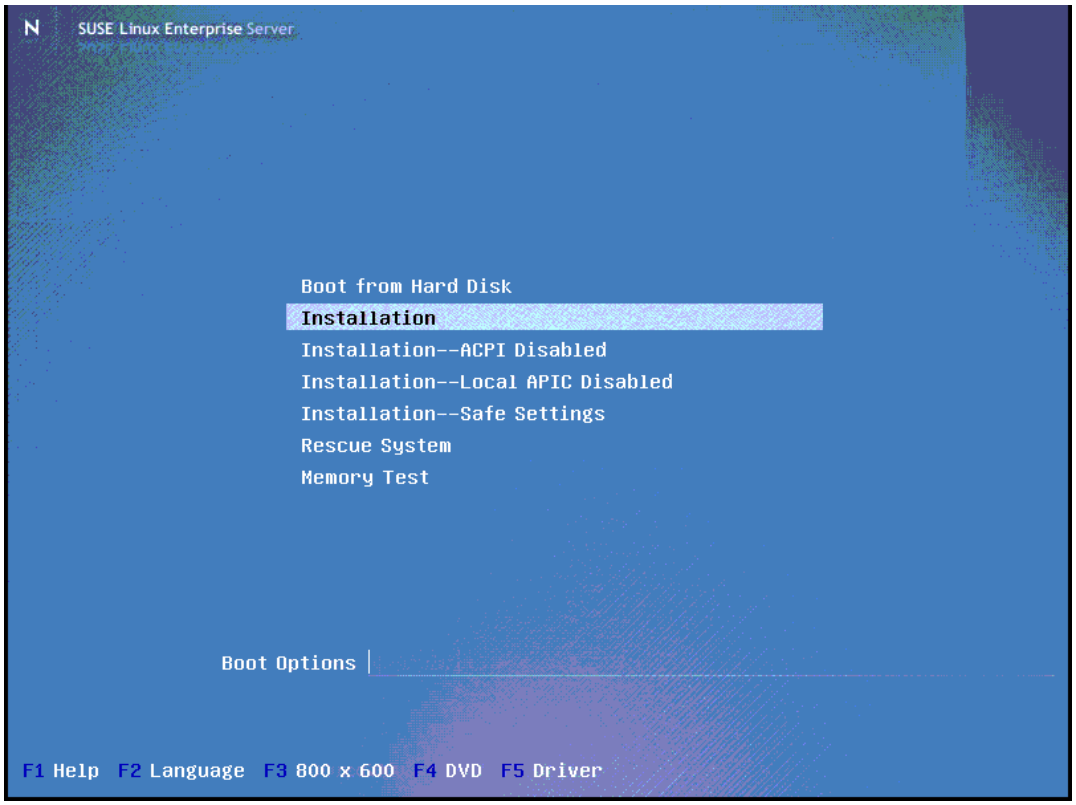
7. Choose **Save Settings** from the main menu. Press **Enter** twice to save the settings.
8. Choose **Exit Setup** and press **Enter** twice to exit BIOS setting.

**4** Wait about five minutes. The system restarts and the **SUSE Linux Enterprise Server** window is displayed.

**NOTE**

If the **SUSE Linux Enterprise Server** window is not displayed but the system enters the server OS, do as follows to restart the management module:

1. Choose **MM Control** > **Restart MM**. Then, click **Restart**. in the Web management widow.
2. Click **OK** in the confirmation dialog box. Then, the management module restarts.




5 Use the up or down arrow key to select **Installation** and press **Enter** to begin to load the Linux core. The system starts the automatic installation of the OS.

**NOTE**

The installation process and remaining time are displayed in the installation window. The entire OS installation process lasts approximately 40 minutes.

6 Do as follows to remove the DVD:

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

   **To log in to the OS, do as follows:**

   - Click **Session** in the lower right corner of the login dialog box. In the **Choose a Session** dialog box, select **GNOME**, and then set the session process to **GNOME**.
   - The default user name and password for logging in to the OS are both **root**.

   **NOTE**

   - By default, the system enables the **root** user to perform remote login and use the FTP tool.
   - If you can log in to the SUSE Linux OS as the **root** user, it indicates that the SUSE Linux OS is successfully installed. Otherwise, install the OS again.

2. On the **GNOME** desktop, right-click, and choose **Open Terminal** from the shortcut menu to open the CLI. Then, run the **eject** command to eject the disk.

   **NOTE**

   If the IBM blade server is installed by using the drive of the virtual media device, run the **eject** ***Name_of_the_virtual_media_device*** command to remove the DVD.

   Run the following command to check the name of the virtual media equipment:
   ```
   # df -hk
   ```
   If **/dev/sr1 132136 132136 0 100% /media/05_04_2009** is displayed, it indicates that the name of the virtual media equipment is **/dev/sr1**. The equipment name varies according to the actual situation.

7 Set the network of the system.

1. Run the following command to log in to the **YaST2 Control Center**:

   ```
   # yast2
   ```

2. In the **YaST2 Control Center** dialog box, choose **Network Devices** > **Network Card**.
3. In the **Network Setup Method** dialog box, select **Traditional Method with ifup** and click **Next**.
4. In the **Network Card Configuration Overview** dialog box, select the NIC to be configured and click **Edit**.

   NOTE

   - The NIC corresponding to the system IP address must be the NIC through which the blade server is connected to the public network.
     - An ATAE blade server is connected to the public network through the base plane. For details about how to view the MAC address of the base plane of an ATAE blade server, see **G.5 How to View the MAC Address of the Base Plane of an ATAE Blade Server**.
     - An IBM blade server is connected to the public network through I/O module 1 and I/O module 2. The system IP address of the IBM blade server must be set on the external communication NIC. For details about how to view the MAC address of the external communication NIC of an IBM blade server, see **G.3 How to View the MAC Address of the External Communication NIC of an IBM Blade Server**.
   - You can view the MAC address of an NIC on the **Address** tab page of the **Network Address Setup** dialog box.
5. In the **Network Address Setup** dialog box, select **Static Address Setup** and set **IP Address** and **Subnet Mask**.
6. Set default gateway IP address.
   a. Click **Routing**.
   b. In the **Routing Configuration** dialog box, enter the default gateway IP address, and then click **OK**.
7. In the **Network Address Setup** dialog box, click **Next** return to the **Network Card Configuration Overview** dialog box.
8. In the **Network Card Configuration Overview** dialog box, click **Finish** to complete the setting of the IP address.
9. Exit **YaST2 Control Center**.

8 Run the following command to restart the OS:

```
# sync;sync;sync;sync
# shutdown -r now
```

9 After the OS is restarted, exit the management console of the blade server.

**----End**

## Follow-up Procedure

- To log in to the SUSE Linux OS by using the remote graphical software in the future, enable the remote login right of the software. For details, see **B.1.6 How to Log In to the OS Through the Remote Login Tools?**.
- After the OS installation is completed by using the quick installation CD-ROM, the default time zone is **Asia** > **Shanghai**. The local time and time zone can be changed as required. For details, see **B.1.10 How to Change the Time and Time Zone of the SUSE Linux OS?**.

# 7 Installing U2000 Software

## About This Chapter

This topic describes how to install U2000 software on the primary and secondary sites. Before starting the U2000 installation program, you must configure the master server and the slave serverusing 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**

- All software packages must be uploaded to the specified directories on the master servers at the primary and secondary sties.
- Only the **Basic components** and **Core components** software packages need to be uploaded to the **/opt/install** directory on the slave servers at the primary and secondary sites and then decompressed.

## 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 Linux 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_sles_x64.tar
   - Database software: U2000***version***_server_db_sles_x64.tar
   - Basic components: U2000***version***_server_nmsbase_sles_x64.tar
   - Core components: U2000***version***_server_nmscore_sles_x64.tar
   - Components of the transport domain (Select it if you want to manage transport or PTN equipment): U2000***version***_server_nmstrans_sles_x64.tar
   - Components of the IP domain (Select it if you want to manage routers, switches, or security equipment): U2000***version***_server_nmsip_sles_x64.tar
   - Components of the access domain (Select it if you want to manage access equipment): U2000***version***_server_nmsaccess_sles_x64.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_sles_x64.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.

**NOTE**

There is no specific sequence for decompressing all software packages.

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

For example, tar xvf U2000***version***_server_nmscore_sles_x64.tar.

5. 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 U2000***version***_server_nmscore_sles_x64.tar.

**2** Do as follows to upload the Veritas software package veritas5.1_sles_x64.tar.gz to the **/opt/vrtstmp** path on the workstation and then decompress it:

1. Run the following command to create the **/opt/vrtstmp** directory:
```
# mkdir /opt/vrtstmp
```

2. Upload the veritas5.1_sles_x64.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
# tar xvfz veritas5.1_sles_x64.tar.gz
# 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_sles_x64.tar.gz.

**----End**

# 7.2 Preconfiguring the OS of the Master Server

Before starting the U2000 installation program, you must configure OSs for the primary and secondary sitesmaster server.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 more information, see **4.3 Configuring the SC IP Address of the OceanStor S2600 Disk Array**.

## Context

**CAUTION**

- The operations mentioned in this topic must be performed on master servers on the primary and secondary sites.
- Do not adjust the size of the CLI when performing the operations described in this topic.

**CAUTION**

By default, the installation program configures bindings for public and private networks in a U2000 distributed system. These bindings maintain proper communication in the private network (between the master server and slave server), as well as that in the public network (between the master server or slave server, and NEs and clients) even when the NIC is faulty. A binding configuration requires two network ports. Therefore, in a U2000 distributed system, each blade server needs to be configured with at least four network ports. Otherwise, the U2000 distributed system will malfunction.

**TIP**

If incorrect characters are entered, press **Ctrl+Backspace** to delete them.

The topic mainly describes the following configurations:

- Modify service network settings, including the server IP address, server host name, and Bond 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.

## Procedure

1. Log in to the OS through the serial port 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 /media/nms/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
   ```

   **NOTE**

   If an IBM blade server is installed by means of the drive of the virtual media device, run the **eject** ***Name_of_the_virtual_media_device*** command to eject the DVD.

   Run the following command to check the name of the virtual media device:

   ```
   # df -hk
   ```

   If **/dev/sr1 132136 132136 0 100% /media/05_04_2009** is displayed, the name of the virtual media device is **/dev/sr1**. The device name varies according to the conditions at your site.

- **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

==========================================


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

Finish...
```

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

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

```
# echo $LANG
```

If **en_US** is not displayed, change the language environment variable description in the **/etc/sysconfig/language** file to **RC_LANG="en_US"**. Perform the following steps:

1. Run the following command to log in to the **YaST2 Control Center**:
   ```
   # yast2
   ```
2. Choose **System** > **/etc/sysconfig Editor**. The **/etc/sysconfig Editor** dialog box is displayed.
3. Choose **System** > **Environment** > **Language** > **RC_LANG**. In **Setting of: RC_LANG**, enter *en_US*.
4. Choose **System** > **Environment** > **Language** > **ROOT_USES_LANG**. Set **ROOT_USES_LANG** to *yes*.
5. Click **Finish**.
6. Run the following commands to restart the OS:
   ```
   # sync;sync;sync;sync
   # shutdown -r now
   ```

**4** Do as follows to configure disk arrays:

**NOTE**

The OceanStor S2600 disk array (6 x 300 GB) supports automatic configuration by means of the **HWICMR**. To use disk arrays that do not support automatic configuration, contact Huawei engineers.

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 Configuring the OceanStor S2600 Disk Array by Using the ISM**.
6. Run the following commands to restart the OS:
   ```
   # sync;sync;sync;sync
   # shutdown -r now
   ```

**5** 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 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 -r now
   ```
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 (SUSE Linux-Distributed)
       2.      High Availability System (SUSE Linux-Distributed)
                     Select[1]:
```

**6** Enter **2** to select the high availability system (SUSE Linux distributed). Then, press **Enter**.

A message similar to the following will be displayed:

```
======= Server Type =======

      The server type, which defines the role of the server in the distributed
system.

               1.      Master Server
               2.      Slave Server (the slave server of distributed system, not
the standby site of HA)

                Enter[1]:
```

**7** Enter **1** to select the master server. 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/oracle]:
```

**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/oracle** 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** Enter a planned system IP address, for example, 129.9.1.1. Then, press **Enter**.

```
Please input the system hostname [Primaster]
```

**11** Enter a planned host name. For example, enter **Primaster** when configuring the OS for the master server on the primary site; enter **Secmaster** when configuring the OS for the master server on the secondary site. Here, configuring the master server on the primary site is taken as an example. Then, press **Enter**.

**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 [255.255.255.0]
```

**12** Enter a planned subnet mask. Then, press **Enter**.

```
Please input the system default router [129.9.1.254]
```

**13** Enter the gateway for a planned route. Then, press **Enter**.

```
======= Config Private Network =======

Enter an IP address as the distribute server installation, such as 192.168.100.0.

Enter[192.168.100.0]:
```

**14** Enter a planned private network segment. Then, press **Enter**.

**CAUTION**

If multiple distributed NMSs are installed in a shelf, you need to modify the private network segment to prevent installation failure of multiple distributed NMSs. Ensure that the private network segments of the distributed NMSs are different from one another.

```
Please confirm the following configurations...
*****************************************************************
                IP              129.9.1.1
                HOSTNAME        Primaster
                NETMASK         255.255.255.0
                MASTERNIC       eth0
                PRINETWORK      192.168.100.0
*****************************************************************
Enter 'y' to apply these values and proceed to the next step, or 'n' to return to
make any changes (y/n):
>
```

**15** Enter **y**. If a configuration needs to be modified, enter **n**.

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.

After the network configuration is compete, information similar to the following is displayed. It takes about 25 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...
```

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

**17** 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.............................
.....................................................................
        Create disk group............................................
.................................................

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

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

**19** 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 20 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.....................................................
    Create disk
group.....................................................................
    Create volumes
        It will take 3-5 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.

**----End**

## Follow-up Procedure

If 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 -r now
   ```
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 Preconfiguring the OS of the Slave Server

Before starting the U2000 installation program, you must configure the OSs for the primary and secondary sitesslave server. Specifically, you need to pre-configure the OS through the DVD or software package. Then, modify the system parameters, modify the network settings of the system, and configure disk mirroring through HWICMR.

## 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**.

## Context

**CAUTION**

- The operations mentioned in this topic must be performed on slave servers on the primary and secondary sites. If there are multiple slave servers, you must perform the associated operations on each slave server.

  If the blade server has only one blade, skip the operation on the slave server.
- By default, the installation program configures bindings for public and private networks in a U2000 distributed system. These bindings maintain proper communication in the private network (between the master server and slave server), as well as that in the public network (between the master server or slave server, and NEs and clients) even when the NIC is faulty. A binding configuration requires two network ports. Therefore, in a U2000 distributed system, each blade server needs to be configured with at least four network ports. Otherwise, the U2000 distributed system will malfunction.
- Do not adjust the size of the CLI when performing the operations described in this topic.
- Perform the following operations by using the HWICMR:
  - Set the shared system memory parameters: Modify the **/proc/sys/kernel/shmmax** and **/proc/sys/kernel/shmmni** file to set the shared system memory parameters.
  - Modify the network settings of the system: You can modify the network settings of the system, including the system host name, the system IP address, the system network interface, and the subnet mask of the system IP address.
  - Mount a disk array.

**TIP**

If incorrect characters are entered, press **Ctrl+Backspace** to delete them.

## Procedure

1. Log in to the OS as user **root**.
2. Start copying software.
   - **Mode 1**: Installation using a software package.
     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
        ```

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

2. Enter **2** to skip copying of the Veritas software.

   A message similar to the following will be displayed:

```
Skip copy Veritas software...

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


Finish...
```

- **Mode 2**: Installation using a DVD.

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 /media/nms/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 **2** to skip copying of the Veritas software.

   A message similar to the following will be displayed:

   ```
   Skip deal with Veritas software...

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

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

5. Run the following commands to eject the DVD.

   ```
   # cd /
   # eject
   ```

   **NOTE**

   If an IBM blade server is installed by means of the drive of the virtual media device, run the **eject** ***Name_of_the_virtual_media_device*** command to eject the DVD.

   Run the following command to check the name of the virtual media device:

   ```
   # df -hk
   ```

   If **/dev/sr1 132136 132136 0 100% /media/05_04_2009** is displayed, the name of the virtual media device is **/dev/sr1**. The device name varies according to the conditions at your site.

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

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

```
# echo $LANG
```

If **en_US** is not displayed, change the language environment variable description in the **/etc/sysconfig/language** file to **RC_LANG="en_US"**. Perform the following steps:

1. Run the following command to log in to the **YaST2 Control Center**:

   ```
   # yast2
   ```

2. Choose **System** > **/etc/sysconfig Editor**. The **/etc/sysconfig Editor** dialog box is displayed.
3. Choose **System** > **Environment** > **Language** > **RC_LANG**. In **Setting of: RC_LANG**, enter *en_US*.
4. Choose **System** > **Environment** > **Language** > **ROOT_USES_LANG**. Set **ROOT_USES_LANG** to *yes*.
5. Click **Finish**.
6. Run the following commands to restart the OS:

   ```
   # sync;sync;sync;sync
   # shutdown -r now
   ```

**4** 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 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 -r now**
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 (SUSE Linux-Distributed)
       2.      High Availability System (SUSE Linux-Distributed)
                     Select[1]:
```

**5** Enter **2** to select the high availability system (SUSE Linux distributed). Then, press **Enter**.

A message similar to the following will be displayed:

```
======= Server Type =======

      The server type, which defines the role of the server in the distributed
system.

               1.      Master Server
               2.      Slave Server (the slave server of distributed system, not
the standby site of HA)

                Enter[1]:
```

**6** Enter **2** to select the slave server. Then, press **Enter**.

A message similar to the following will be displayed:

```
======= Host Name =======
Host name is the only ID of the host. It is the name used to indicate the host in
the network. Host name for each host is unique in the network.
Press Enter to use the current host name, or enter a new host name. The new host
name will take into effect after the host reboots.
The host name can contain numerals, letters. It must begin with a letter.
Enter [Masterserver]:
```

**7** Enter a planned host name. Then, press **Enter**.

A message similar to the following will be displayed:

```
======= IP Address of the Master NIC of bond =======
Enter an IP address for the master NIC.
You need to configure the IP address for the NIC before the server can communicate
with other devices in the network.
The IP address must be unique and not be occupied by any other equipment in the
network. Otherwise, the IP address conflict may cause abnormal communication.
Press Enter to use the default value (The default is the current IP address. If no
default is displayed, you need to enter a valid IP address.)

Enter[129.9.1.2]:
```

**8** Enter a planned IP address for the master NIC. Then, press **Enter**.

A message similar to the following will be displayed:

```
======= Subnet Mask of the Master NIC =======

        Enter a subnet mask for the master NIC.
       The subnet mask is a 32-digit value. It defines the network ID and the host
ID. A network can be divided into several subnets by subnet mask.
        The subnet masks of different hosts in one subnet are consistent.
        Press Enter to use the default value. (The default is the subnet mask
configured for the current system. If no default is displayed, you need to enter a
valid subnet mask.)

Enter[255.255.255.0]:
```

**9** Enter a planned subnet mask for the master NIC. Then, press **Enter**.

A message similar to the following will be displayed:

```
Please confirm the following configurations...
************************************************************
            IP                    10.78.218.18
            HOSTNAME              NMSServer
            NETMASK               255.255.255.0
            MASTERNIC             eth0
************************************************************
Enter 'y' to apply these values and proceed to the next step,
or 'n' to return to make any changes (y/n):
```

**10** Enter **y** to confirm the information. Then, press **Enter**.

A message similar to the following will be displayed:

```
...
Modifying system network configuration..................
Modifying system parameters..................

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

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

**12** After the OS restarts, log in to the OS as user **root**.

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

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

A message similar to the following will be displayed:

```
...

Modifying system network configuration..................
Modifying the system parameters.........................
Mounting disk array.....................................
...

All operations defined in the task flow have been completed.

All operation logs are saved in:
             /var/ICMR/ICMR_20090915024631.log
```

- 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.

**14** Run the following commands to start the Network Management System Maintenance Suite process:

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

**----End**

### Follow-up Procedure

If 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 -r now
   ```
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**.

# 7.4 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.

7.4.1 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 SUSE Linux OS.

7.4.2 Installing the U2000 Through the CLI
This topic describes how to install the U2000 software on the master server through the CLI. This method is recommended if you cannot log in to the GUI of the OS.

# 7.4.1 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 SUSE Linux OS.

### Prerequisite

- In the scenario where the OSs of the master server and slave server have already been preconfigured, see the **7.2 Preconfiguring the OS of the Master Server** and **7.3 Preconfiguring the OS of the Slave Server**. In the scenario where the OSs of the master server and slave server have not yet been preconfigured, the single-server system (SUSE Linux-distributed) fails to be installed.

- The database software is installed along with the U2000. If the database has already been installed on the master server, you must make sure that the database is started. For details, see **B.3.4 How to Start the Oracle Database in the High Availability System**.
- The size of the installation directory of the master server and slave server must meet requirements. For example, the free space of the installation directory must be larger than 30 GB for the installation of all components.

  **TIP**

  Run the **df -hk /opt** command to view the remaining space of the **/opt** directory.
- The remote desktop control software is ready.
- The Network Management System Maintenance Suite server of the slave servers on the primary and secondary sites is started.

  **NOTE**

  If the Network Management System Maintenance Suite process of the slave server server on the primary and secondary sites is not started, run the following commands to start it:

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

## Context

**CAUTION**

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

**TIP**

To log in to the **GNOME**, perform the following operations: Click **Session** in the lower left corner of the login dialog box of the remote desktop control software. In the **Choose a Session** dialog box, select **GNOME**, and then set the session to **GNOME**.

## Procedure

1. Log in to the **GNOME** session process of the master server OS as the **root** user.
2. On the desktop, right-click and choose **Open Terminal** from the shortcut menu to display a CLI.
3. 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**

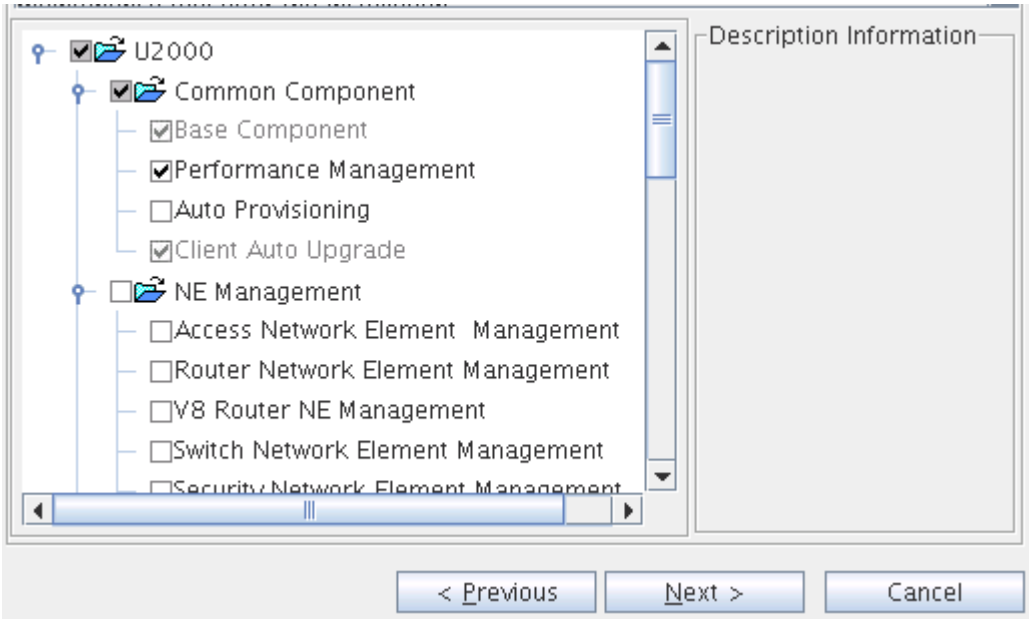
   If the U2000 is not pre-configured, the **/opt/HWENGR** directory and the **install.sh** will not be generated and the U2000 cannot be installed.

   Read the terms of the software license agreement carefully.
4. 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**.

5 Select a language as required, such as **English**. Then, click **Next**. The **Select Component** dialog box is displayed.



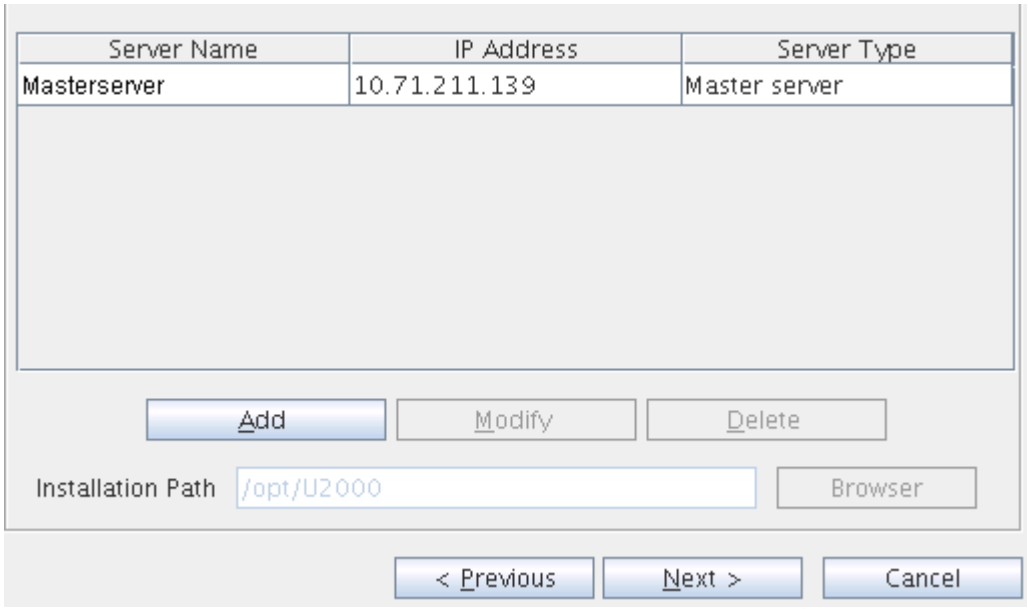

6 Select the components according to the type of the equipment to be managed. Then, click **Next**. The **Configure Server** dialog box is displayed.

**CAUTION**

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

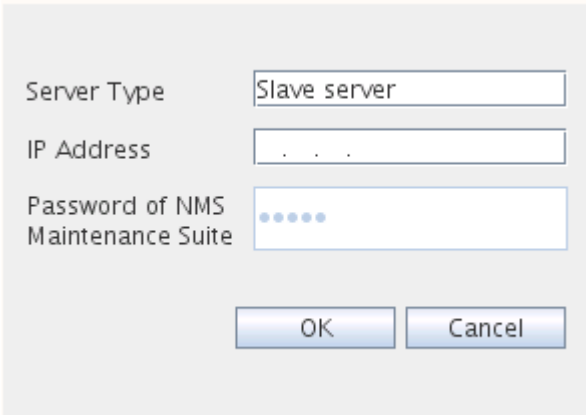
**TIP**

Select components according to preinstallation component planning. If component planning is not performed before installation, see **Deployment Planning of NMS Components** in the *iManager U2000 Planning Guide* to perform component planning.




**7** Do as follows to configure the server:

1. Click **Add**. The **Add Server** dialog box is displayed.




Set the related parameters. The following table shows the parameter description.

| Parameter | Description |
| --- | --- |
| Server Type | Specifies the type of a slave server. The default value is **Slave Server**. You do not need to set this parameter. |
| IP Address | Specifies the IP address of the slave server for external communication. |
| Password of Network Management System Maintenance Suite | Specifies the password for the **admin** user on the slave server. The default value is **admin**. You do not need to set this parameter. |

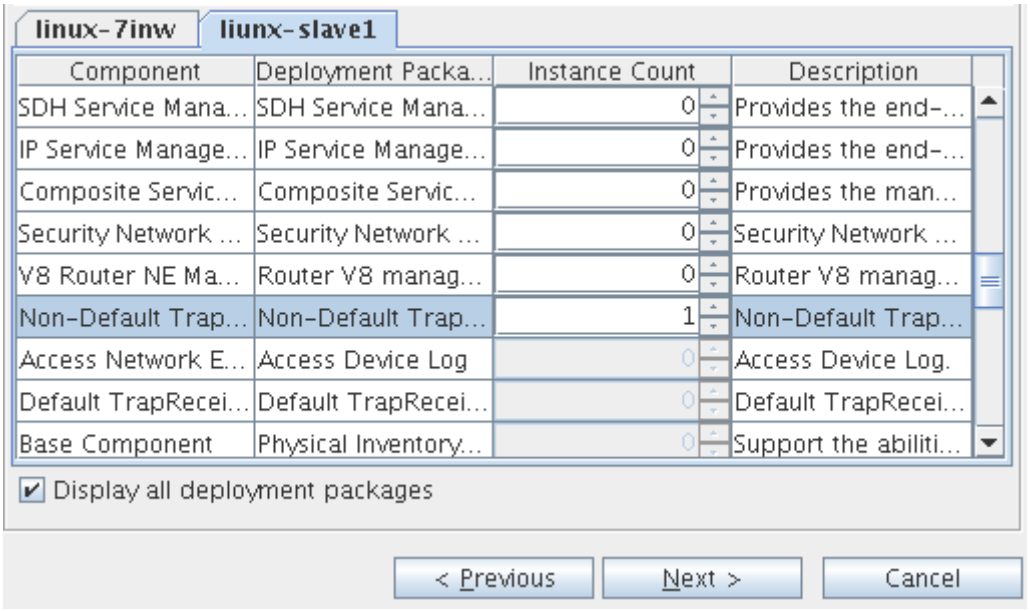
2. Click **OK**. The system returns to the **Configure Server** dialog box.
   - To add multiple slave servers, click **Add**. Set the server type to **Slave Server** to add more slave servers.

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

3. Click **Next**. The **Deployment Parameters** dialog box is 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.




8 Set the number of installed instances for the master server and slave server.

**NOTE**

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

Select the master server and slave server to view the selected components and the instance numbers related to the components respectively.

- 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.
- The non-default TrapReceiver service component is deployed together with the deployment packages that are applicable to SNMP. Common deployment packages applicable to SNMP include **Access Network Single Element Management Service**, **Switch Network Element Management**, **RouterMgr/SgMgr Component**, and **Security Network Element Management**. For example, if the **Access Network Single Element Management Service** deployment package is deployed on a slave server, you also need to deploy the **Non-Default TrapReceiver Service component** deployment package on this server.
- **DeskTop Service Component** can be deployed only on the master server and only one instance can be deployed.

- **NMS Log Zip Management** needs to be deployed on each server and one instance needs to be deployed on each server.

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

NOTE

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

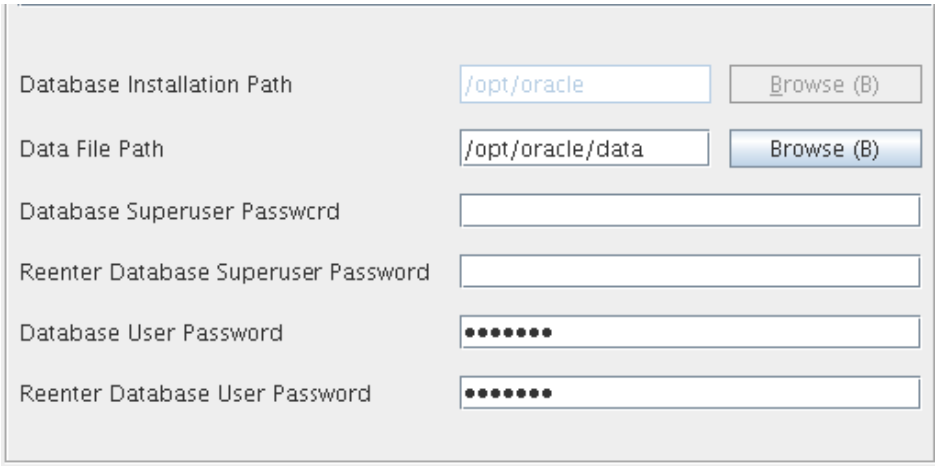
- For the default style, alarms are displayed in the following descending order of severity: **Critical**, **Major**, **Minor** and **Warning**.
- For the North America style, alarms are displayed in the following five levels in descending order of severity: **Critical**, **Major**, **Minor**, **Not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

10 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 Oracle database. The default value is **/opt/oracle**. This parameter does not need to be set. |
| Data File Path | Specifies the path of the data file. The default value is **/opt/oracle/oradb/data**. This parameter does not need to be set. |

| Parameter | Description |
| --- | --- |
| Database Superuser Password | Specifies the superuser password of the database. This password cannot be left blank and must be at least six characters long and consist of letters or digits. Special characters are not allowed. For example, it can be **changeme**.<br>**CAUTION**<br>● The password of the database superuser at the primary site must be consistent with that at the secondary site.<br>● 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.<br>**NOTE**<br>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**.<br>**CAUTION**<br>● The password of the database user at the primary site must be consistent with that at the secondary site.<br>● 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. |

**11** 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**.

**12** 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.
- If a message indicating an installation failure or interruption is displayed during installation, perform the following operations on each server (including the master server and all slave servers) 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 Step 3 to install the U2000.

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

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

**15** Run the following commands to stop the VCS service:

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

**16** 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.

**17** Run the following commands to restart the OS:

**CAUTION**

Run the following commands on both the master server and slave server to restart the OS:

```
# sync;sync;sync;sync
# shutdown -r now
```

**18** After the OS is restarted, log in to each slave server and run the following commands to configure the NFS:

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

A message similar to the following will be displayed:

```
Getting the current working directory...
Working directory:/opt/HWICMR/bin
The server private ip is 192.168.100.18.
Starting service automounter                                done
Succeed to enable the autofs.
```

**NOTE**

If **Succeed to enable the autofs** is displayed, it indicates that the NFS is configured successfully. Run the following commands to check the **/share/ftproot** directory on the slave server:

```
# cd /share/ftproot
# cd /share
# ls
```

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

**CAUTION**

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

**NOTE**

The **/opt/oracle/oradb/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/oracle/oradb/data**.
8. Click **Default value** and choose **Disable alarm generation** from the drop-down list.
9. Click **OK**.

**----End**

## Follow-up Procedure

In the NAT networking scenario, you must configure the **ipmap.cfg** file. For details, see **B.4.5 How to Configure the ipmap.cfg Mapping File**.

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**.

# 7.4.2 Installing the U2000 Through the CLI

This topic describes how to install the U2000 software on the master server through the CLI. This method is recommended if you cannot log in to the GUI of the OS.

## Prerequisite

- In the scenario where the OSs of the master server and slave server have already been preconfigured, see the **7.2 Preconfiguring the OS of the Master Server** and **7.3 Preconfiguring the OS of the Slave Server**. In the scenario where the OSs of the master server and slave server have not yet been preconfigured, the single-server system (SUSE Linux-distributed) fails to be installed.
- The database software is installed along with the U2000. If the database has already been installed on the master server, you must make sure that the database is started. For details, see **B.3.4 How to Start the Oracle Database in the High Availability System**.
- The size of the installation directory of the master server and slave server must meet requirements. For example, the free space of the installation directory must be larger than 30 GB for the installation of all components.

  **TIP**

  Run the **df -hk /opt** command to view the remaining space of the **/opt** directory.
- The Network Management System Maintenance Suite server of the slave servers on the primary and secondary sites is started.

  **NOTE**

  If the Network Management System Maintenance Suite process of the slave server server on the primary and secondary sites is not started, run the following commands to start it:

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

## Context

**CAUTION**

The operations mentioned in this topic must be performed on the master servers of 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.

## Procedure

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

**2** 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.

**3** 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]:
```

**4** 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]:
```

**5** 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]:
```

**6** 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.

**7** Enter **1** to select components.

A message similar to the following will be displayed:

```
...
Please select the operation
```

```
options[a:Select, b:Deselect, c:Display, d:Reset, e:Select All, f:Finished
configuration, f]:
```

8 Select the components according to the type of the equipment to be managed as prompted. Then, enter **f** to finish selecting the components.

A message similar to the following will be displayed:

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

**CAUTION**

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

9 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]:
```

10 Enter **n** to proceed with the next step. Then, press **Enter**.

A message similar to the following will be displayed:

```
===============< Deployment Server >===============
+------------+-------------+-------------+----------------------+-----------------
+
|Server Name |IP Address|Server Type|Administrator Password|Installation Path|
+------------+-------------+-------------+----------------------+-----------------
+
|Masterserver|10.111.66.203|Master Server|****                  |/opt/U2000
|
+------------+-------------+-------------+----------------------+-----------------
+

[1:Add, 2:Modify, 3:Delete 4:Complete, 4]:
```

- To modify the master server, enter **2**, and then press **Enter**. The system modifies the master server parameters as prompted.
- To delete the master server, enter **3**, and then press **Enter**. The system deletes the master server, and then adds the master server again.

11 Add the slave server.

1. Enter **1** to add a server. Then, press **Enter**.

   A message similar to the following will be displayed:

   ```
   Server Name[]:
   ```

2. Enter the name of the slave server. Then, press **Enter**. The default value is the host name of the slave server.

   A message similar to the following will be displayed:

```
Server Type[1:Slave Server, 1]:
```

3. Enter **1** to select the slave server. Then, press **Enter**.

   A message similar to the following will be displayed:

```
IP Address[]:
```

4. Enter the IP address of the slave server for external communication. Then, press **Enter**.

   A message similar to the following will be displayed:

```
===============< Deployment Server >===============
+------------+-------------+-------------+----------------------
+-----------------+
|Server Name |IP Address|Server Type|Administrator Password|Installation Path|
+------------+-------------+-------------+----------------------
+-----------------+
|Masterserver|10.111.66.203|Master Server|****                  |/opt/
U2000         |
+------------+-------------+-------------+----------------------
+-----------------+
|Slaveserver |10.111.66.206|Slave Server |****                  |/opt/
U2000         |
+------------+-------------+-------------+----------------------
+-----------------+

[1:Add, 2:Modify, 3:Delete 4:Complete, 4]:
```

5. Enter **4** to complete installation. Then, press **Enter**.

   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:

```
===============< 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]:
```

**13** 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.
- The non-default TrapReceiver service component is deployed together with the deployment packages that are applicable to SNMP. Common deployment packages applicable to SNMP include **Access Network Single Element Management Service**, **Switch Network Element Management**, **RouterMgr/SgMgr Component**, and **Security Network Element Management**. For example, if the **Access Network Single Element Management Service** deployment package is deployed on a slave server, you also need to deploy the **Non-Default TrapReceiver Service component** deployment package on this server.
- **DeskTop Service Component** can be deployed only on the master server and only one instance can be deployed.
- **NMS Log Zip Management** needs to be deployed on each server and one instance needs to be deployed on each server.

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:

```
===============< 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**.

**15** 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]:
```

**16** 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/oracle]
Data File Path []: /opt/oracle/oradb/data
DB Super Password[]:
```

**17** 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 cannot be left blank and must be at least six characters long and consist 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]:
   ```

**18** 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.
- If a message indicating installation failure or abnormal interruption is displayed during installation, perform the following operations on each server (including the master server and all slave servers) 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.

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

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

**20** 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.
...
```

**21** Run the following commands to stop the VCS service:

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

**22** 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.

**23** Run the following commands to restart the OS:

**CAUTION**

Run the following commands on both the master server and slave server to restart the OS:

```
# sync;sync;sync;sync
# shutdown -r now
```

**24** After the OS is restarted, log in to each slave server and run the following commands to configure the NFS:

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

A message similar to the following will be displayed:

```
Getting the current working directory...
Working directory:/opt/HWICMR/bin
The server private ip is 192.168.100.18.
Starting service automounter                                    done
Succeed to enable the autofs.
```

**NOTE**

If **Succeed to enable the autofs** is displayed, it indicates that the NFS is configured successfully. Run the following commands to check the **/share/ftproot** directory on the slave server:

```
# cd /share/ftproot
# cd /share
# ls
```

**25** Do as follows to set **Disable alarm generation** for **/opt/oracle/oradb/data**:

**CAUTION**

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

**NOTE**

The **/opt/oracle/oradb/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/oracle/oradb/data**.
8. Click **Default value** and choose **Disable alarm generation** from the drop-down list.
9. Click **OK**.

**----End**

## Follow-up Procedure

In the NAT networking scenario, you must configure the **ipmap.cfg** file. For details, see **B.4.5 How to Configure the ipmap.cfg Mapping File**.

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 primary and secondary sites using MSuite.

## Prerequisite

- The preceding installation steps must be complete.
- The instances deployed on the master servers for the primary and secondary sites must be the same. The numbers of the slave servers on the primary and secondary sites must be the same and the slave servers correspond to each other in a one-to-one manner.

## 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 SUSE Linux 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 server has been started for all servers on the primary and secondary sites.

     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      9281     1  0 02:47 pts/0    00:01:55 /opt/HWNMSJRE/jre_linux/
     bin/java -server -Dlanguage=en -Xverify:none -Xmx128m -Xms64m -
     XX:MinHeapFreeRatio=10 -XX:MaxHeapFreeRatio=95 -XX:+UseParNewGC -XX:
     +UseConcMarkSweepGC -Dequinox.conf=engineering/conf/equinox.ini -
     Dos.native.path=engineering/lib -DCoreFramework.logFilePath=engineering/
     conf/loggerservice_Server.cfg -Djava.library.path=./engineering/lib/ -
     Drunway=install -DautoLogin=true -DinstallDiskMode=cmd -
     DinstallType=server -classpath ./engineering/lib/Launcher.jar:./
     engineering/lib/equinox.jar com.oss.core.launcher.Launcher
     ```

**NOTE**

If the displayed information contains **/opt/HWNMSJRE/jre_linux/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 **GNOME** session of the OS for the master server on the primary site as the **root** user.
3. On the master server on the primary site, Run the following commands to start the MSuite client:

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

Wait for about one minute. The following dialog box is displayed.


Set associated parameters. The following table shows parameter description.

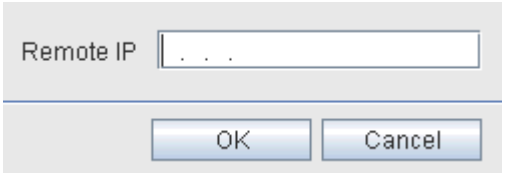
| Parameter | Settings |
|---|---|
| IP Address | System IP address on the primary site master server. |
| Port Number | The default value is **12212**. |
| User Name | The default value is **admin**. |
| Password | Password for the **admin** user. The default password is **admin**. |

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 of the master server 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 sitemaster server, 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:                    129.9.1.30
     RVG name:                     datarvg
     DG name:                      datadg
     RVG state:                    enabled for I/O
     Data volumes:                 1
     VSets:                        0
     SRL name:                     srl
     SRL size:                     3.00 G
     Total secondaries:            1

   Secondary:
     Host name:                    129.9.1.40
     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, up-to-datestale**, 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 master server of 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 master server 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 master server as the **root** 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 master server, check data replication status as the **root** user. For details, see Step 8 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 master 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 5, and then enter the license key of VRTS VOLUME REPLICATOR OPTION that is newly applied for.
7. Repeat step 5, and then enter the license key of VRTS CLUSTER SERVER HA/DR that is newly applied for.
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 Run the following commands to restart the OS:

```
# sync;sync;sync;sync
# shutdown -r now
```

**----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

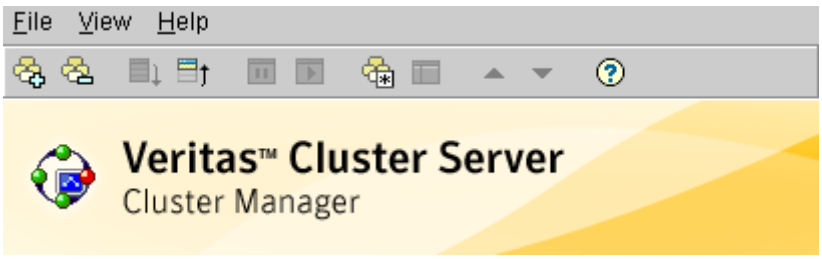
The U2000 license needs to be installed on the master servers of the primary and secondary sites separately.

## Procedure

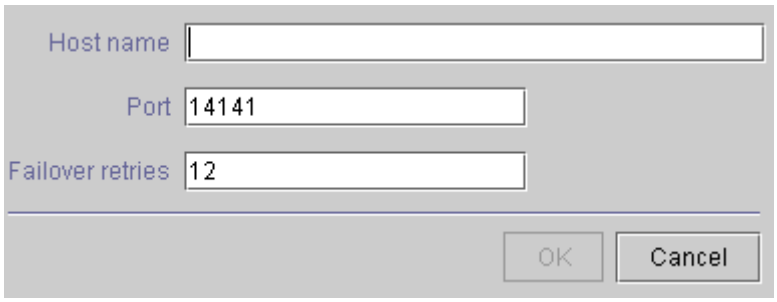
1 On the master server of the primary site, run the following command to start the U2000 processes:

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

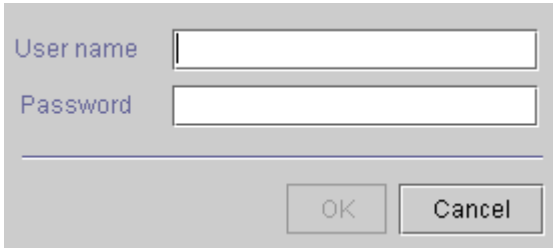
```
# hagui &
```




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, ListenerRes, DatabaseServer, mountRes and RVGPrimary, are in the **Online on Primaster** state, it indicates that the NMS server is started.

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 master server installation directory **/export/home/nmsuser** of primary site in ASCII mode through FTP as the **root** user. Details are as follows:
   a. Log in to a PC where the license file is stored.
   b. Choose **Start** > **Run**. Then, enter **ftp** ***system IP address of the server*** and click **OK**. An FTP connection is established and a CLI is displayed.
   c. Enter **root** as the name for the OS user.
      ```
      User (IP_address:(none)):root
      ```
   d. Enter the password for the **root** user.

```
Password:
```

e. Set the format of the file to be transferred by FTP to ASCII.
```
ftp> ascii
```

f. Access the path where the license file is stored.
```
ftp> lcd PC_directory
```

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

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

i. Exit the FTP program.
```
ftp> quit
```

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

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

b. To update the U2000 license file, run the following commands:
```
# cd /opt/U2000/server
# . svc_profile.sh
# 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 master server of secondary site in ASCII mode by FTP as the **root** user. For details, **3.1**.

**Method two**: Load the license in the GUI.

Update the license on the master server of 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 (master 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 master server of 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 (SUSE Linux-distributed).

## 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 master servers on the primary and secondary sites as the **root** user.
2. Run the following commands to check the U2000 version:

   ```
   # 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 version of the U2000. If the displayed version does not meet the actual requirement, uninstall the U2000 and obtain the correct software version to install the U2000 again according.
3. Run the following command to check whether disk arrays are correctly mounted:

   ```
   # df -h
   ```

   Information similar to the following is displayed:

   ```
   Filesystem            size   used  avail capacity  Mounted on
   /dev/sda1              11G  2.1G  8.0G  21% /
   udev                  4.0G  260K  4.0G   1% /dev
   /dev/sda7              11G   33M   10G   1% /export/home
   /dev/sda6              80G   16G   65G  19% /opt
   /dev/sda3              11G  3.0G  7.1G  30% /usr
   /dev/sda5              11G  301M  9.8G   3% /var
   ```

```
tmpfs                 4.0K     0  4.0K   0% /dev/vx
/dev/vx/dsk/datadg/lvapp
                      197G  7.1G  180G   4% /opt/U2000
/dev/vx/dsk/datadg/lvoracle
                       20G  4.5G   15G  24% /opt/oracle
/dev/vx/dsk/datadg/lv_engr
                      5.0G  713M  4.0G  15% /opt/HWENGR
/dev/vx/dsk/datadg/lv_icmr
                      496M   41M  430M   9% /opt/HWICMR
/dev/vx/dsk/datadg/lv_backup
                      197G  188M  187G   1% /opt/backup
/dev/vx/dsk/datadg/lv_ftproot
                      296G  191M  281G   1% /share/ftproot
/dev/vx/dsk/datadg/lvdata
                      119G  51G  62G   45% /opt/oracle/oradb/data
```

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** Run the following commands to check the Veritas and version information.

1. To check the VxVM version, run the following command:

   ```
   # rpm -qa | grep VRTSvxvm
   ```

   If the VxVM version is correct, information similar to the following is displayed:

   ```
   VRTSvxvm-5.1.001.000-RP1_SLES10
   ```

   If the information to the right of **VRTSvxvm** is not **5.1.001.000-RP1_SLES10**, you must reinstall Veritas 5.1 and patches or contact Huawei engineers. For details, see **7.2 Preconfiguring the OS of the Master Server**.

2. To check the VCS version, run the following command:

   ```
   # rpm -qa | grep VRTSvcs
   ```

   If the VCS version is correct, information similar to the following is displayed:

   ```
   VRTSvcsag-5.1.001.000-RP1_SLES10
   VRTSvcsdr-5.1.00.00-GA_SLES10
   VRTSvcs-5.1.001.000-RP1_SLES10
   VRTSvcsea-5.1.001.000-RP1_SLES10
   ```

   Pay attention to information to the right of **VRTSvcs**. If the information to the right of **VRTSvcs** is not **5.1.001.000-RP1_SLES10**, you must reinstall Veritas 5.1 and patches or contact Huawei engineers. For details, see **7.2 Preconfiguring the OS of the Master Server**.

**5** Run the following command to check disk group status:

```
# vxdg list
```

Information similar to the following is displayed:

```
NAME         STATE           ID
datadg       enabled              1353913938.7.Site129
```

- 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** Run the following command to check disk status:

```
# vxdisk list
```

Information similar to the following is displayed:

```
DEVICE       TYPE            DISK         GROUP        STATUS
sda          auto:none       -            -            online invalid
sdb          auto:sliced     disk02       datadg       online
```

- 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** Run the following command to check disk volume status:

```
# vxprint -v
```

Information similar to the following is displayed:

```
Disk group: datadg

TY NAME         ASSOC        KSTATE   LENGTH   PLOFFS   STATE    TUTIL0  PUTIL0
v  lv_backup    fsgen        ENABLED  419430400 -       ACTIVE   -       -
v  lv_engr      fsgen        ENABLED  10485760 -        ACTIVE   -       -
v  lv_ftproot   fsgen        ENABLED  629145600 -       ACTIVE   -       -
v  lv_icmr      fsgen        ENABLED  1048576  -        ACTIVE   -       -
v  lvapp        fsgen        ENABLED  419430400 -       ACTIVE   -       -
v  lvdata       datarvg      ENABLED  251658240 -       ACTIVE   -       -
v  lvoracle     fsgen        ENABLED  41943040 -        ACTIVE   -       -
v  srl          datarvg      ENABLED  6291456  SRL      ACTIVE   -       -
```

**Reference Standards**

- For all the disk volumes, **KSTATE** must be **ENABLED**.
- For all the disk volumes, **STATE** must be **ACTIVE**.

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:

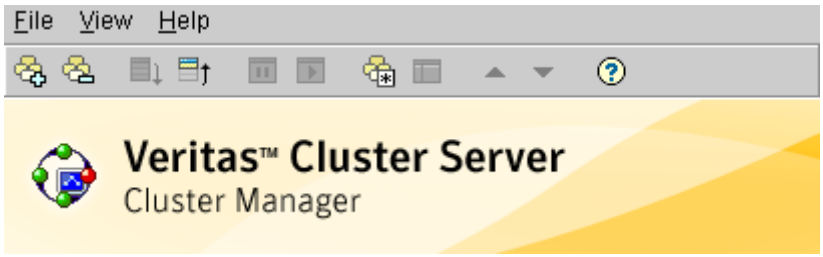
```
Replicated Data Set: datarvg
Primary:
  Host name:                    129.9.1.30
  RVG name:                     datarvg
  DG name:                      datadg
  RVG state:                    enabled for I/O
  Data volumes:                 1
  VSets:                        0
  SRL name:                     srl
  SRL size:                     3.00 G
  Total secondaries:            1

Secondary:
  Host name:                    129.9.1.40
  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
```

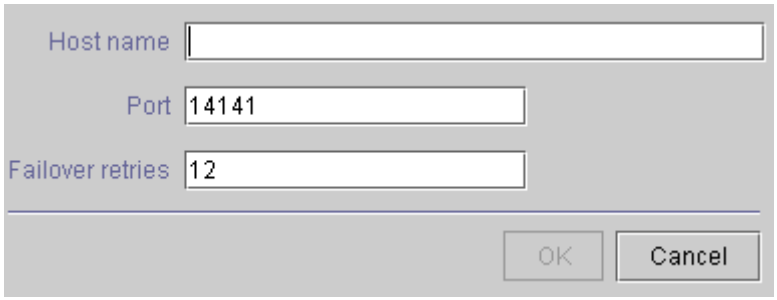
**9** Do as follows on the primary site to start the U2000 server:

1. To start the VCS client, run the following command:

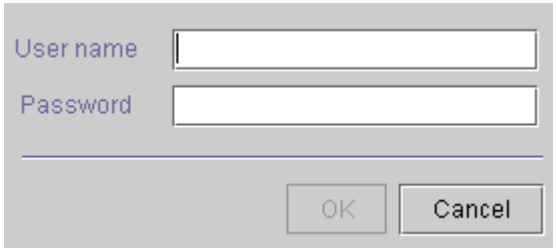
   ```
   # hagui &
   ```




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 ListenerRes, DatabaseServer, mountRes, NMSAgent, NMSServer and RVGPrimary, are in the Online on **Primaster** state, it indicates that the NMS server is started.

**10** Start a System Monitor client to view the running status of each process. Details are as follows:

**CAUTION**

The SUSE Linux OS is unavailable for a U2000 client or System Monitor client.

- To view the status of processes as the **root** user, run the following commands:

```
# cd /opt/U2000/server
# . svc_profile.sh
# svc_adm -cmd status -all
```

  **NOTE**

  Leave a space between the dot (.) and the command **svc_profile.sh**.

- Log in to the U2000 using an independent client. .

1. On the desktop of the OS, double-click the **U2000 System Monitor** shortcut icon.

   **NOTE**

   The default ACL range is the entire network segment. It is recommended that you set the ACL restriction range based on the security requirements. For details, see *iManager U2000 Commissioning Guide*.

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.

**----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.

## 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      9281     1  0 02:47 pts/0    00:01:55 /opt/HWNMSJRE/jre_linux/
     bin/java -server -Dlanguage=en -Xverify:none -Xmx128m -Xms64m -
     XX:MinHeapFreeRatio=10 -XX:MaxHeapFreeRatio=95 -XX:+UseParNewGC -XX:
     +UseConcMarkSweepGC -Dequinox.conf=engineering/conf/equinox.ini -
     Dos.native.path=engineering/lib -DCoreFramework.logFilePath=engineering/
     conf/loggerservice_Server.cfg -Djava.library.path=./engineering/lib/ -
     Drunway=install -DautoLogin=true -DinstallDiskMode=cmd -
     DinstallType=server -classpath ./engineering/lib/Launcher.jar:./
     engineering/lib/equinox.jar com.oss.core.launcher.Launcher
     ```

     **NOTE**

     If the displayed information contains **/opt/HWNMSJRE/jre_linux/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 **GNOME** session of the OS of the primary site as the **root** 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.<br>● 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.<br>● 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 master server 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 master server as the **root** 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 SUSE Linux OS
This topic provides the FAQs occurred in the SUSE Linux OS.

B.2 Veritas HA System
This topic covers FAQs about the Veritas HA system.

B.3 Oracle Database
This topic describes the FAQs about the Oracle database.

B.4 U2000 System
This topic covers FAQs about the U2000 system.

# B.1 SUSE Linux OS

This topic provides the FAQs occurred in the SUSE Linux OS.



## B.1.1 How to Start/Stop the FTP, TFTP, SFTP, and Telnet Services

### Question

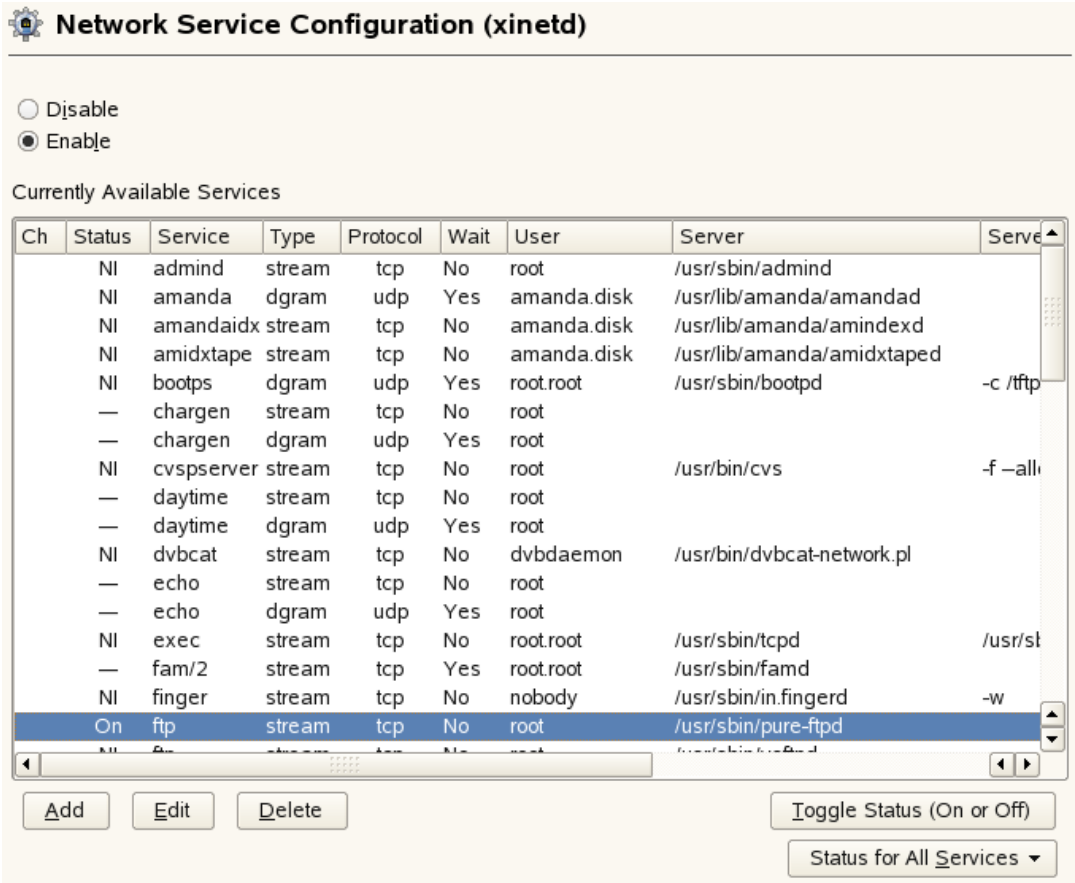
How to start/stop the FTP, TFTP, SFTP, and Telnet services in the SUSE Linux OS?

### Answer

- Perform the following operations for the FTP, TFTP and Telnet services:
  1. Run the following command in the **YaST2 Control Center** window as user **root** to enter the **Network Service Configuration** window:

     # **yast2 inetd**
  2. In the **Currently Available Services** list, select the FTP, TFTP, and Telnet services respectively, the following dialog box is displayed.

**Figure B-1** Starting the FTP, TFTP, and Telnet services




3. Click **Toggle Status (On or Off)** to configure the FTP, TFTP, and Telnet services respectively.

   **NOTE**

   - If **Status** is **On**, it indicates that the FTP service is started; if **Status** is **-**, it indicates that the FTP service is configured but not started; if **Status** is **NI**, it indicates that the FTP service is not configured.
   - When starting the FTP service, insert the OS disk and then click **OK** if the system prompts you to insert the OS disk.

4. Click **Finish**.

- Perform the following operations for the SFTP service:
  - Run the following command to start the SFTP service:

    # **service sshd start**
  - Run the following command to stop the SFTP service:

    # **service sshd stop**

**----End**

# B.1.2 How to Enable and Disable the FTP/Telnet Authority of the root User in the SUSE Linux OS?

## Question

How to Enable and Disable the FTP/Telnet Authority of the root User in the Solaris OS?

## Answer

- The method of enable the FTP authority of the root user is as follow:
  1. Log in to the SUSE Linux OS as the root user.
  2. Use the text editor to open the **ftpusers** file in the **/etc** directory. Add the comment tag (#) to the beginning of the following line in the **ftpusers** file to comment out this line:
     ```
     root
     ```
  3. Run the command **wq!** to save and close the **ftpusers** file.
- The method of disable the FTP authority of the root user is as follow:
  1. Log in to the SUSE Linux OS as the root user.
  2. Use the text editor to open the **ftpusers** file in the **/etc** directory. delete the comment tag (#) to the beginning of the following line in the **ftpusers** file:
     ```
     root
     ```
  3. Run the command **wq!** to save and close the **ftpusers** file.
- The method of enable the Telnet authority of the root user is as follow:
  1. Log in to the SUSE Linux OS as the root user.
  2. Edit the **/etc/securetty**file, run the following command:
     ```
     # vi /etc/securetty
     ```
  3. Add the following character string to the end of the file:

     **pts/0**

     **pts/1**

     **pts/2**

     **pts/3**

     **pts/4**

     **pts/5**

     **pts/6**

     **pts/7**
  4. Run the command **wq!** to save and close the **securetty** file.
- The method of disable the Telnet authority of the root user is as follow:
  1. Log in to the SUSE Linux OS as the root user.
  2. Edit the **/etc/securetty**file, run the following command:
     ```
     # vi /etc/securetty
     ```
  3. delete the following character string to the end of the file:

     **pts/0**

**pts/1**

**pts/2**

**pts/3**

**pts/4**

**pts/5**

**pts/6**

**pts/7**

4. Run the command **wq!** to save and close the **securetty** file.

**----End**

# B.1.3 How to Check Disk Partitions

## Question

How do I check disk partitions?

## Answer

1 Run the following command in the terminal window to open the **YaST2 Control Center** window.

# **yast2**

NOTE

If the GUI is unavilable, run the **yast** command to start the **YaST Control Center**.

2 Select **System** on the left.

3 Select **Partitioner** on the right.

4 Carefully read the information in the **Warning** dialog box, and then click **Yes**.

5 In the **Expert Partitioner** window, view the disk partition information and check whether the partitions meet the requirements of the U2000 system software.

**----End**

# B.1.4 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.1.5 How to Monitor System Processes and Application Ports?

## Question

How to monitor system processes and application ports after the SUSE Linux OS is installed?

## Answer

Click the **Computer** > **More Applications** > **System** > **GNOME System Monitor** to manage processes or run the **ps -ef | grep** *processe name* command to view processes. You can run the **vmstat** or **top** command to view the usage of the CPU, memory, and I/O bus.

# B.1.6 How to Log In to the OS Through the Remote Login Tools?

## Question

What should I do when I fail to log in to the SUSE Linux OS through the remote login tools?

## Answer

1. Log in to the OS as user **root**.
2. Run the following command in the terminal window:

   # **yast remote allow set=yes**

   # **rcxdm restart**
3. Use the remote login tools to log in to the U2000 server again.

**----End**

# B.1.7 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.1.8 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.1.9 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. |
| **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.1.10 How to Change the Time and Time Zone of the SUSE Linux OS?

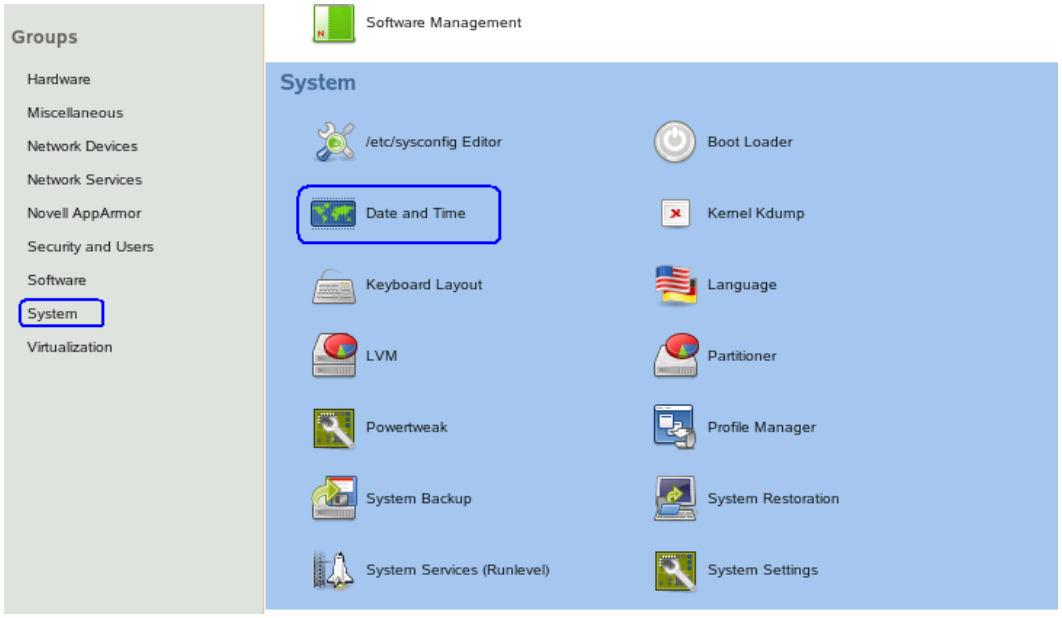
## Question

How to change the time and time zone of a SUSE Linux OS where the U2000 is nt installed yet?

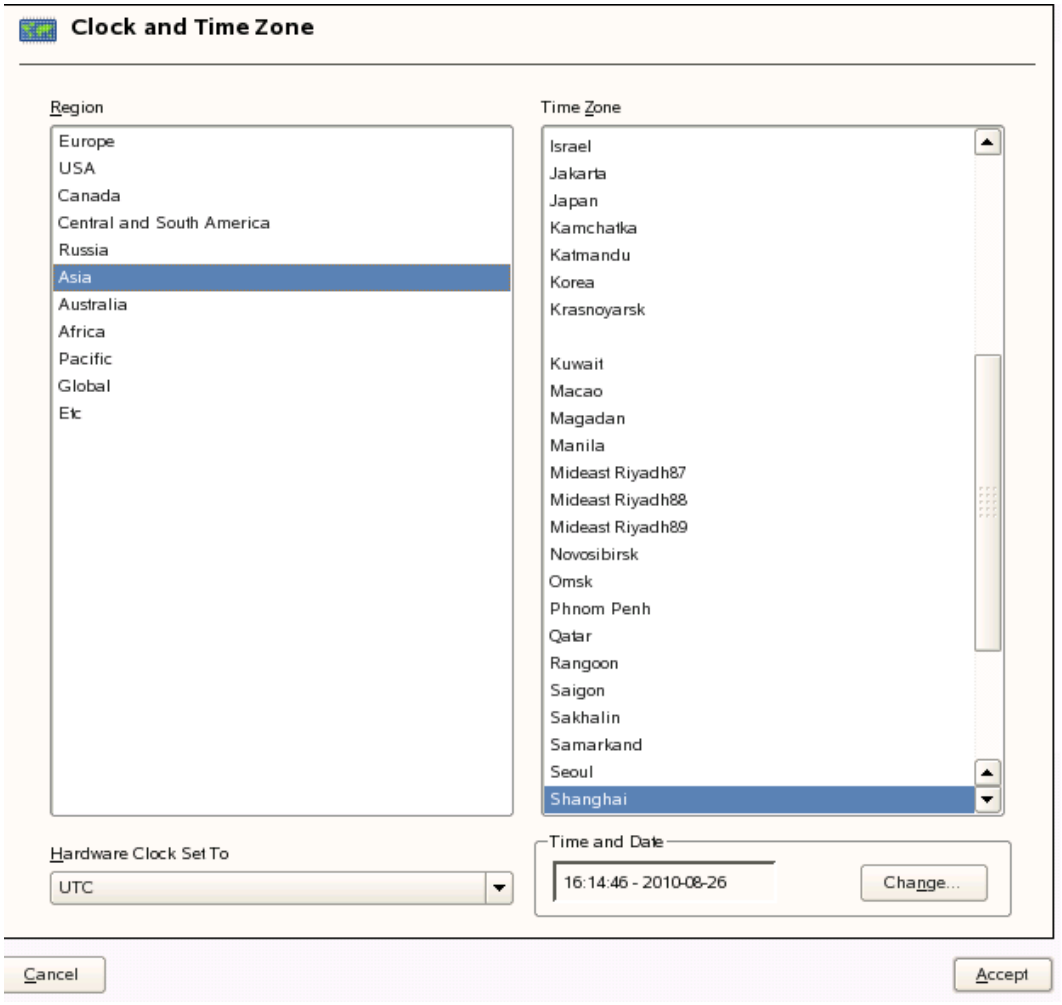
## Answer

1. Log in to the graphical desktop system of the SUSE Linux OS as the **root** user.
2. Open the CLI and run the following command to start the YaST2 control center.
   ```
   # yast2
   ```

3 Choose **System** > **Date and Time**.




4 In the dialog box that is displayed, set the area and time zone.



5 To change the time, click **Change**. In the dialog box that is displayed, set the date and time, and then click **Apply**.

6 Click **Accept**.

7 To restart the OS ,run the following commands:

```
# sync;sync;sync;sync
# shutdown -r now
```

**----End**

# 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.2.1.1 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?

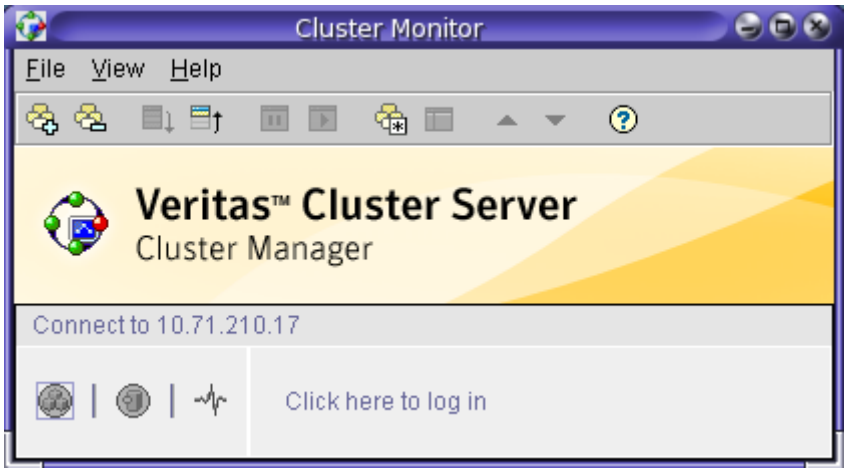
### Answer

**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.

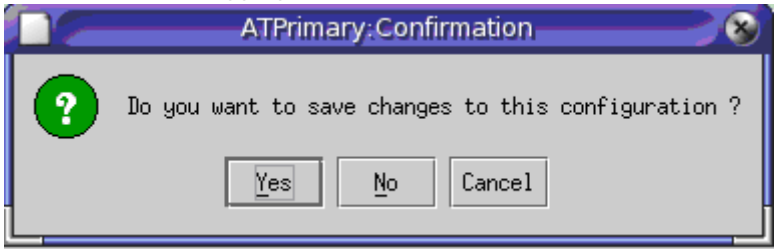
4. Click **OK**.

**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:<br>● **state** is set to **ACTIVE**.<br>● **kernel** is set to **ENABLED**. |
| assoc | Indicates the association information about the RVG.<br>● **datavols** indicates the data disk volume that the RVG contains.<br>● **srl** indicates the SRLog disk volume that the RVG contains.<br>● **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**. |
| 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. |

| Field | Description |
|---|---|
| info | Indicates the information about the Rlink.<br>● **timeout** indicates the timeout period.<br>● **rid** indicates the ID of the Rlink.<br>● **latency_high_mark** indicates the highest delay flag.<br>● **latency_low_mark** indicates the lowest delay flag.<br>● **bandwidth_limit** indicates the bandwidth limit. |
| state | Indicates the status of the Rlink. In normal cases, the situations are as follows:<br>● **state** is set to **ACTIVE**.<br>● **synchronous** is set to **off**.<br>● **latencyprot** is set to **off**.<br>● **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?

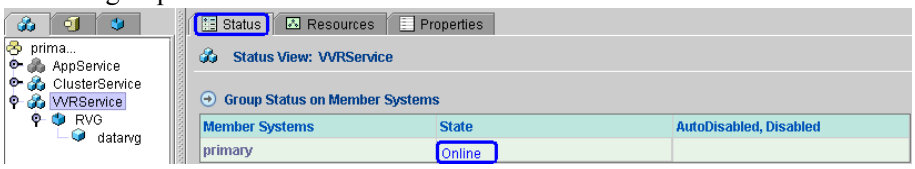
## Answer

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:

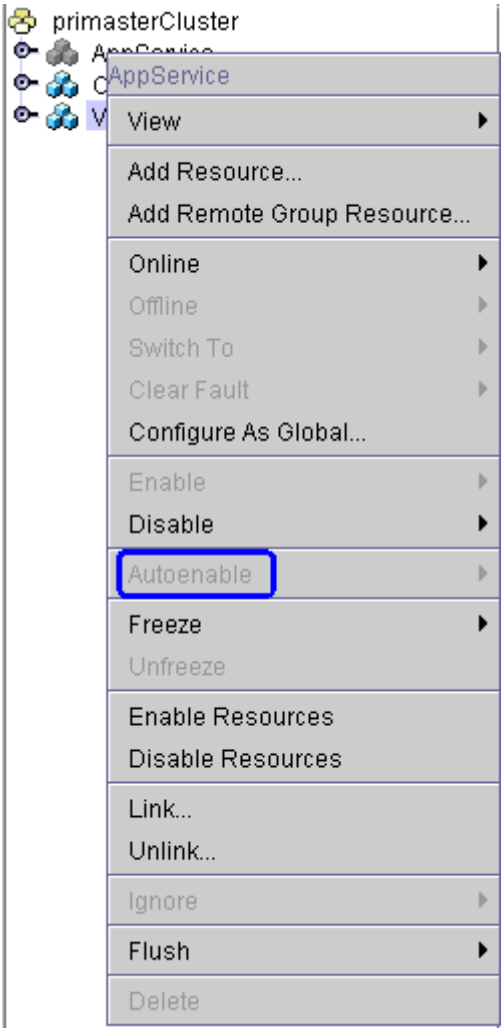
1. Right-click the VVRService resource group and choose **Online** > **host name** from the shortcut menu.
2. In the dialog box that is displayed, click **Yes** to make the resource group online.

**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 Oracle Database

This topic describes the FAQs about the Oracle database.



# B.3.1 How to Check Whether the Oracle Database Has Been Installed

## Question

How to check whether the Oracle database has been installed?

### Answer

NOTE

- If the Oracle database has not been installed, when you install the U2000, the Oracle database is automatically installed along with the U2000.
- If the Oracle database has been installed, when you install the U2000, a dialog box is displayed asking you whether to reuse the Oracle database. If you choose to reuse it, you do not need to re-install the Oracle database and thus can save time; if you choose not to reuse it, you need to re-install the Oracle database. Generally, it is recommended that the Oracle database not be reused.

- Consult the PC administrator to learn whether the Oracle database has been installed.
- Check whether the installation directory and file of the Oracle database exist. A sample directory is **/opt/oracle**.
- Check whether the Oracle database has been started and whether the version of the Oracle database is correct. For details, see **B.3.6 How Can I Check Whether the Oracle Database Is Started?**. For details about how to start the Oracle database, see **B.3.4 How to Start the Oracle Database in the High Availability System**.

**----End**

## B.3.2 How to Check the Version of the Oracle Database

### Question

How to check the version of the Oracle database?

### Answer

See **B.3.6 How Can I Check Whether the Oracle Database Is Started?**.

## B.3.3 How to Check the Name of the Oracle Database

### Question

How to check the name of the Oracle database?

### Answer

1. Log in to the SUSE Linux OS as the **oracle** user.

   NOTE

   The **oracle** user is the user that manages the Oracle database.

2. Run the following command to connect to the Oracle database:

   ```
   $ sqlplus / as sysdba
   ```

3. Run the following command to check the name of the Oracle database:

   ```
   SQL> select name from v$database;
   ```

   Information similar to the following is displayed:

   ```
   NAME --------- U2KDB
   ```

**NOTE**

Alternatively, you can run the following command to check **db_name**:
`SQL> show parameter db`

**----End**

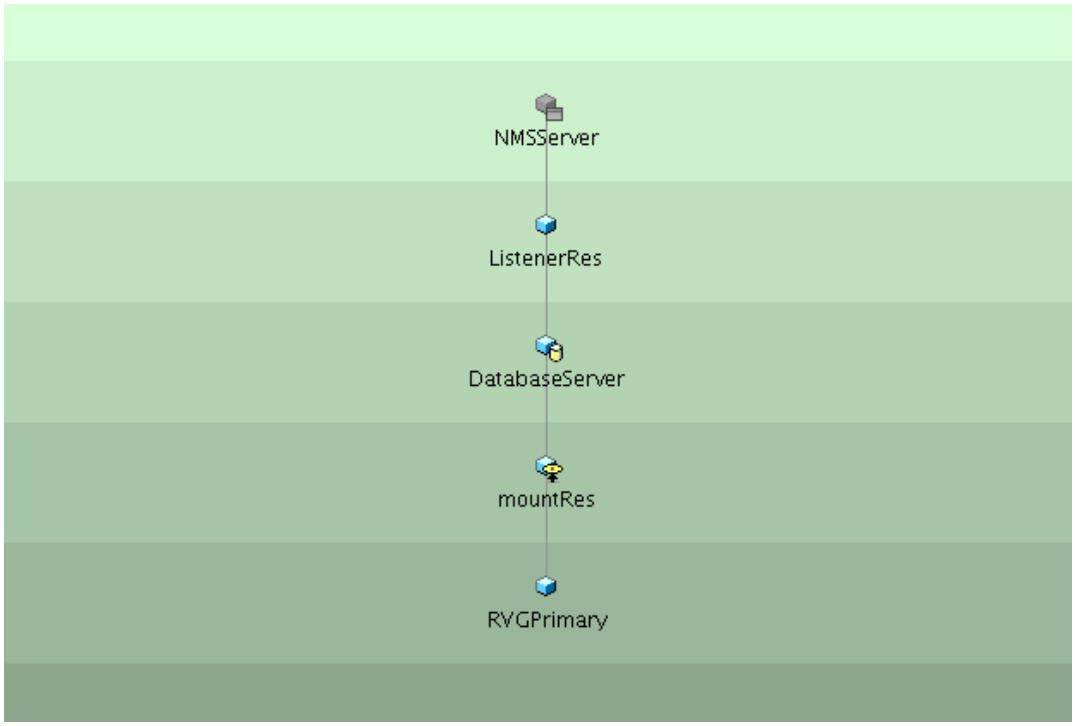
# B.3.4 How to Start the Oracle Database in the High Availability System

## Question

How do I start the Oracle database?

## Answer

1. Log in to the OS as user **root**.
2. Open the CLI.
3. To start the VCS client, run the following command:
   `# hagui&`
4. Choose **File** > **New Cluster**. Then, enter the server IP address and click **OK**.
5. Enter the default user name **admin** and default password **password** of the VCS client, and then click **OK**.
6. Select the **AppService** node. In the right-hand pane, click the **Resources** tab.
7. Right-click **ListenerRes** and choose **Online** > ***host name*** from the shortcut menu.
   Wait until information shown in the following figure is displayed indicating that the Oracle database is started.




**----End**

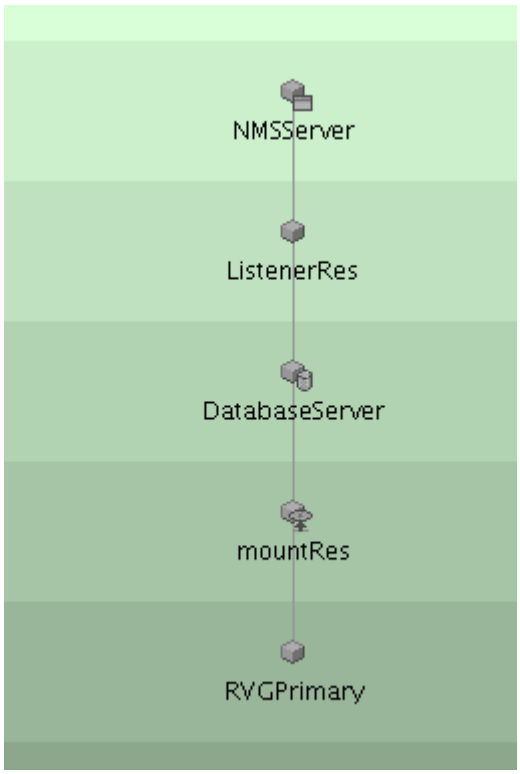
# B.3.5 How to Shut Down the Oracle Database (High Availability System)

## Question

How do I shut down the Oracle database?

## Answer

1. Log in to the OS as user **root**.
2. Open the CLI.
3. To start the VCS client, run the following command:
   ```
   # hagui&
   ```
4. Choose **File** > **New Cluster**. Then, enter the server IP address and click **OK**.
5. Enter the default user name **admin** and default password **password** of the VCS client, and then click **OK**.
6. Choose **AppService** from the navigation tree. In the right-hand pane, click the **Resources** tab.
7. Right-click **ListenerRes** and choose **Offline** > ***host name*** from the shortcut menu.
   Wait until information shown in the following figure is displayed indicating that the Oracle database is shut down.




**----End**

# B.3.6 How Can I Check Whether the Oracle Database Is Started?

## Question

How Can I Check Whether the Oracle Listener Is Started?

## Answer

1 Log in to SUSE Linux as **oracle**.

NOTE

**oracle** is a user who manages the Oracle database.

2 In the command prompt window, run the following command to connect to the Oracle database:

$ **sqlplus / as** *sysdba*

3 On the CLI, run the following command to check whether the Oracle database is installed successfully by viewing the version information:

> **select * from v$version;**

The following is a display sample:

```
BANNER
--------------------------------------------------------------------------------
Oracle Database 11g Enterprise Edition Release 11.1.0.7.0 - 64bit Production
PL/SQL Release 11.1.0.7.0 - Production
CORE    11.1.0.7.0      Production
TNS for Linux: Version 11.1.0.7.0 - Production
NLSRTL Version 11.1.0.7.0 - Production
```

The information indicates that the Oracle database is connected and started successfully. You can query data normally.

Otherwise, for HA system, see **B.3.4 How to Start the Oracle Database in the High Availability System** to start the Oracle database.

**----End**

# B.3.7 How Can I Check Whether the Oracle Listener Is Started?

## Question

How Can I Check Whether the Oracle Listener Is Started?

## Answer

1 Log in to SUSE Linux as **oracle**.

NOTE

**oracle** is a user who manages the Oracle database.

2 On the CLI, run the following command to view the state of the Oracle listener:

$ **lsnrctl status**

The following is a display sample:

```
STATUS of the LISTENER
------------------------
```

```
Alias                     LISTENER
Version                   TNSLSNR for Linux IA64: Version 10.2.0.3.0 - Production
Start Date                23-MAR-2009 10:16:36
```

Here,**STATUS of the LISTENER**indicates that the Oracle listener is already started. If the listener is not restarted, run the following command on the CLI to start the listener:

$ **lsnrctl start**

**----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 **root**.

2. 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 (SUSE Linux-Distributed) Are Started

## Question

How to check whether the U2000 processes of the high availability system (SUSE Linux-distributed) are started?

## Answer

**1** Log in to the OS of the master server on the active site as the **root** user.

**2** Check the U2000 processes.

To check whether U2000 processes are started, run the following commands:

```
# cd /opt/U2000/server
# . svc_profile.sh
# daem_ps
```

**NOTE**

Leave a space between the dot (.) and the command **svc_profile.sh**.

Information similar to the following is displayed:

```
root     11800     1  0 15:09 ?        00:00:02 /opt/U2000/server/bin/imapmrb
root     11909     1  0 15:09 ?        00:00:00 imapwatchdog -cmd start
root     11902     1  1 15:09 ?        00:00:10 imapsysd -cmd start
root     11906     1  0 15:09 ?        00:00:00 imapeventmgr
root     12479 11909  2 15:09 ?        00:00:11 /opt/U2000/server/bin/
imap_sysmonitor -cmd start >/dev/null 2>&1
root     11948     1  0 15:09 ?        00:00:02 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 (SUSE Linux-Distributed)

## Question

How do I start the U2000 processes of the high availability system (SUSE Linux-distributed)?

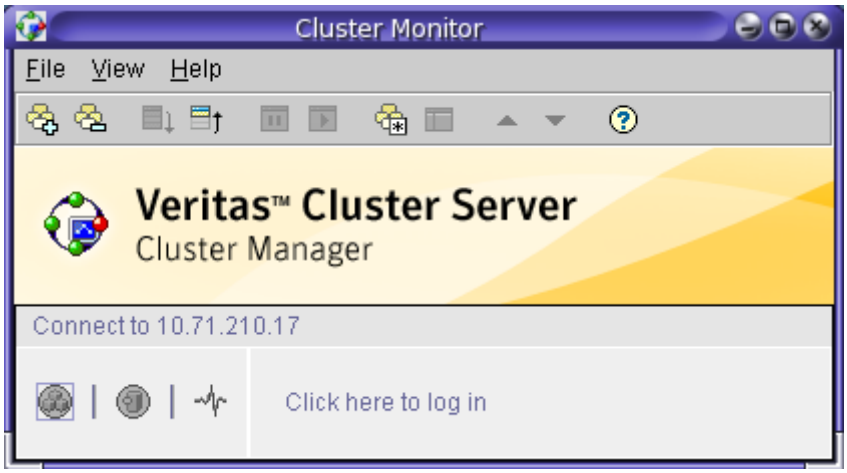
## Answer

**1** Log in to the OS of the master server at 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 (SUSE Linux-Distributed)

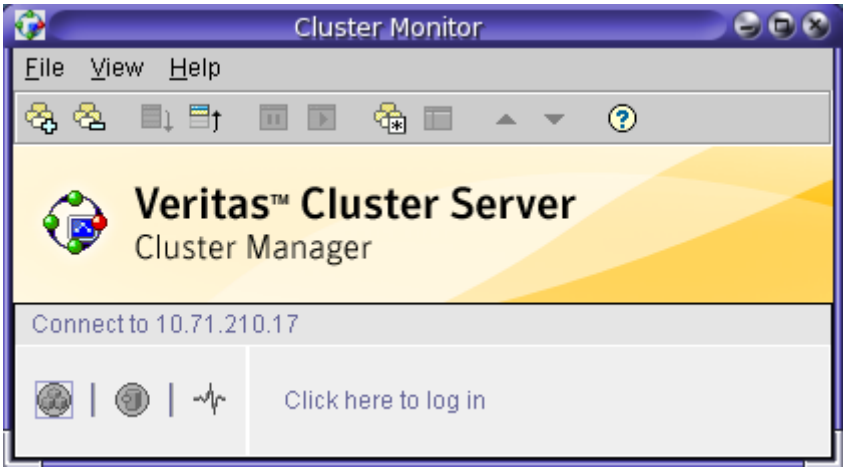
## Question

How do I end the U2000 processes of the high availability system (SUSE Linux-distributed)?

## Answer

1. Log in to the OS of the master server on the active 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. 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 Configure the ipmap.cfg Mapping File

## Question

If NAT networking is applied in a distributed system, after the U2000 software is installed or the server IP address is changed, the **ipmap.cfg** mapping file need to be manually configured on the master server. How do I configure the **ipmap.cfg** mapping file?

## Answer

**1** Obtain and record the following IP addresses.

**TIP**

- You can obtain system IP addresses of servers in the distributed system from the NMS administrator. Alternatively, run the **ifconfig -a** command on the servers. The IP addresses indicated by **bond0** are system IP addresses of the servers.
- To obtain private IP addresses of servers in the distributed system, run the **ifconfig -a** command on the servers. The IP addresses indicated by **bond1** are private IP addresses of the servers.
- You can obtain the public IP address of the NAT server from the NMS administrator.

**Table B-4** Mapping relationship between U2000 IP addresses and NAT server IP addresses

| System IP Addresses of All Servers in the Distributed System | Private IP Addresses of All Servers in the Distributed System | Public IP Addresses of the NAT Server |
|---|---|---|
| System IP address of the master server. For example, *129.9.1.30*. | Private IP address of the master server. For example, *192.168.100.20*. | Public IP address 1 on the NAT server. For example, *10.1.1.10*. |
| System IP address of slave server 1. For example, *129.9.1.31*. | Private IP address of slave server 1. For example, *192.168.100.21*. | Public IP address 2 of the NAT server. For example, *10.1.1.11*. |
| System IP address of slave server 2. For example, *129.9.1.32*. | Private IP address of slave server 2. For example, *192.168.100.22*. | Public IP address 3 of the NAT server. For example, *10.1.1.12*. |
| ... | ... | ... |
| System IP address of slave server N: | Private IP address of slave server N. | Public IP address N of the NAT server. |

**2** Log in to the master server as user **root**.

**3** Open a terminal window. Run the associated commands to access the **server/etc/conf** directory in the U2000 installation path. For example, if the default installation path of the U2000 is **/opt/U2000**, run the following command:

```
cd /opt/U2000/server/etc/conf
```

**4** Run the **vi** command to modify the **ipmap.cfg** file.

1. If the **ipmap.cfg** file exists in the installation path, run the following command to delete the file. If the **ipmap.cfg** file does not exist in the installation path, directly go to **4.2**.
   ```
   rm -f ipmap.cfg
   ```
2. Create and modify the **ipmap.cfg** file.
   ```
   vi ipmap.cfg
   ```

3. Run the **vi** command to modify the **ipmap.cfg** file. The following uses the IP address collected in Step 1 as an example.

```
internal=129.9.1.30,client=10.1.1.10,server=192.168.100.20
internal=129.9.1.31,client=10.1.1.11,server=192.168.100.21
internal=129.9.1.32,client=10.1.1.12,server=192.168.100.22
```

   **NOTE**

   The statement format is as follows: **internal** = **System IP address of the server**, **client** = **Public IP Addresses of the NAT Server**

4. After the **ipmap.cfg** file is modified, save the file and exit.

**----End**

# B.4.6 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.4.7 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-5** Software required for installation (blade server)

| Software | Medium Description |
| --- | --- |
| SUSE Linux OS | You can install the SUSE Linux OS through the quick installation disk or common installation disk.<br>● Quick installation DVD: U2000***version***_server_ha_os_en_sles_x64_dvd2<br>● Common installation DVD: SUSE Linux 10 Enterprise Server 10 SP3 |
| Database | ● Installation DVD: U2000***version***_server_db_sles_x64_dvd3<br>● Installation package: U2000***version***_server_db_sles_x64.tar |
| Veritas Software | Veritas software installation DVD or installation package<br>● Veritas software installation DVD: Storage Foundation and HA Solutions 5.1 for SuSE Linux<br>● Veritas software installation package: veritas5.1_sles_x64.tar.gz<br>● Veritas patch installation DVD: U2000***version***_server_patch_sles_x64_dvd2<br>● Veritas patch installation package: U2000***version***_server_veritas5-1_patch_sles_x64.tar |

| Software | Medium Description |
| --- | --- |
| U2000 server software | Installation DVD or installation package<br>● Installation DVD: U2000***version***_server_nms_sles_x64_dvd4<br>● Installation package:<br>**NOTE**<br>Prepare software packages required by the components to be installed.<br>– Basic component:<br>U2000***version***_server_nmsbase_sles_x64.tar<br>**It must be available.** It is used to install the U2000.<br>– Core component:<br>U2000***version***_server_nmscore_sles_x64.tar<br>**It must be available.** It is used to install the U2000.<br>– Transport domain component:<br>U2000***version***_server_nmstrans_sles_x64.tar<br>**It is required only if the U2000 needs to manage Huawei transport equipment**. Huawei transport equipment includes:<br>– MSTP equipment<br>– WDM equipment<br>– NA WDM equipment<br>– Submarine equipment<br>– RTN equipment<br>– PTN equipment<br>– IP domain component:<br>U2000***version***_server_nmsip_sles_x64.tar<br>**It is required only if the U2000 needs to manage Huawei IP equipment**. Huawei IP equipment includes:<br>– Routers<br>– Switches<br>– Metro service equipment<br>– Broadband access equipment<br>– VoIP gateways<br>– Firewalls<br>– Service inspection gateway<br>– SVN equipment<br>– Access domain component:<br>U2000***version***_server_nmsaccess_sles_x64.tar<br>**It is required only if the U2000 needs to manage Huawei access equipment**. Huawei access equipment includes:<br>– FTTx equipment<br>– MSAN equipment<br>– DSLAM equipment |

# B.4.8 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 SUSE Linux OS, the message is as follows:

```
The communication port (12212,12213,12214,12215) of the installation framework is
used. Run the "/bin/netstat -ant" 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.4.9 How to Check Whether the daem Process Is Started

## Question

The NMS server processes can be started only after the daem process of the slave server is started. In normal cases, the daem process is started along with the SUSE Linux OS. How do I check whether the daem process is started?

## Answer

1. Log in to the OS of the server as user **root**.
2. Open a terminal window and run the following command:

   ```
   # ps -ef|grep start
   ```

   Information similar to the following is displayed:

   ```
   root      1702     1  0 20:48 pts/0    00:00:00 /bin/bash ./start_daem -type
   StandbyNode
   root      1770  1702  1 20:48 pts/0    00:00:00 /opt/U2000/server/3rdTools/python/
   bin/python /opt/U2000/server/bin/script/start_daem.py -type StandbyNode
   root      1782  1355  0 20:48 pts/0    00:00:00 grep start
   ```

   Or a message similar to the following will be displayed:

   ```
   root 27069     1   0 10:31:39 ?           1:39 imapmrb
       root 27079     1   0 10:31:39 ?           0:00 imapwatchdog -cmd start
       root 27075     1   0 10:31:39 ?           0:50 imapsysd -cmd start
       root 27086     1   0 10:31:39 ?           0:09 imapeventmgr
       root 23679     1   1 17:57:06 pts/8       0:02 imap_sysmonitor -cmd start
       root 27116     1   0 10:31:40 ?           0:52 ResourceMonitor -cmd start
   ```

NOTE

If **/bin/bash ./start_daem -type StandbyNode**, **/opt/U2000/server/3rdTools/python/bin/python**, or **imapsysd -cmd start** is displayed, the daem process of the slave server has been started.

**----End**

# B.4.10 How to Start the daem Process

## Question

In normal cases, the daem process is started along with the SUSE Linux OS. If the daem process is not started, how do I start it?

## Answer

1. Log in to the OS of the server as user **root**.
2. Open a terminal window and run the following command:
   ```
   # /etc/init.d/u2kdaem start
   ```

**----End**

# B.4.11 How to End the daem Process

## Question

How do I end the daem process in the SUSE Linux OS?

## Answer

1. Log in to the OS of the server as user **root**.
2. Open a terminal window and run the following command:
   ```
   # /etc/init.d/u2kdaem stop
   ```

**----End**

# B.4.12 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.4.13 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.4.14 How to Set the Communication Mode of the Server in a High Availability System (SUSE Linux-Distributed)

## Question

The server in a high availability system (SUSE Linux-distributed) 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 (SUSE Linux-distributed), 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 master server as user **root** and run the following commands to query the current communication mode.

```
# cd /opt/U2000/server
# . svc_profile.sh
# ssl_adm -cmd query
```

**NOTE**

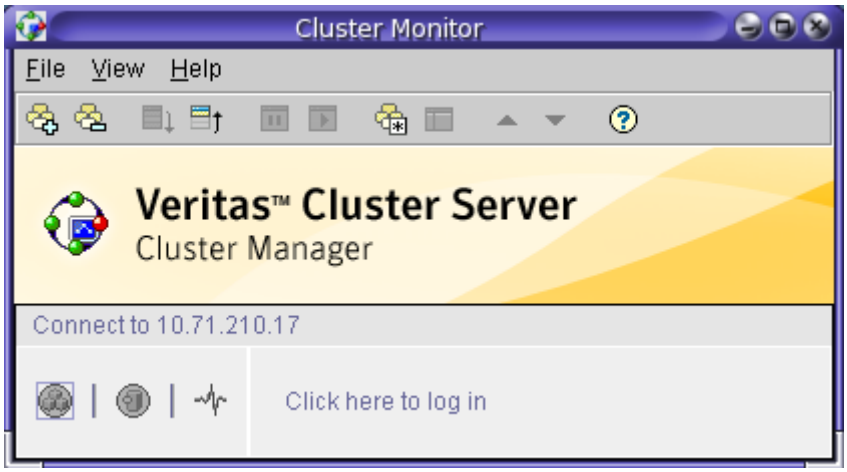
In the **. svc_profile.sh** command, there is a space between **.** and **svc_profile.sh**.

2 Log in to the OS of the master server on the active site as user **root**.

3 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.

**4** 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.

**5** Run the following command to configure the master server communication mode.

```
#  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.

**6** Run the following command to configure the slave server communication mode.

**NOTE**

- If there is no slave server, skip this step.
- If there are multiple slave servers, perform this step on each slave server.

1. Log in to the slave server as user **root** and run the following commands to stop the daem process.

```
# /etc/init.d/u2kdaem stop
```

2. Run the following command to configure the slave server communication mode.

```
# 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.

**7** Restart the daem process.

**NOTE**

- If there is no slave server, skip this step.
- If there are multiple slave servers, perform this step on each slave server.

```
# /etc/init.d/u2kdaem start
```

**8** 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.

**9** 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.
- In the scenario where a high availability system (SUSE Linux-distributed) needs to be uninstalled, ensure that the public network and private network must be interconnected for the master servers and slave servers on the primary and secondary sites. Otherwise, the high availability system (SUSE Linux-distributed) fails to be uninstalled properly.

**CAUTION**

- Step 1 to Step 3 needs to be performed only on the server on the active site. Step 4 to Step 10 must be performed on both the primary and secondary sites.
- In the scenario where a high availability system (SUSE Linux-distributed) needs to be uninstalled, you need to uninstall the U2000 software only on the master servers on the primary and secondary sites.

## Procedure

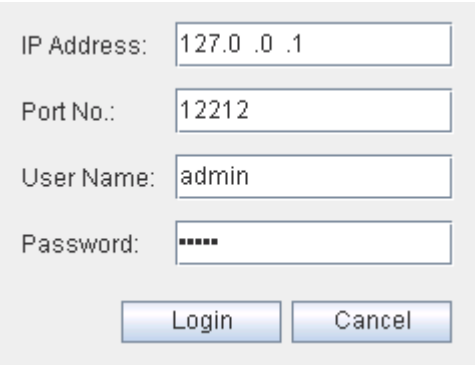
**1** Log in to the **GNOME** session of the master server at primary site OS as the **root** user.

**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.<br>● 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.<br>● 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** Navigate to the following path and then run the environment variable:

```
# cd /opt/U2000/server
# . svc_profile.sh
```

**NOTE**

Leave a space between the dot (.) and **svc_profile.sh**.

**4** 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:

```
root     11800     1  0 15:09 ?        00:00:02 /opt/U2000/server/bin/imapmrb
root     11909     1  0 15:09 ?        00:00:00 imapwatchdog -cmd start
root     11902     1  1 15:09 ?        00:00:10 imapsysd -cmd start
root     11906     1  0 15:09 ?        00:00:00 imapeventmgr
root     12479 11909  2 15:09 ?        00:00:11 /opt/U2000/server/bin/
imap_sysmonitor -cmd start >/dev/null 2>&1
root     11948     1  0 15:09 ?        00:00:02 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:

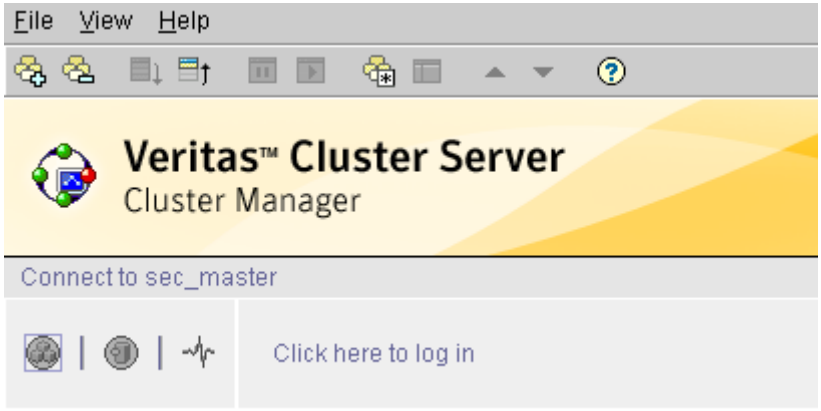
1. On the primary site, log out as the **nmsuser** user and then log in the OS again as the **root** user.
2. Open a CLI. Then, run the following command to start the VCS client:

   **NOTE**

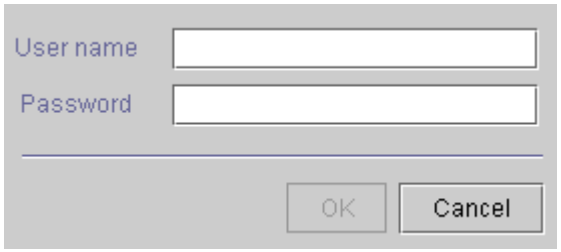
   If the server does not have the GUI desktop, run the following commands to stop the U2000 processes and start the database:

   ```
   # hares -offline NMSServer -sys host name
   # hares -online DatabaseServer -sys host name
   ```

   ```
   # 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 **DatabaseServer** is in the **Online on *host name*** state, it indicates that the database has been started.

**5** Run the following commands to check whether the database status is correct:

```
# cd /opt/U2000/server
# . svc_profile.sh
[ /opt/U2000/server ]testDB
```

**NOTE**

Leave a space between the dot (.) and the command **svc_profile.sh**.

- If no information is displayed, it indicates that the database status is correct.
- If the following information is displayed, it indicates that the database status is abnormal:
  ```
  testDB catch an unknown database exception.
  ORA-12541: TNS:no listener
  ```
  In this case, do as follows:
  1. Ensure that all resources in the AppService resource group are in the **Enable** state. If any resource is not in the **Enable** state, log in to the VCS browser, select the AppService resource group, right-click, and then choose **Enable** > **hostname** from the shortcut menu.
  2. On the **Resources** tab page of the AppService resource group, select the **ListenerRes** resource, right-click, and then choose **Online** > **hostname** from the shortcut menu.

**6** Run the following commands on the server on the primary and secondary sites to stop the MSuite server:

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

**CAUTION**

In a high availability system (SUSE Linux-distributed), this step needs to be performed only on the master servers on the primary and secondary sites. Performing this step on the slave servers to shut down the Network Management System Maintenance Suite servers on the slave servers is prohibited.

**7** Log in to the slave servers on the OS on the primary and secondary sites as the **root** user. Then, open a CLI and run the following command to stop daem processes.

```
# /etc/init.d/u2kdaem stop
```

**NOTE**

Perform this step on each slave server.

**8** 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.

**9** 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.

**10** After the uninstall is complete, the **Uninstallation Complete** dialog box is displayed.

11 Click **Finish**.

12 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 master server as user **root**.

2 Confirm that the installation path is correct during the uninstall.

The NMS installation path **/opt/U2000**, is 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: user nmsuser does not exist
```

**----End**

# D Getting Started

This topic describes certain common operations that can be performed on the SUSE Linux workstation. After learning this topic, you can improve the efficiency of the operations in the SUSE Linux OS.

## Syntax Structure of Command Lines

The syntax structure of command lines is as follows:

```
command option parameter
```

The SUSE Linux 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 SUSE Linux 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
```

## 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. |
| fdisk *option* | fdisk *-l* | Views the quantity of disks. |

| Command/Usage | Example | Description |
|---|---|---|
| q | | Exits the man query. |

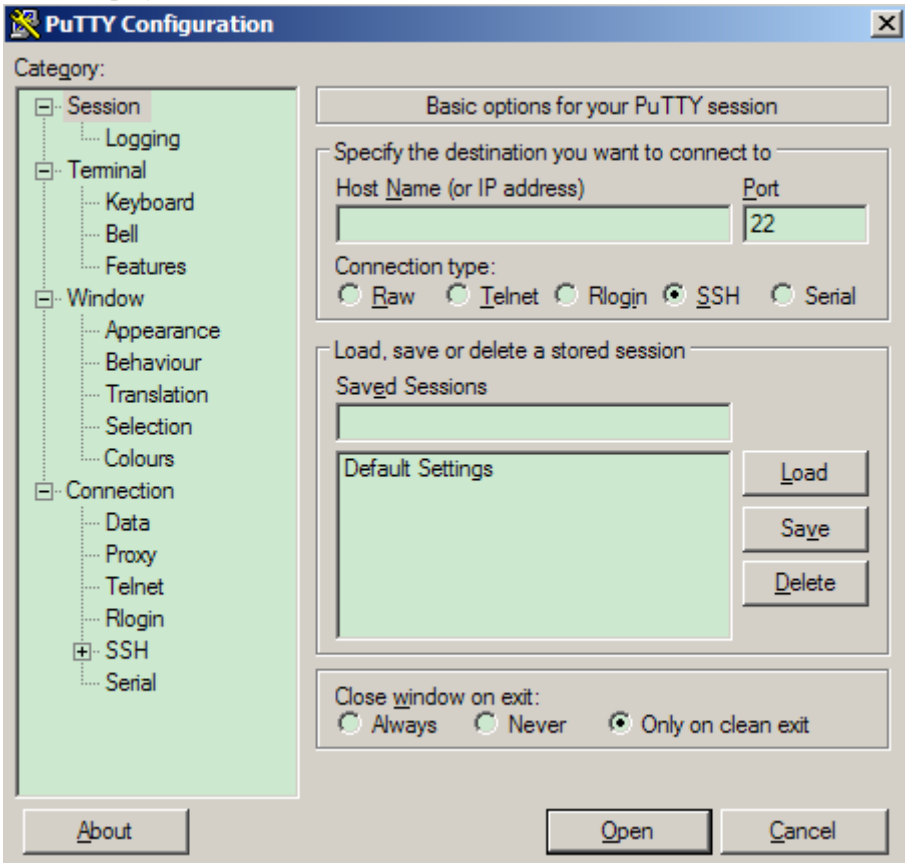
## Logging In to the SUSE Linux OS Through Remote Login Software

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. |

| Parameter | Description |
| --- | --- |
| 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 SUSE Linux 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 SUSE Linux OS

Run the following commands to restart the OS:

```
# sync;sync;sync;sync
# shutdown -r
```

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 (SUSE Linux-Distributed)

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 Oracle process.

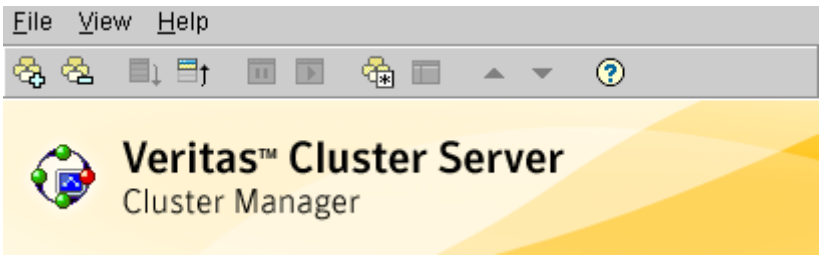
   Check whether the U2000 processes are stopped. Do as follows:

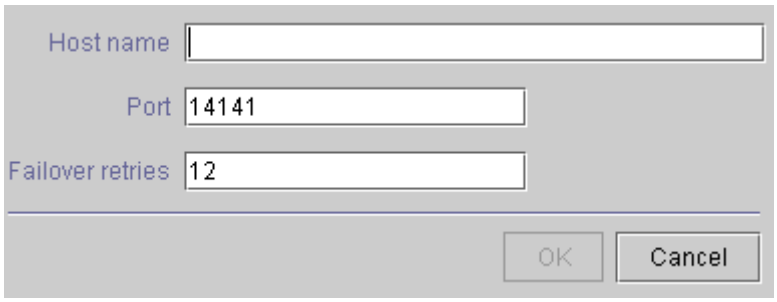
   1. Access the **GNOME** session process of the OS of the master server of the active site as the **root** user.

      **NOTE**

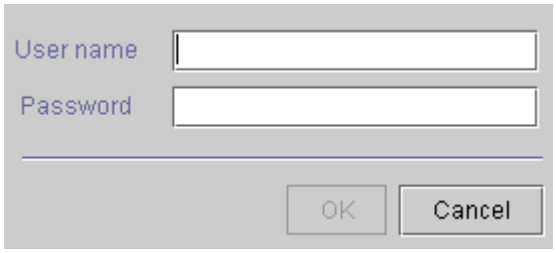
      Do as follows to access the **GNOME** session process: Select **GNOME** from **Session Type**.
   2. Run the following command to start the VCS client:

      ```
      # hagui &
      ```

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




4. Enter the system IP address of the master server 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 OS of the master server of the active site as the **root** user 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 master server of the standby site as the **root** user and perform the **3** and **4** orderly to stop the VCS service on the master server of the standby site.

**6** Shut down the OS of the slave server of the standby site.

**NOTE**

If the standby site has multiple slave servers, do as follows on each slave server:

1. Log in to the OS of the slave server of the standby site as the **root** user.
2. Run the following command to shut down the OS of the slave server of the standby site:

```
# sync;sync;sync;sync
# shutdown -h now
```

**7** Shut down the OS of the master server of the standby site.

1. Log in to the OS of the master server of the standby site as the **root** user.
2. Run the following command to shut down the OS of the master server of the standby site:

```
# sync;sync;sync;sync
# shutdown -h now
```

**8** Shut down the OS of the slave server of the active site.

**NOTE**

If the active site has multiple slave servers, do as follows on each slave server:

1. Log in to the OS of the slave server of the active site as the **root** user.
2. Run the following command to shut down the OS of the slave server of the active site:

```
# sync;sync;sync;sync
# shutdown -h now
```

**9** Run the following command to shut down the OS of the master server of the active site:

```
# sync;sync;sync;sync
# shutdown -h now
```

**----End**

# F Manually Installing the SUSE Linux OS and Its Patches

This topic describes how to manually install the OS by using the SUSE Linux installation DVD delivered with the product.

F.1 Installing the SUSE Linux OS
This topic describes how to install the SUSE Linux OS.

F.2 Verifying the Installation and Configuration of the OS
This topic describes how to check the OS version, OS patch, the disk partitioning of the system and the language environment variable of the system.

# F.1 Installing the SUSE Linux OS

This topic describes how to install the SUSE Linux OS.

## Prerequisite

- The MAC addresses of NICs through which blade servers are connected to the public network must be collected.
  - An ATAE blade server is connected to the public network through the base plane. For details about how to view the MAC address of the base plane of an ATAE blade server, see **G.5 How to View the MAC Address of the Base Plane of an ATAE Blade Server**.
  - An IBM blade server is connected to the public network through I/O module 1 and I/O module 2. The system IP address of the IBM blade server must be set on the external communication NIC. For details about how to view the MAC address of the external communication NIC of an IBM blade server, see **G.3 How to View the MAC Address of the External Communication NIC of an IBM Blade Server**.
- The installation CD-ROM must be available.
- For the ATAE server, if the USB drive is connected to the ATAE server card, the indicator of the USB drive is green and flashes.

## Context

During the installation, use the keyboard as follows:

- Press **Tab** to switch between buttons, option buttons, and check boxes.
- Press **Enter** to select a button.
- Press an arrow key to select a parameter.
- Press the spacebar to select an option or a button.

**NOTE**

The installation DVD-ROM of the OS is described in the following procedure.

## Procedure

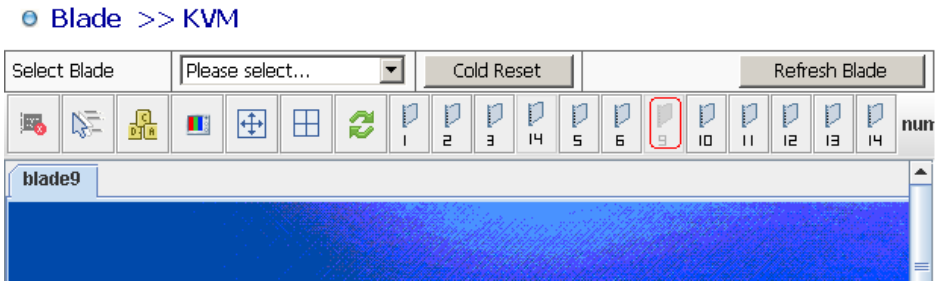
1 **Optional:** In the case of the ATAE blade server, in BIOS, set the order for starting the OS so that the OS boots from the CD-ROM.

**NOTE**

This step is applicable only to the ATAE blade server. In the case of other servers, skip this step.

1. Insert the installation disk to the USB drive.
2. **Logging In to the Management Console of an ATAE Blade Server**.
3. In the Blade >> KVM panel, select the required board from **Select Blade**, and click **Cold Reset** to restart the blade server.

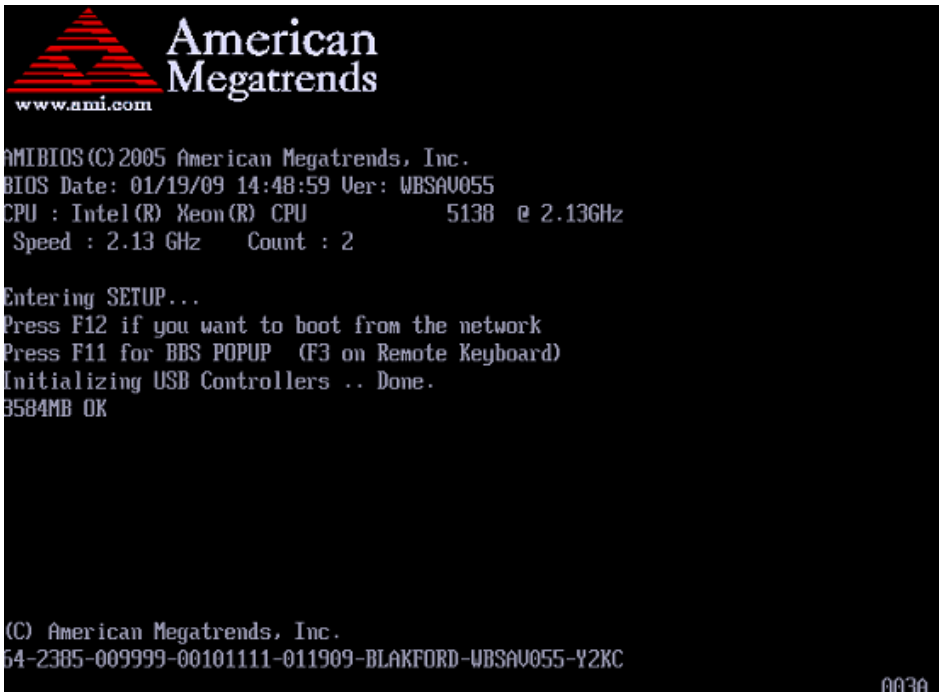
   On the toolbar of the Blade >> KVM panel, click the icon of the card to be operated to display the related tab page.




**TIP**

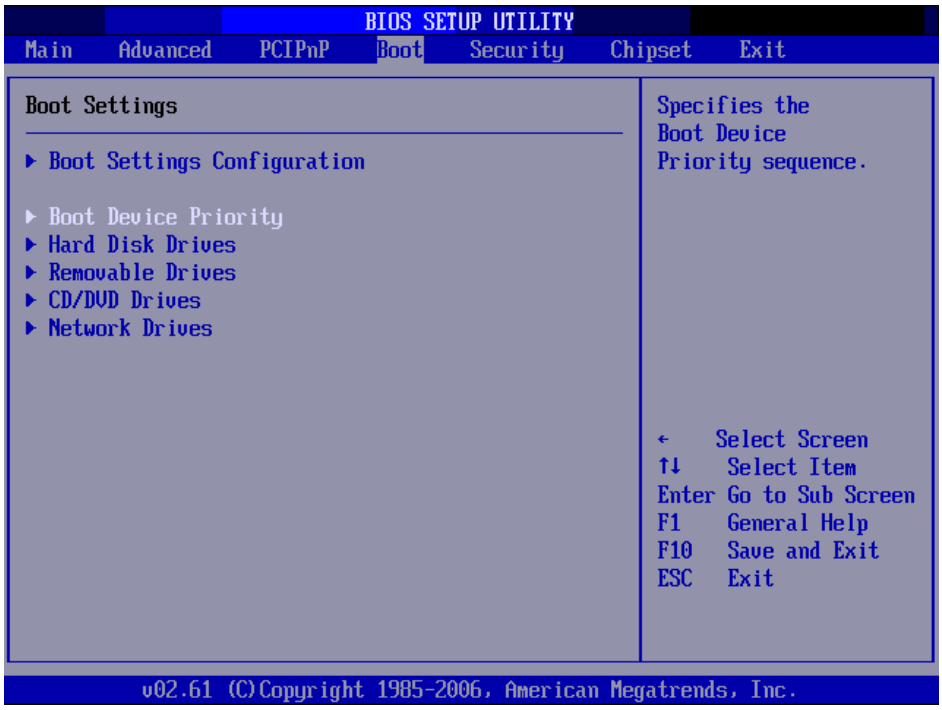
- To enter the full screen mode, click  on the toolbar.
- To restore from the full screen mode to window, move the mouse to upper middle of the screen, press **Ctrl+Shift+Alt** and click  in the upper portion of the screen.

4. In the process of restarting the blade server, when the **American Megatrends** window is displayed, press **Delete** to display the **BIOS SETUP UTILITY** window.

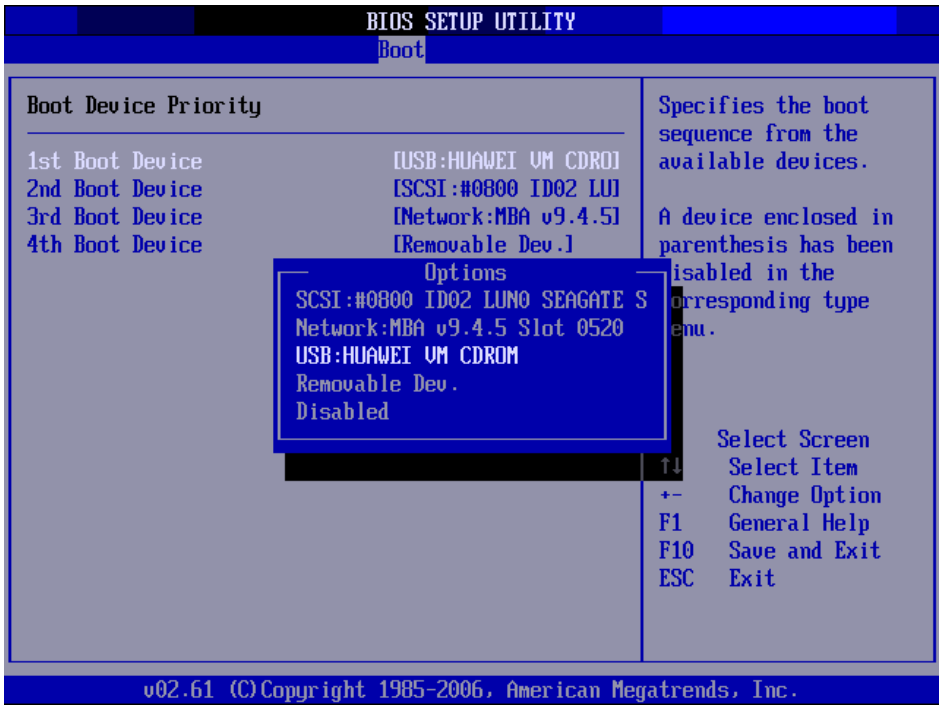



5. In the **BIOS SETUP UTILITY** window, use the left arrow and right arrow keys to choose **Boot** from the main menu.

   On the **Boot Settings** tab page, use the up arrow and down arrow keys to select **Boot Device Priority**. Then, press **Enter**.




6. In the **Boot Device Priority** pane, set the order for starting the OS of the blade server so that the OS boots from the USB disk drive.
   a. Select **1st Boot Device**, and then press **Enter**. The **Options** dialog box is displayed.
   b. Use the up arrow and down arrow keys to select **USB:HUAWEI VM CDROM**. Then, press **Enter**.




7. Press **F10** after the previous settings, the confirm dialog box is displayed.
8. Click **OK**, and then press **Enter** to save the settings and exit.

**2 Optional:** In the case of the IBM HS22 blade server, in BIOS, set the order for starting the OS so that the OS boots from the CD-ROM.

**NOTE**

This step is applicable only to the IBM HS22 blade server. In the case of other servers, skip this step.

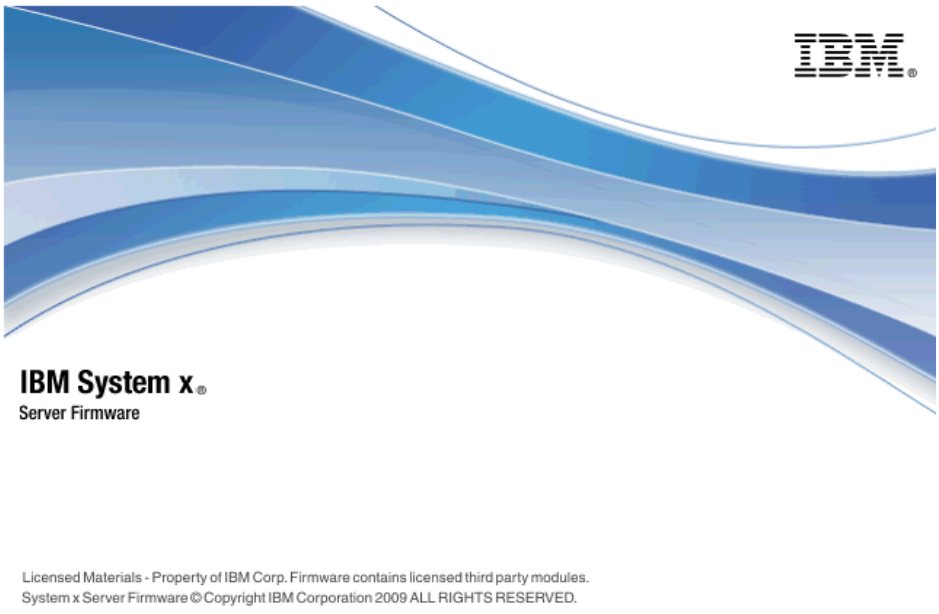
1. **Mount the virtual media of the IBM blade server**.

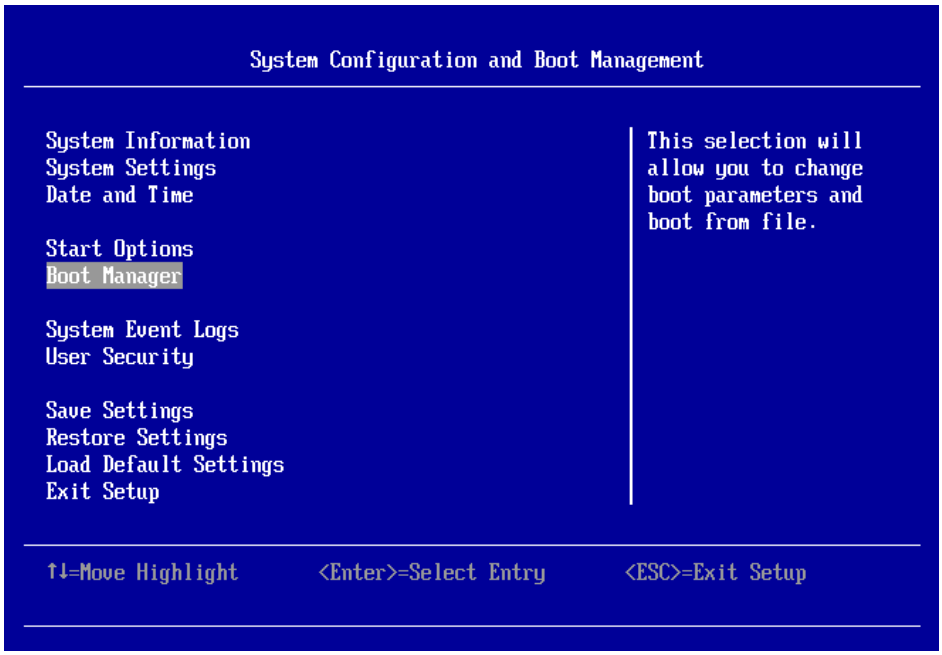
   **NOTE**

   - The purpose of mounting the virtual media of the IBM blade server is to mount the CD/DVD drive or ISO file of the PC where the Web console is installed to a blade server, thus implementing remote installation of the OS of the blade server. Alternatively, the default CD/DVD drive of the IBM BladeCenter E can be used to install the OS of the blade server.
   - To use the default CD/DVD drive of the IBM BladeCenter E to install an OS on a blade server, you need to insert the OS installation DVD into the default CD/DVD drive of the IBM BladeCenter E and then press **MT** at the middle of the blade server, If the **MT** indicator is on, it indicates that the blade server is connected to the default CD/DVD drive.

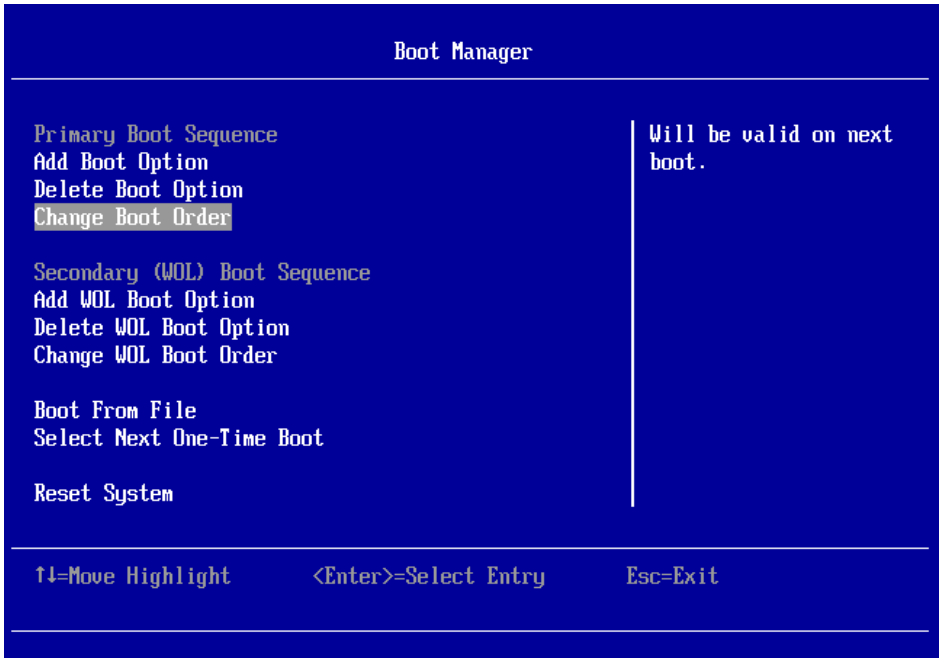
2. In the remote console window, click 

. Then, select the required card.
3. In the **Power Control** area, select **Restart** to restart the blade server.
4. In the process of restarting the blade server, when the **System x** window is displayed, press **F1** and the **System Configuration and Boot Management** window is displayed.

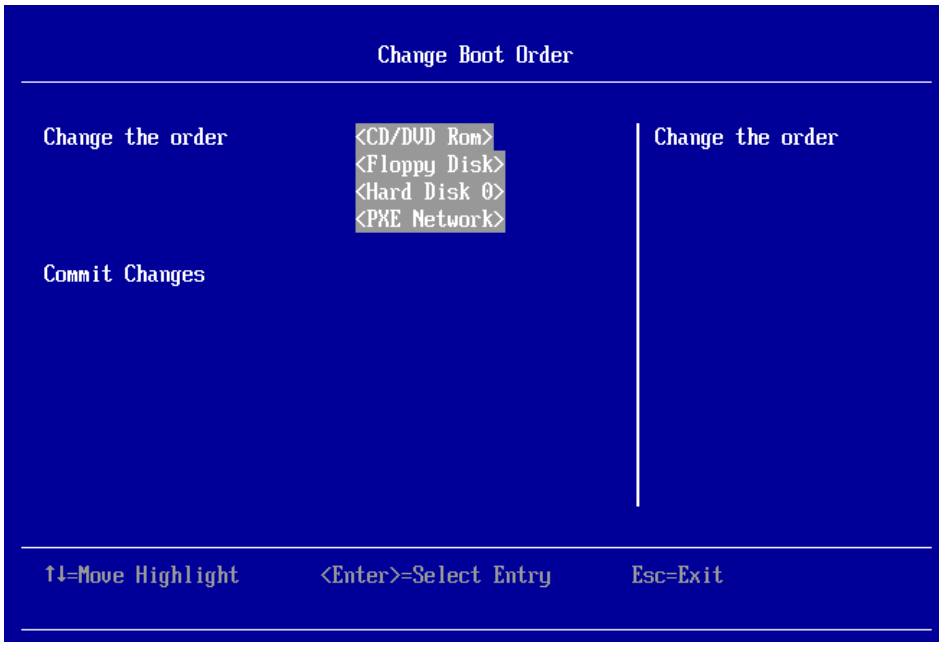





5. Press an arrow key to choose **Boot Manager** from the main menu. Press **Enter**.




6. Press an arrow key to choose **Change Boot Order** from the **Boot Manager**. Press **Enter**.




7. Press an arrow key to choose **CD/DVD Rom** from the **Change Boot Order**. Press **Enter**.
8. Choose **Save Settings** from the main menu. Press **Enter** twice to save the settings.
9. Choose **Exit Setup** and press **Enter** twice to exit BIOS setting.

**3 Optional:** In the case of the IBM HS21 blade server, in BIOS, set the order for starting the OS so that the OS boots from the CD-ROM.

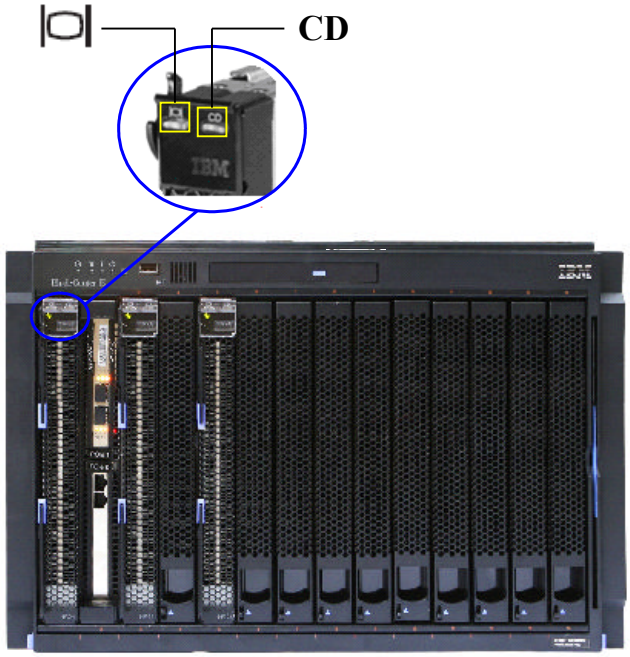
**NOTE**

This step is applicable only to the IBM HS21 blade server. In the case of other servers, skip this step.

1. **Mount the virtual media of the IBM blade server**.

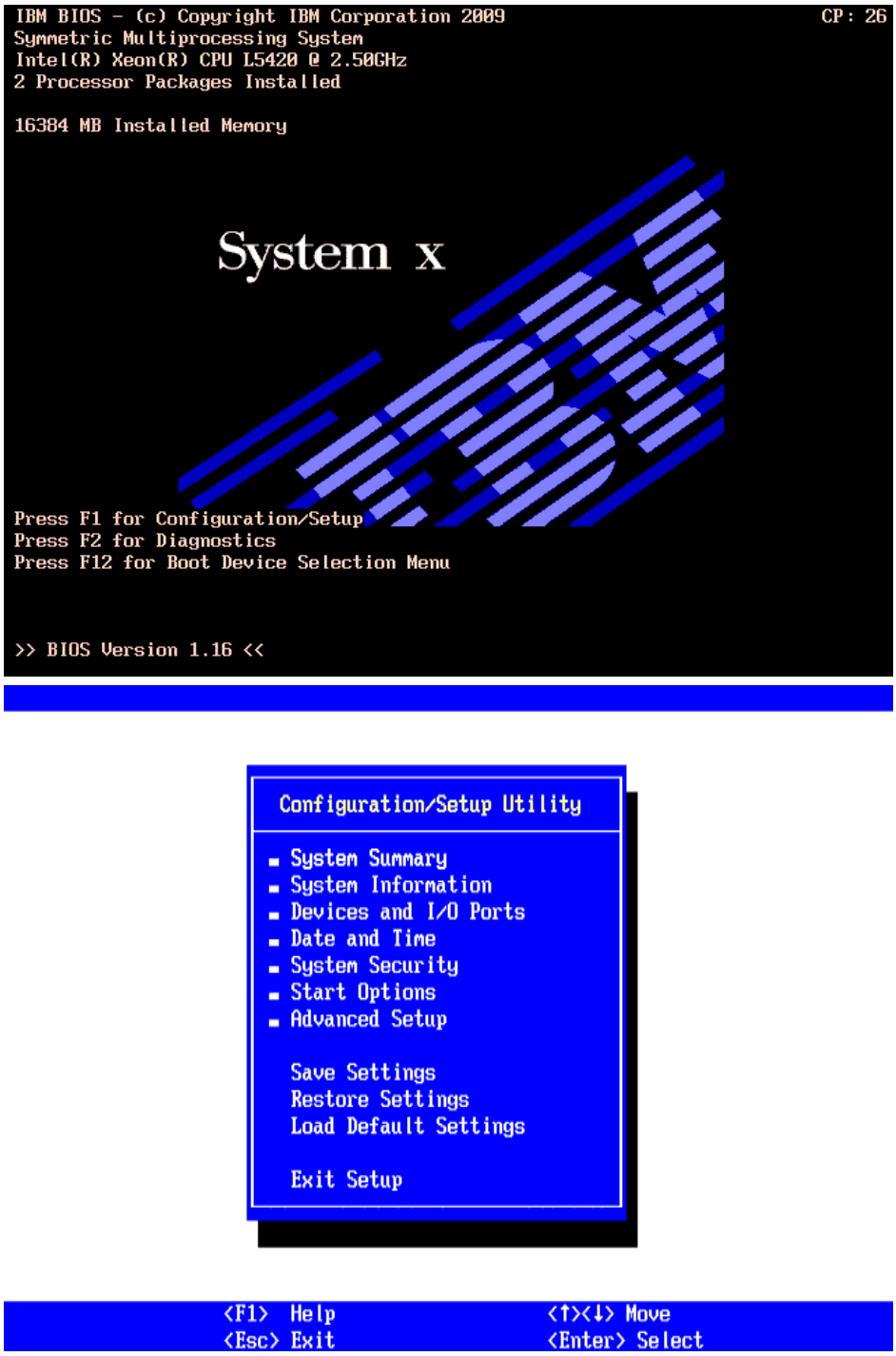
**NOTE**

- The purpose of mounting the virtual media of the IBM blade server is to mount the CD/DVD drive or ISO file of the PC where the Web console is installed to a blade server, thus implementing remote installation of the OS of the blade server. Alternatively, the default CD/DVD drive of the IBM BladeCenter E can be used to install the OS of the blade server.
- To use the default CD/DVD drive of the IBM BladeCenter E to install an OS on a blade server, you need to insert the OS installation DVD into the default CD/DVD drive of the IBM BladeCenter E and then press **CD** at the top of the blade server, as shown in the following figure. If the **CD** indicator is on, it indicates that the blade server is connected to the default CD/DVD drive.




2. In the remote console window, click 

. Then, select the required card.
3. In the **Power Control** area, select **Restart** to restart the blade server.
4. In the process of restarting the blade server, when the **System x** window is displayed, press **F1** and the **Configuration/Setup Utility** window is displayed.




5. Press an arrow key to choose **Start Options** > **Startup Sequence Options** from the main menu. Press **Enter**.
6. In the **Startup Sequence Options** window, do as follows:
   - Set **First Startup Device** to **CD ROM**.
   - Set **Second Startup Device** to **Diskette Drive 0**.
   - Set **Third Startup Device** to **Hard Disk 0**.


After you complete the settings, press **Esc** twice to return to the main menu.

7. Choose **Save Settings** from the main menu. Press **Enter** twice to save the settings.
8. Choose **Exit Setup** and press **Enter** twice to exit BIOS setting.

**4** The system restarts automatically.

**5** Select an installation mode.

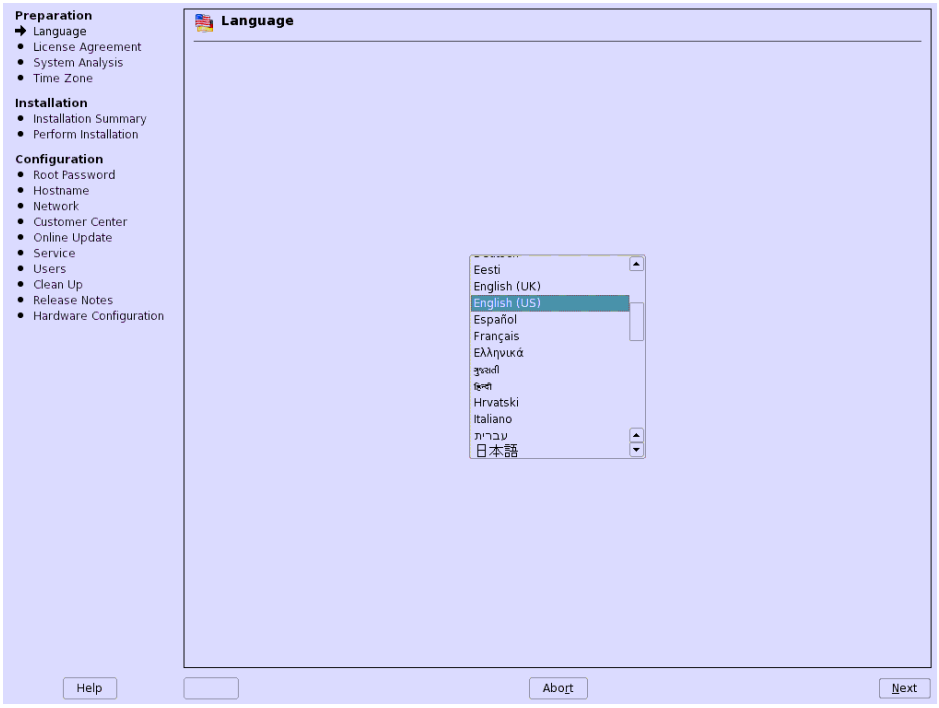
In the **SUSE Linux Enterprise Server** window, press the arrow key to select **Installation**. Then, press **Enter** to load the SUSE Linux kernel.

**NOTE**

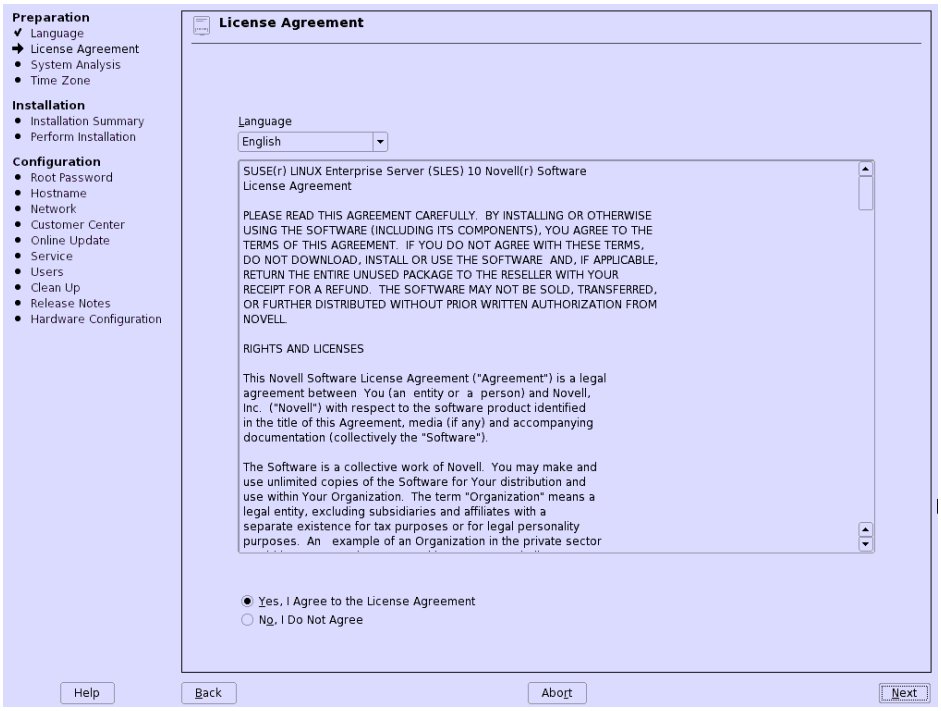
It takes approximately five minutes to complete the loading of the SUSE Linux kernel.

**6** Select the setup language, time zone, and installation mode.

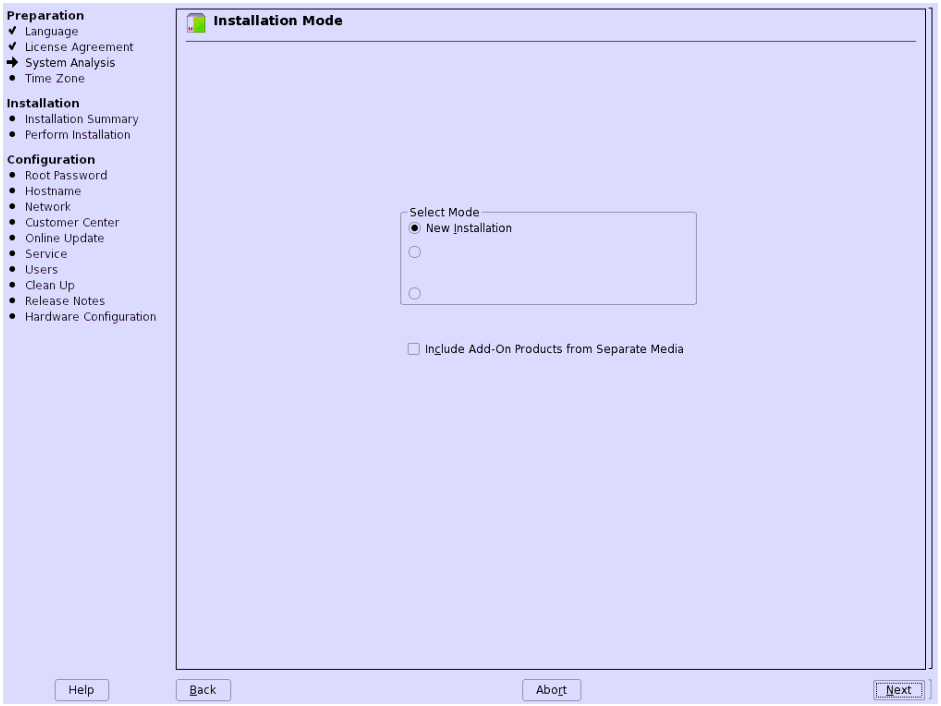
1. In the **Language** dialog box, select **English (US)** and click **Next**.




2. In the **License Agreement** dialog box, select **Yes, I Agree to the License Agreement** and click **Next**.




3. In the **Installation Mode** dialog box, select **New Installation** and click **Next**.

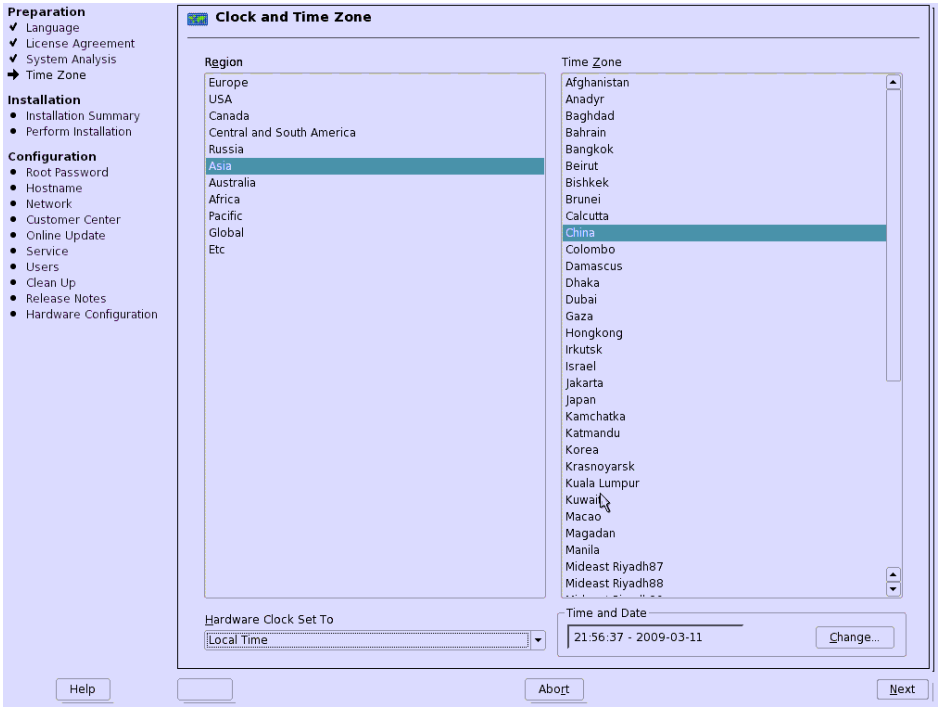



4. In the **Clock and Time Zone** dialog box, set parameters by referring to the following table and click **Next**.

   **NOTE**

   The proceeding settings are provided for reference only. During the on-site installation process, set the parameters based on the actual situation.

| Parameter | Setting |
|---|---|
| Region | **Asia** |
| Time Zone | **China** |
| Hardware Clock Set to | **Local Time** |
| Time and Date | Set this parameter to the correct current time. |




**7** Perform the installation settings.

1. Set the type of keyboard layout.

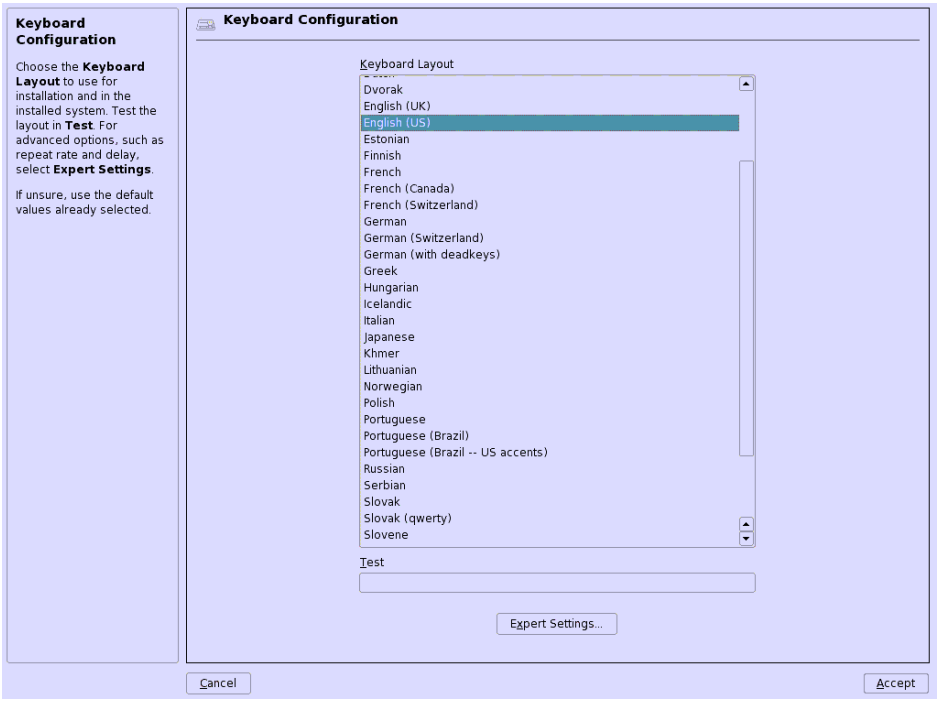
   a. In the **Installation Settings** dialog box, select **Keyboard Configuration**, and press **Enter**.

   **NOTE**

   If the installed server is not configured with a mouse, you can use the keyboard to perform the installation as follows:

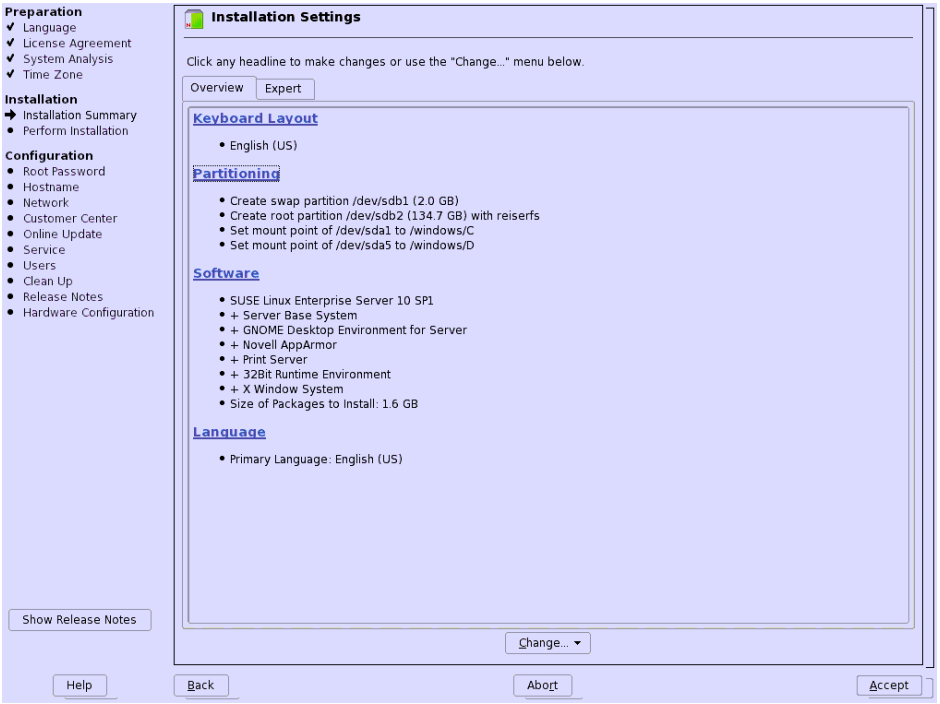
   - Press **Tab** to switch between buttons, option buttons, and check boxes.
   - Press **Enter** to select a button.
   - Press an arrow key to select a parameter.
   - Press the spacebar to select an option or a button.

   b. Select **English (US)** and press **Enter**.

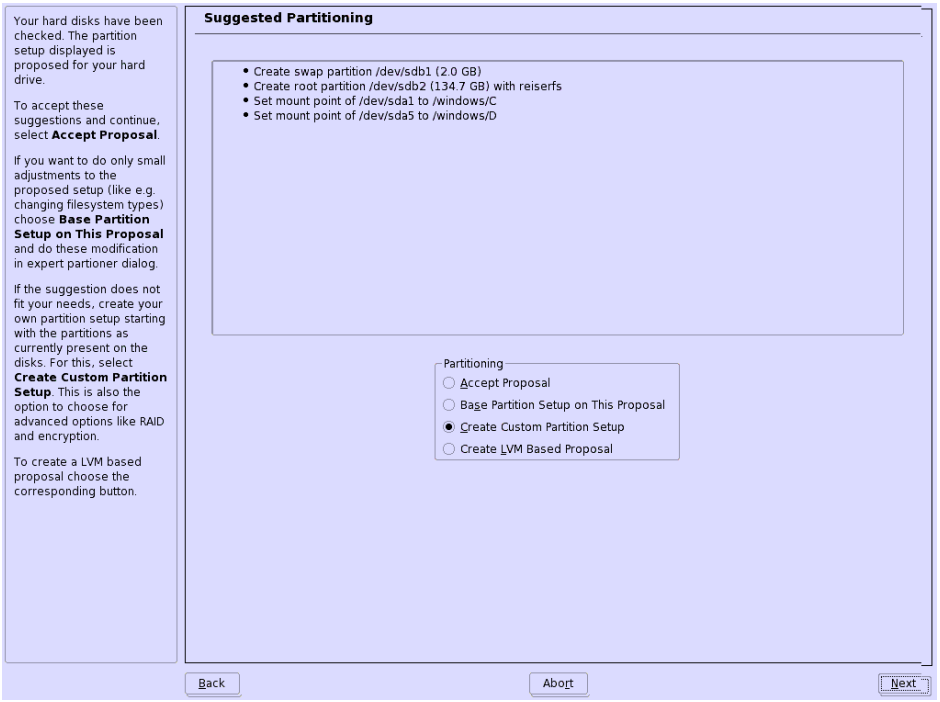



2. Set the size of a partition.

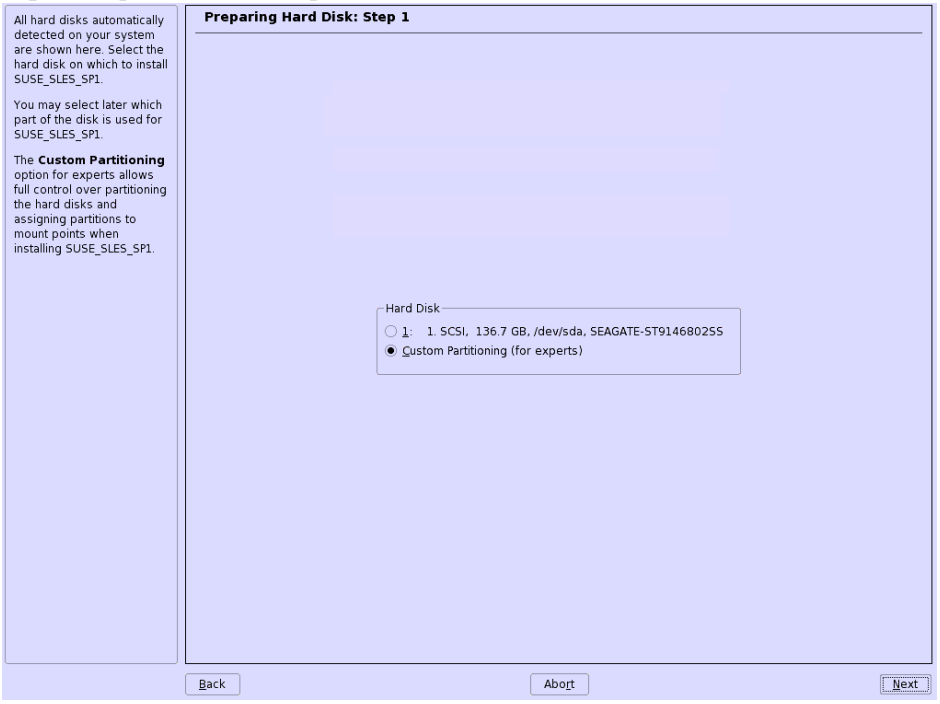
   a. In the **Installation Settings** dialog box, select **Partitioning** and press **Enter**. The **Suggested Partitioning** dialog box is displayed.



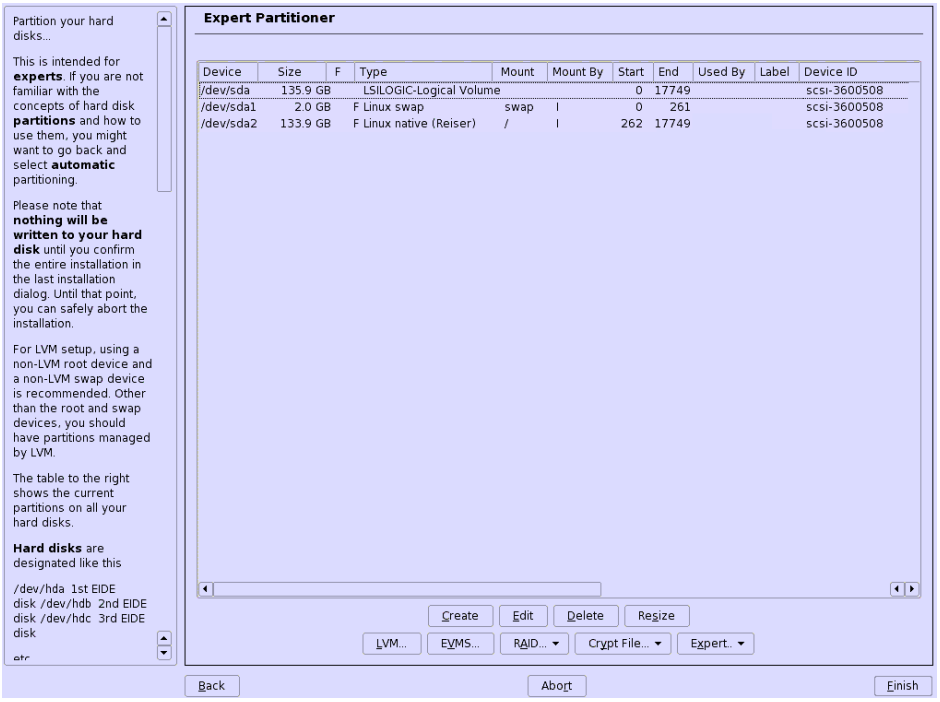

   b. In the **Suggested Partitioning** dialog box , select the **Create Custom Partition Setup** option button and press **Enter**.



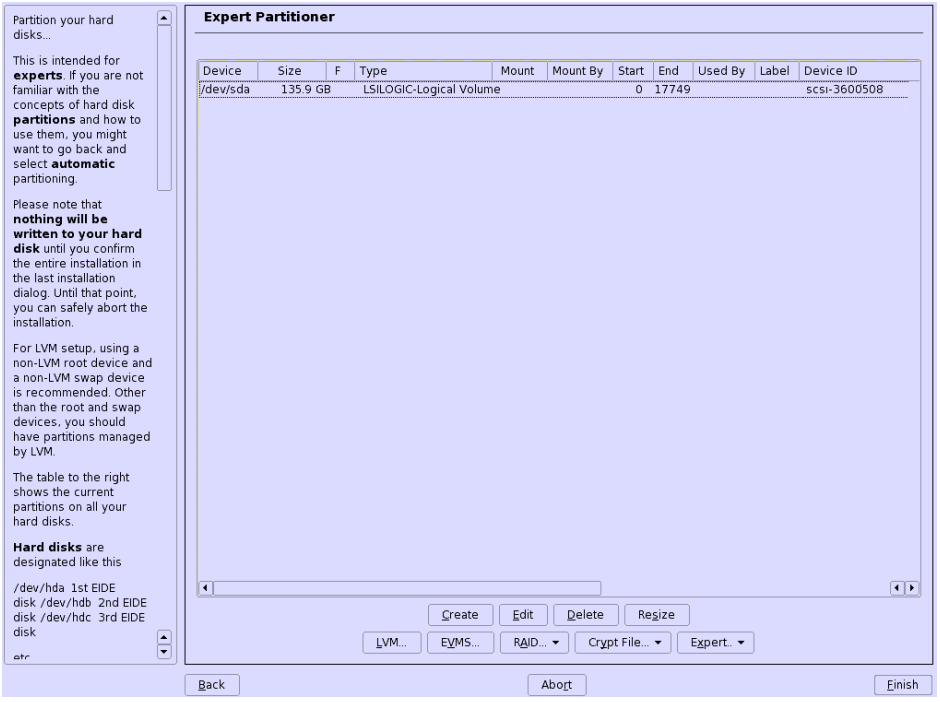

c. In the **Preparing Hard Disk: Step1** dialog box , select the **Custom Partitioning (for experts)** option button and press **Enter**.



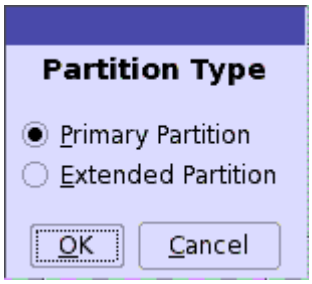

d. In the **Expert Partitioner** dialog box, select the /dev/sda1 equipment and click **Delete**. Then, delete the /dev/sda2 equipment in the same manner.




e. In the **Expert Partitioner** dialog box, click **Create**.



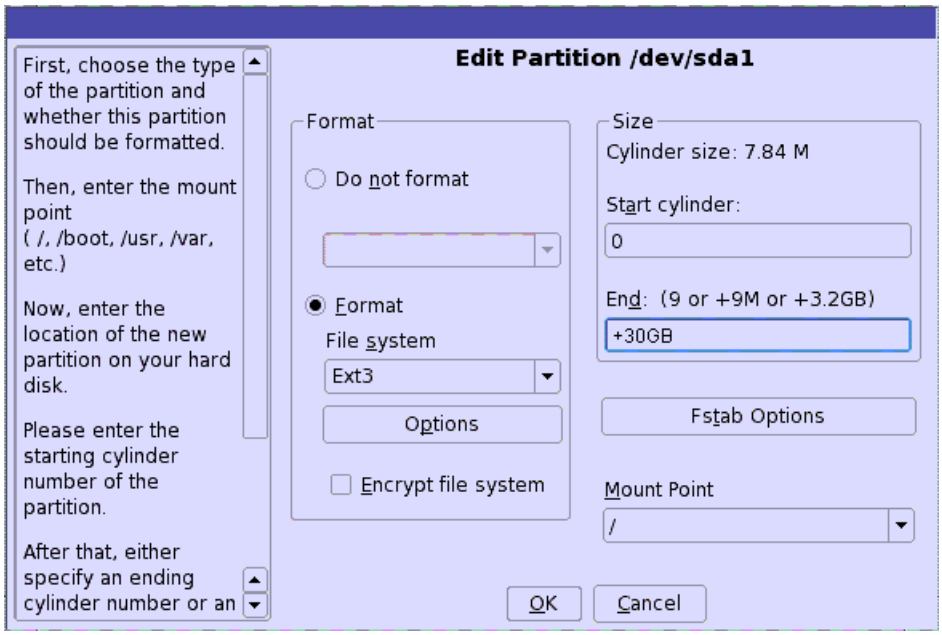

f. In the **Partition Type** dialog box, select the **Primary Partition** option button and click **OK**.




g. In the **Create a Primary Partition on /dev/sda** dialog box, set the following parameters. The parameters are described as follows:

1) Select the **Format** option button.
2) Set **File system** to *Ext3*.
3) In the text box below **End:(9 or +9M or +3.2GB)**, enter **30 GB** or **+30 GB** to set the size of a partition.
4) Set **Mount Point** to /.
5) Press **Enter** or click **OK**.

| Parameter | Description |
|---|---|
| **Do not format** | This parameter indicates that the hard disk is not to be formatted. Do not select this value at the first installation. |
| **Format** | This parameter indicates that the hard disk is to be formatted. Select this value at the first installation. |
| **File system** | This parameter indicates the format of the file system. For details of settings, refer to the "Partition Type" column in **I Planning Disk Partitions**. |
| **start cylinder** | This parameter indicates the start volume address of the current partition. When this parameter is created, it automatically uses the end volume address of the last partition. In this case, you need not set this parameter. |
| **End:(9 or +9M or +3.2GB)** | This parameter indicates the end volume address of the current partition. Set this parameter according to the partition size in **I Planning Disk Partitions**. |

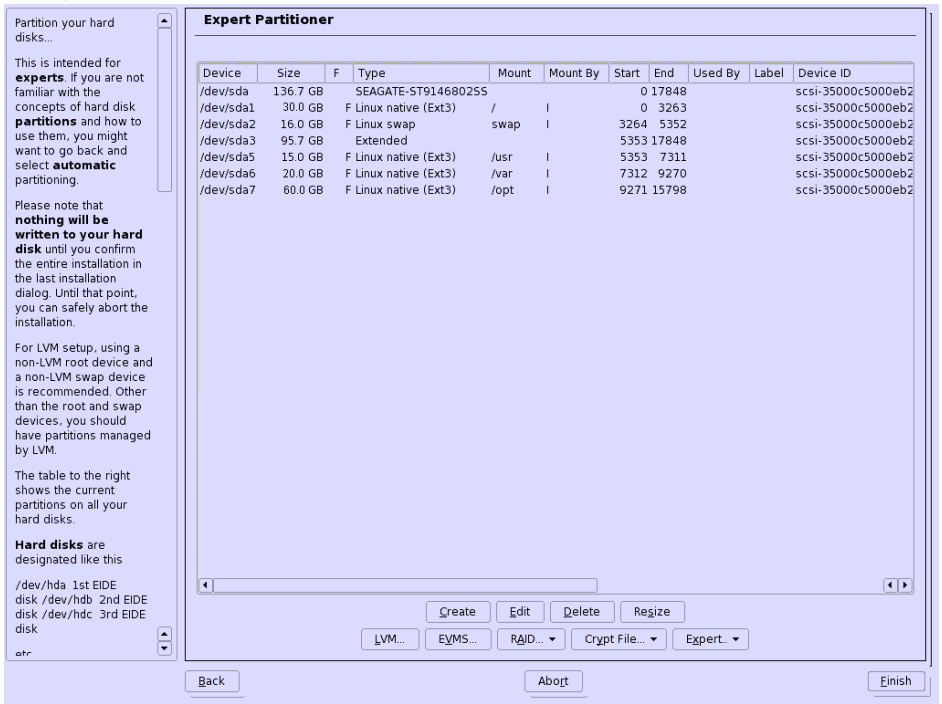



**NOTE**

If the information about the partitions exception the /dev/sda partition is not required, select **Delete** to delete the information, or press **Alt+D** to delete the old partition information.

h. Refer to 7.2.e to 7.2.g to create the **swap**, **/usr**, **/var**, and **/opt** partitions.

i. The follow dialog box shows after the previous settings. In the **Expert Partitioner** dialog box, click **Finish** to continue.

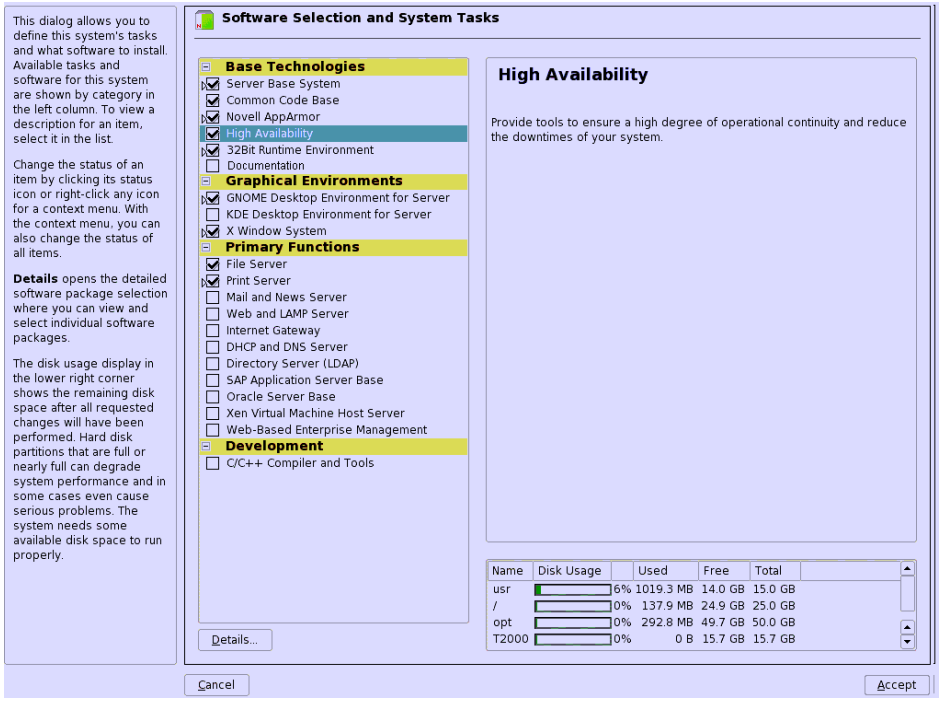



3. Set the software to be installed.

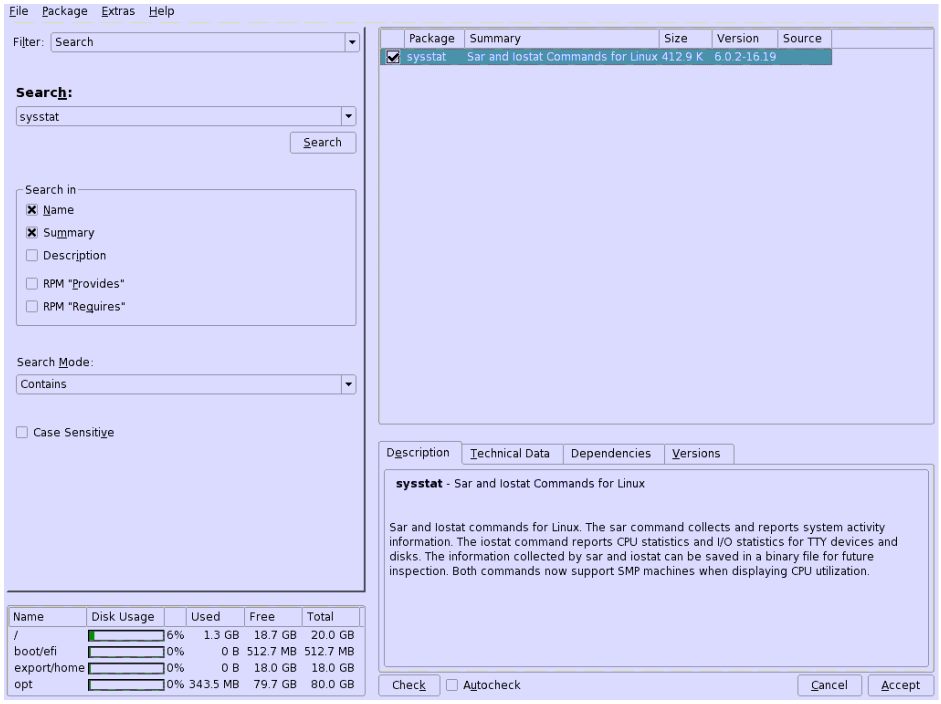
a. In the **Installation Settings** dialog box, select **Software** and the **Software Selection and System Tasks** dialog box is displayed.

b. As shown in the following figure, select the **Server Base System**, **Common Code Base**, **Novell AppArmor**, **High Availability**, **32 Bit Runtime Environment**,

**GNOME Desktop Environment for Server**, **X Window System**, **File Server**, and **Print Server** parameters, and then click **Details**.




c. Select *Search* from the **Filter** drop-down list, enter **sysstat** in the *Search* text box, and then click **Search**.



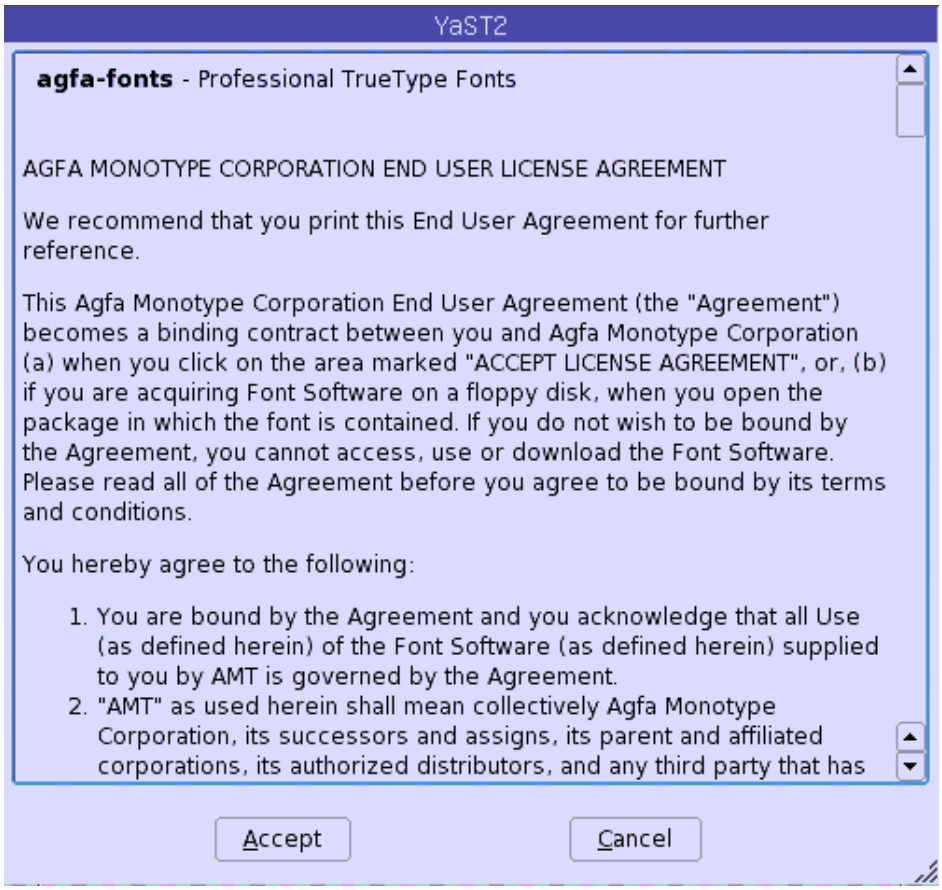

d. The names of required software packages are displayed in the right-hand pane of the dialog box. Press **Tab** and spacebar or use the mouse to select *sysstat*.

e. Refer to **7.3.c** to **7.3.d** to install other software. The following lists the software that needs to be installed.

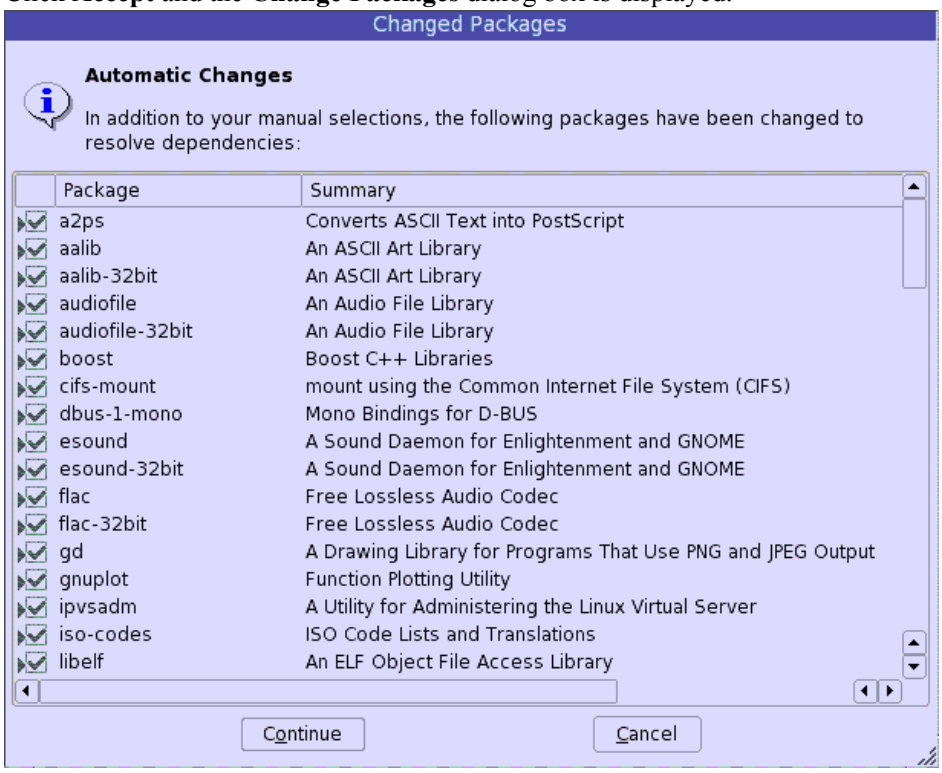
1) binutils

2) compat
3) compat-libstdc++
4) compat-32bit
5) compat-curl2
6) compat-curl2-32bit
7) expect
8) gcc
9) glibc-devel
10) glibc-devel-32bit
11) glibc
12) glibc-32bit
13) gcc-c++
14) glib2
15) glib2-32bit
16) glib2-devel
17) glib2-doc
18) libmudflap
19) libstroke
20) libstroke-devel
21) libsvg
22) libsvg-cairo
23) libaio
24) libaio-32bit
25) libaio-devel
26) libelf
27) libgcc
28) libstdc++
29) libstdc++-devel
30) make
31) pam
32) pam-32bit
33) pam-devel
34) pam_krb5
35) sysstat
36) unixODBC-devel-32bit
37) unixODBC-gui-qt
38) unixODBC
39) unixODBC-devel

f. Click **Accept** and the **YaST2** dialog box is displayed.




g. Click **Accept** and the **Change Packages** dialog box is displayed.



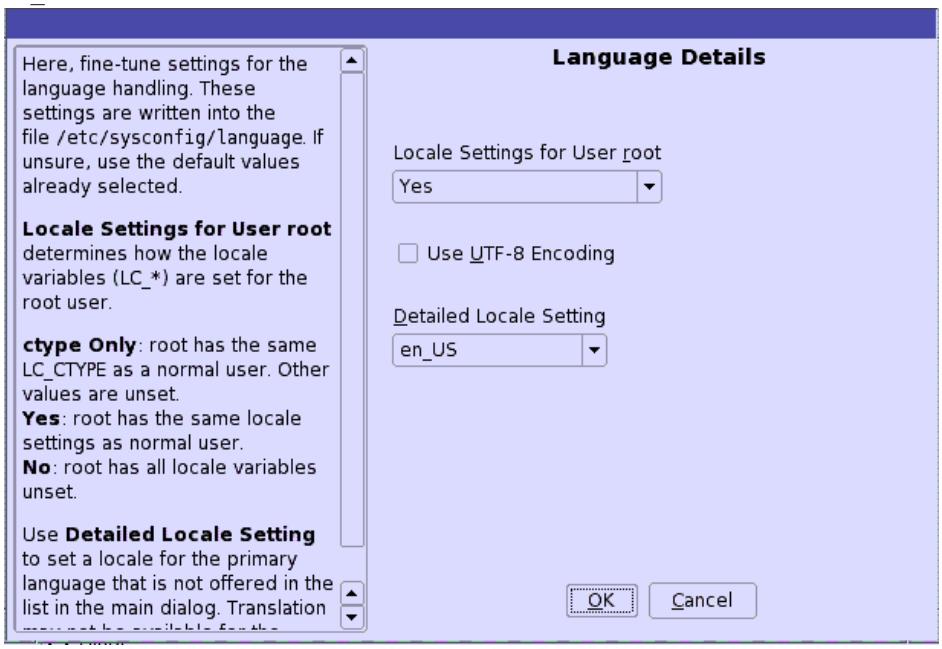

h. Click **Continue**.

4. Set the setup language of the OS.

a. In the **Installation Settings** dialog box, click **Language**.

b. In the **Language** dialog box, set **Primary Language** to *English (US)* and click **Details**.

c. In the **Language Details** dialog box, set **Local Settings for User root** to *Yes*, clear the **Use UTF-8 Encoding** check box, and then set **Detailed Locale Setting** to *en_US*.



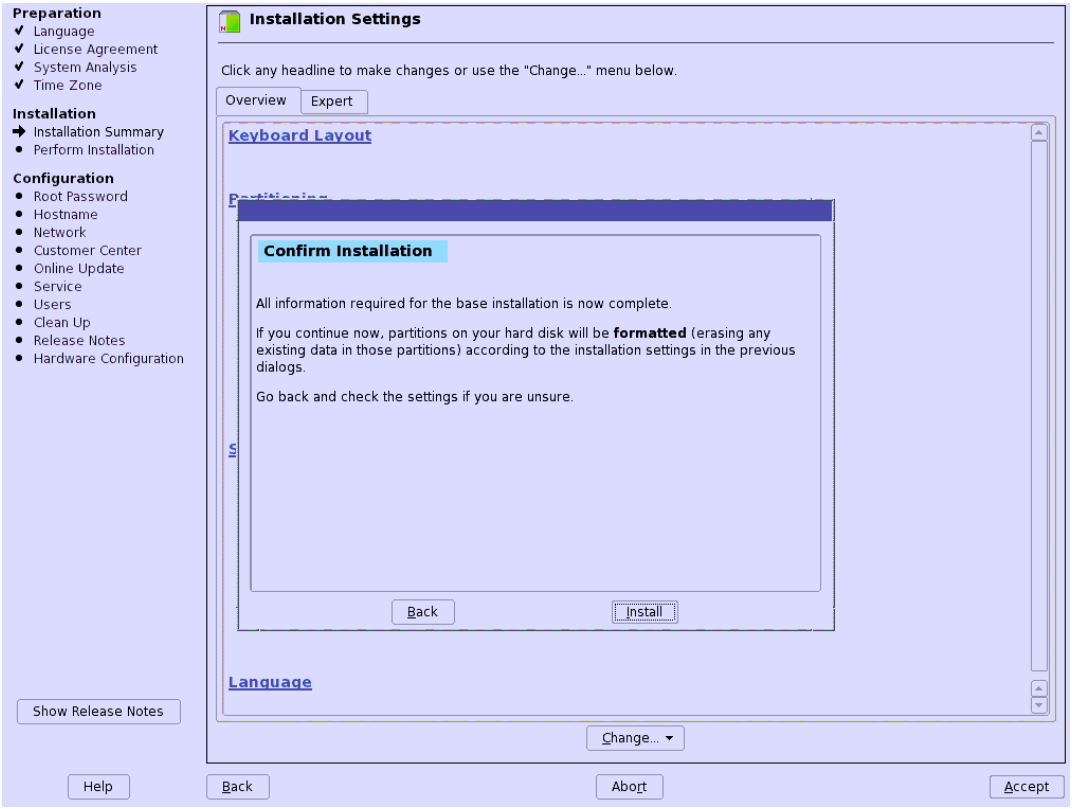

d. Click **OK** to return to the **Languages** window.

e. Click **OK** .

5. In the **Installation Settings** dialog box, click **Accept**.

**8** Confirm the installation.

In the **Confirm Installation** dialog box, click **Install**.



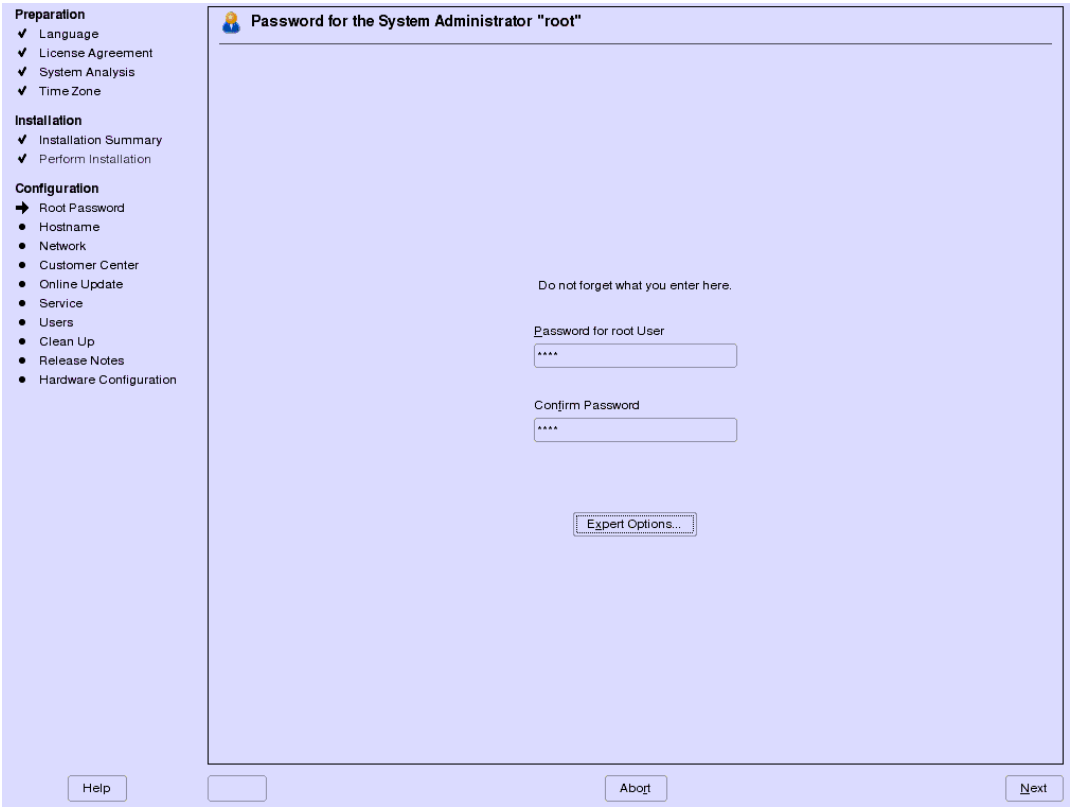

The OS is being installed formally. The installation progress is displayed on the setup program window. It takes approximately 50 minutes to complete the installation.

9 Set the password of user **root**.

In the **Password for the System Administrator "root"** window, enter and confirm the password of user **root**, and click **Next**.

**NOTE**

- The default password of the super user **root** of the SUSE Linux OS is **root**. You can change the password. The password is often required in the subsequent installation procedure.
- If a message is displayed indicating that the password is too simple, click **Yes** to continue as prompted.




**10** Set the host name and domain name.

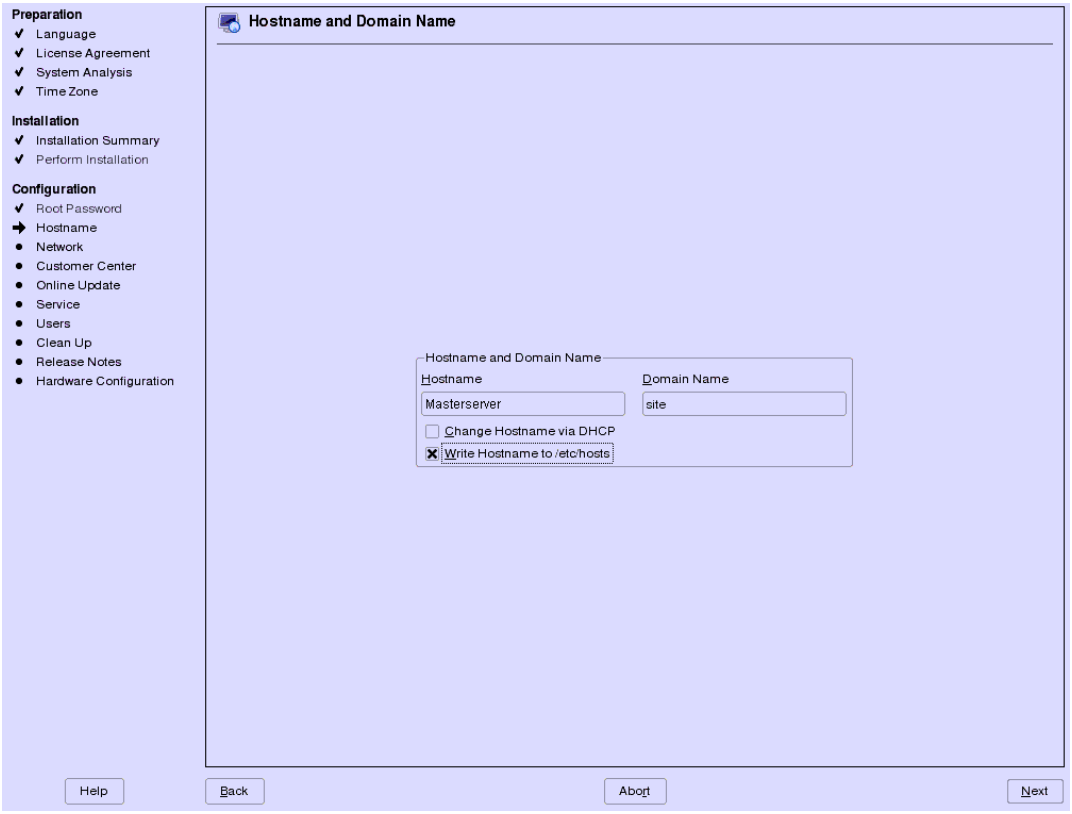
In the **Hostname and Domain Name** dialog box, do as follows:

- Set the host name to Masterserver.
- Clear the **Change Hostname via DHCP** check box.
- Select the **Write Hostname to /etc/hosts** check box.

Click **Next**.

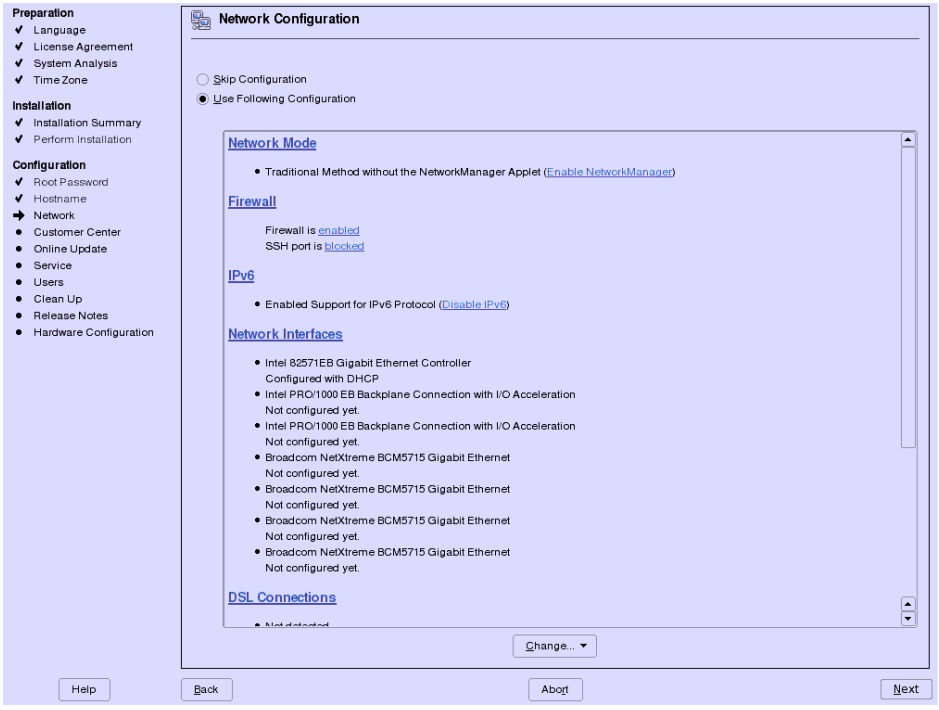
**NOTE**

Use the default value in the **Domain Name** field.




**11** Configure the network.

1. In the **Network Configuration** dialog box, select the **Use Following Configuration** option button.
2. Click **enabled** next to **Firewall**, and change **enabled** to **disabled**.

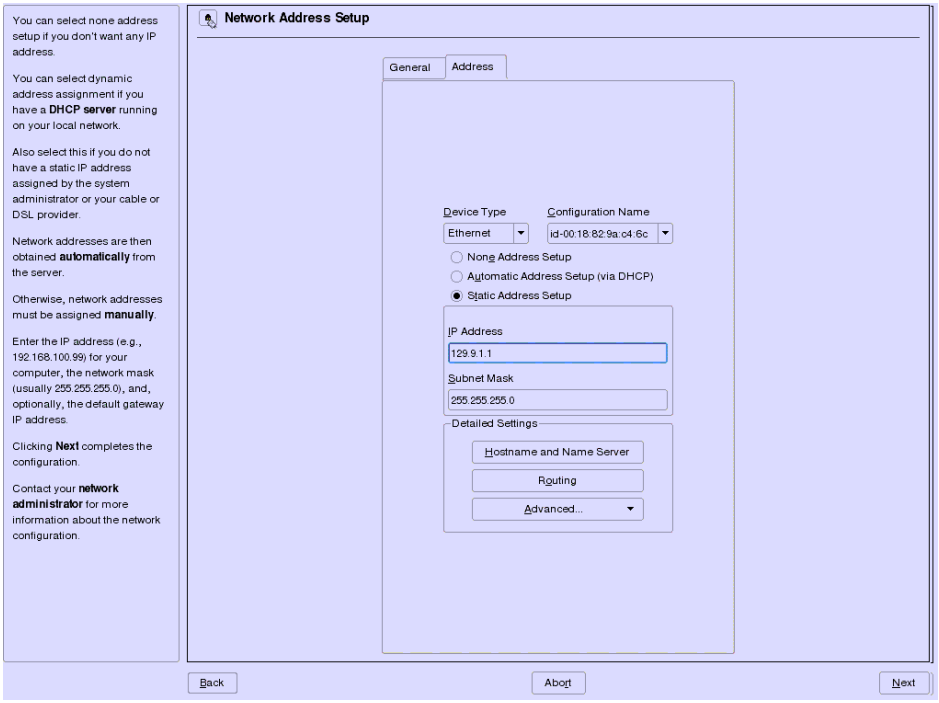


3. In the **Network Configuration** dialog box, select **Network Interface**. In the **Network Card Configuration Overview** dialog box that is displayed, select the network adapter that provides the external communication function and click **Edit**.

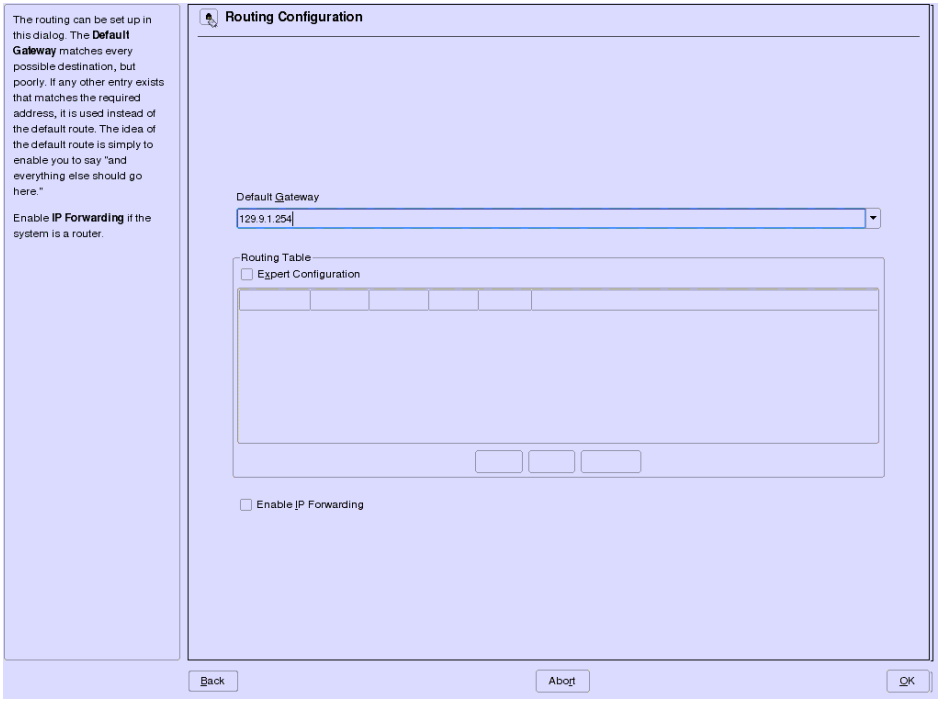
   **NOTE**

   - The NIC corresponding to the system IP address must be the NIC through which the blade server is connected to the public network.
     - An ATAE blade server is connected to the public network through the base plane. For details about how to view the MAC address of the base plane of an ATAE blade server, see **G.5 How to View the MAC Address of the Base Plane of an ATAE Blade Server**.
     - An IBM blade server is connected to the public network through I/O module 1 and I/O module 2. The system IP address of the IBM blade server must be set on the external communication NIC. For details about how to view the MAC address of the external communication NIC of an IBM blade server, see **G.3 How to View the MAC Address of the External Communication NIC of an IBM Blade Server**.
   - You can view the MAC address of an NIC on the **Address** tab page of the **Network Address Setup** dialog box.

4. In the **Network Address Setup** dialog box, select the **Static Address Setup** option button. Enter **129.9.1.1** in the **IP Address** field, and enter **255.255.255.0** in the **Subnet Mask** field. Click **Routing**.



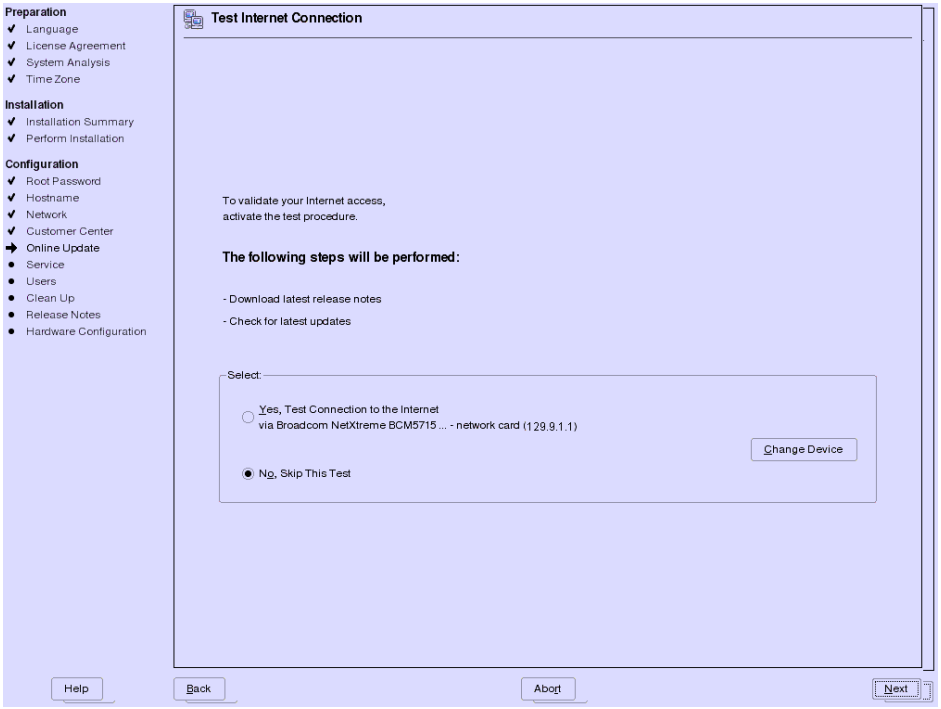

5. In the **Routing Configuration** dialog box, enter **129.9.1.254** in the **Default Gateway** field and click **OK**.




6. In the **Network Address Setup** dialog box, click **Next**.
7. In the **Network Card Configuration Overview** dialog box, click **Next**.

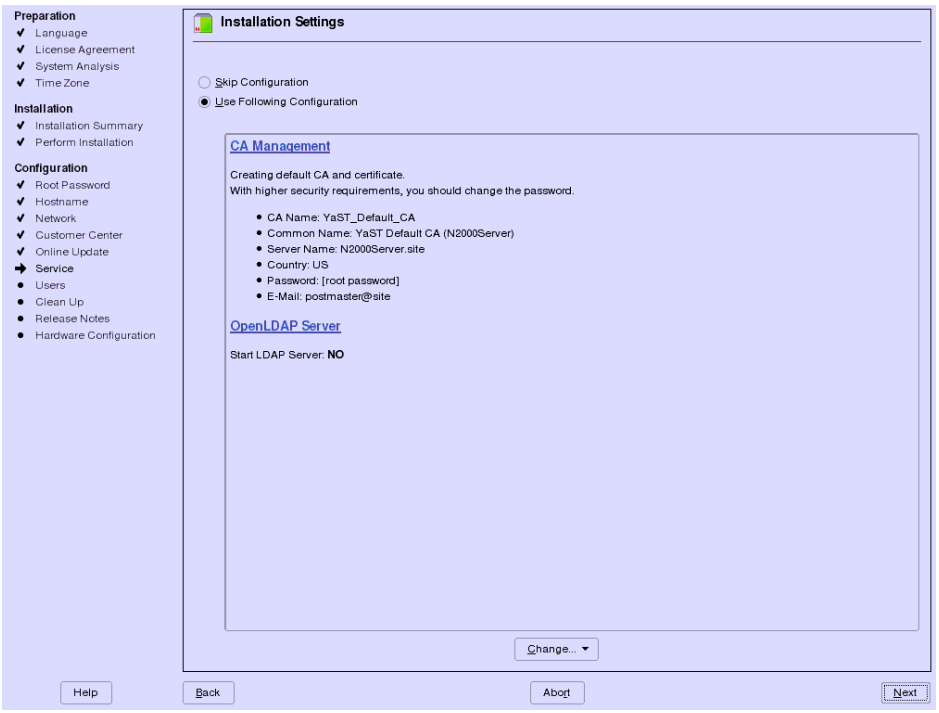
   **NOTE**

   If you want to configure multiple network adapters, follow Steps **3** to **6** to configure other network adapters.
8. In the **Network Configuration** dialog box, click **Next**.
9. In the **Test Internet Connection** dialog box, select the **No, Skip This Test** option button and click **Next**.



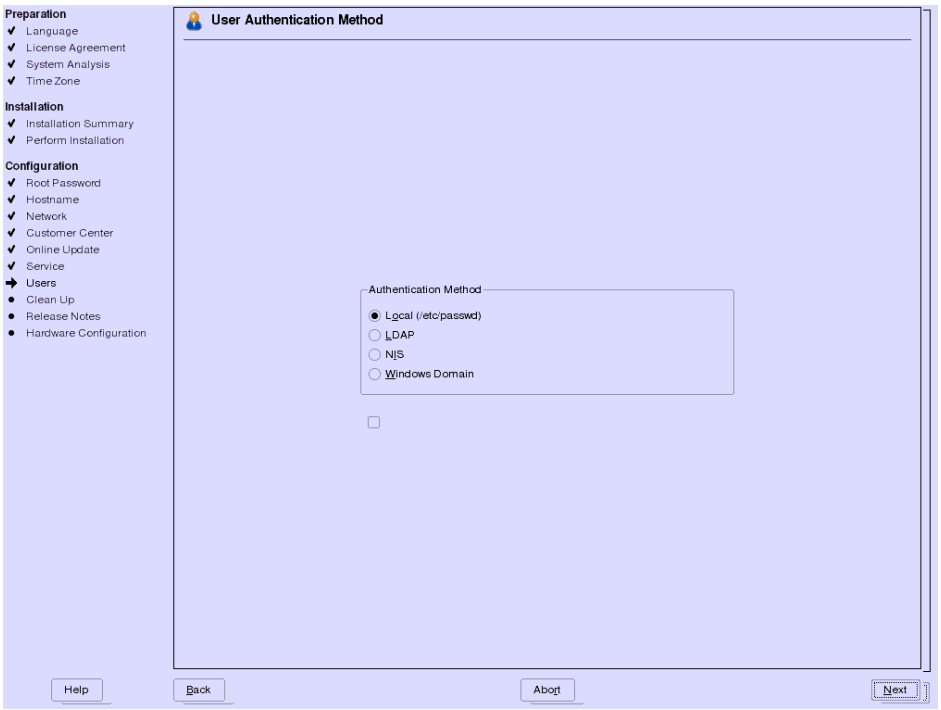
**12** Configure a service.

In the **Installation Settings** dialog box, use all the default values, and click **Next**.

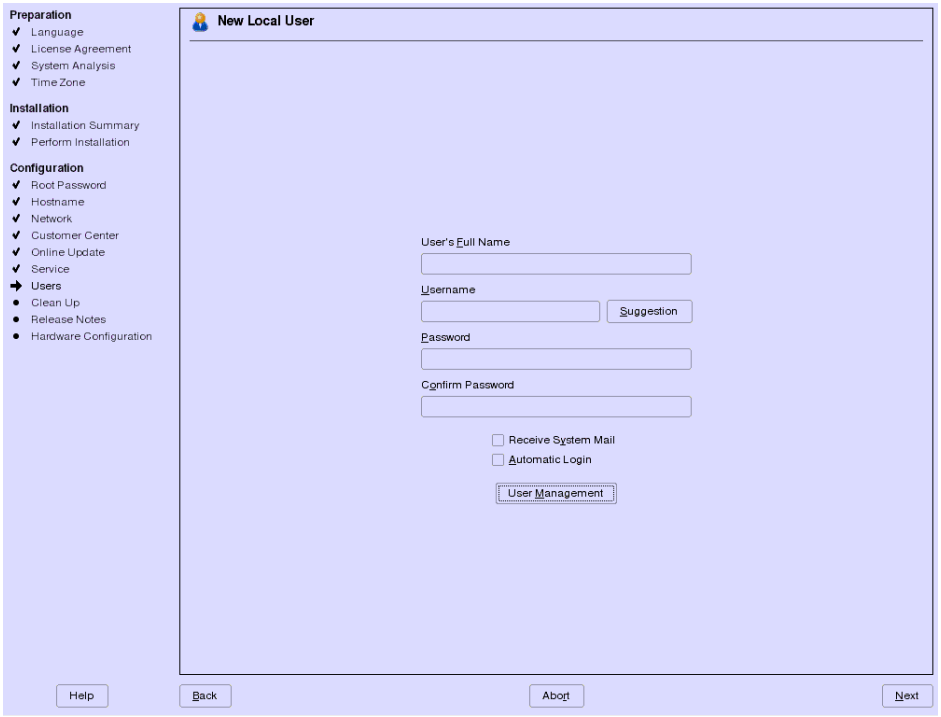



**13** Configure a user.

1. In the **User Authentication Method** dialog box, select the **Local** option button and click **Next**.

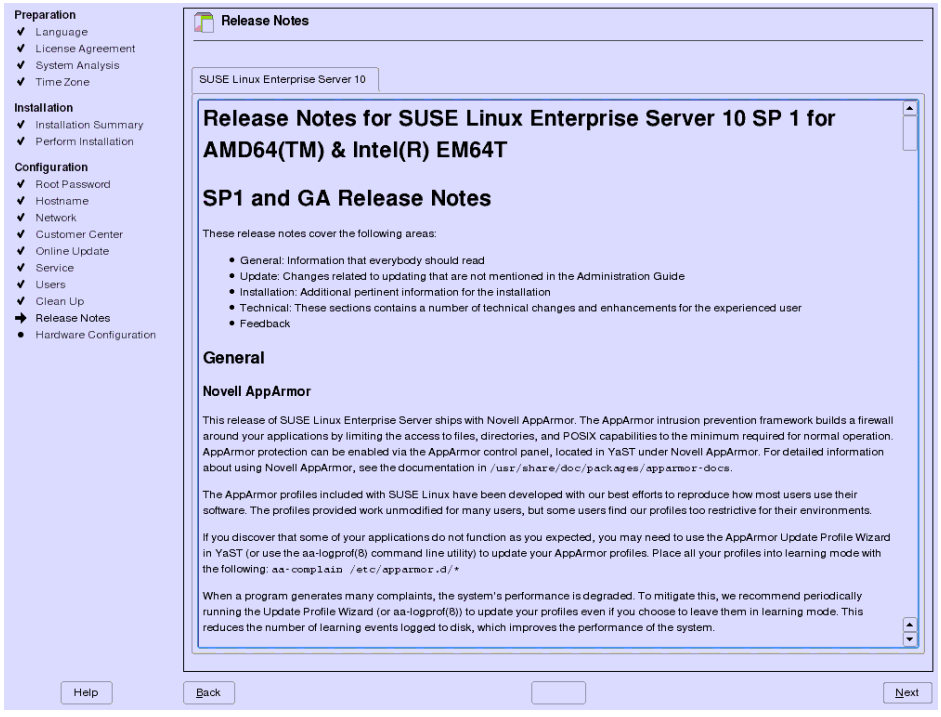



2. In the **New Local User** dialog box, leave all fields blank and click **Next**. A message is displayed indicating that no user is logged in. Click **Yes**.




**14** Confirm the release notes.

In the **Release Notes** dialog box, click **Next**.



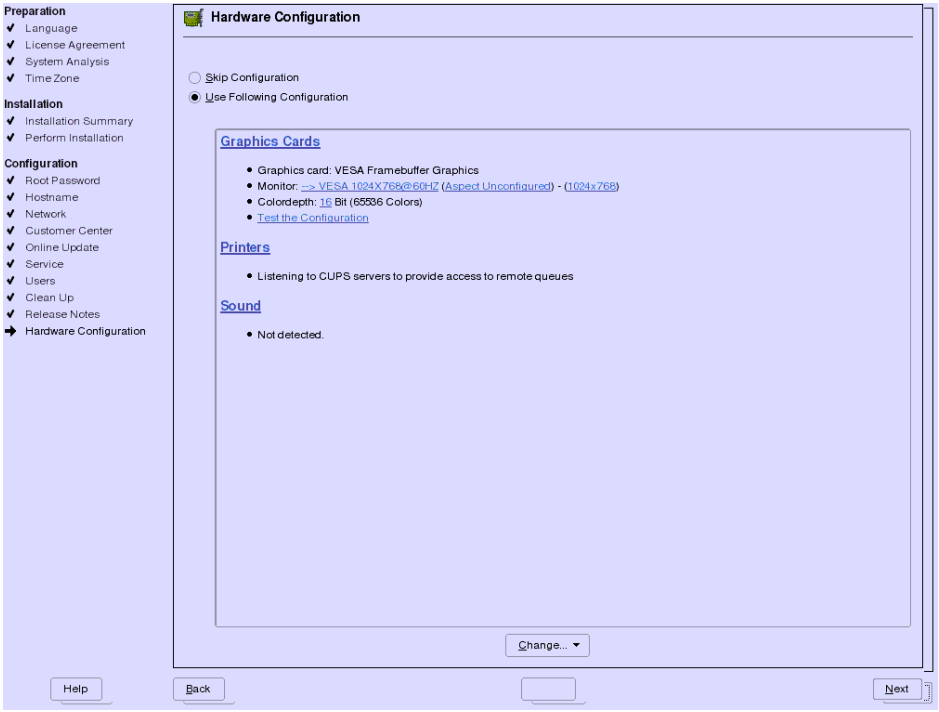

**15** Configure the equipment.

1. In the **Hardware Configuration** dialog box, keep the default value of the **Monitor** and **Colordepth**.
2. Click **Test the Configuration** to test the configuration of the graphic card.

**NOTE**

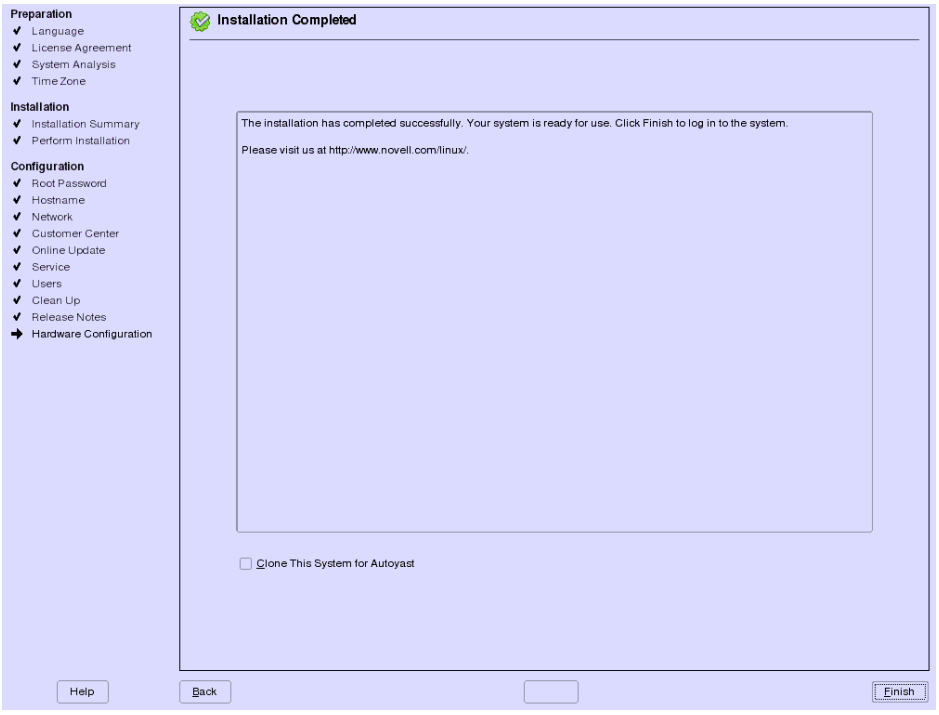
If graphics are displayed, it indicates that the graphic card is configured successfully. Click **Save** to exit.

3. Click **Next**.




**16** Complete the installation.

In the **Installation Completed** window, clear the **Clone This System for Autoyast** check box and click **Finish**.



**17** log in to the OS and eject the disk.

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

   If you can log in to the SUSE Linux OS as the **root** user, it indicates that the SUSE Linux OS is successfully installed. Otherwise, install the OS again.

2. On the **GNOME** desktop, right-click, and choose **Open Terminal** from the shortcut menu to open the CLI. Then, run the **eject** command to eject the disk.

   **NOTE**

   If the IBM blade server is installed by using the drive of the virtual media device, run the **eject** ***Name_of_the_virtual_media_device*** command to remove the DVD.

   Run the following command to check the name of the virtual media equipment:
   `# df -hk`
   If **/dev/sr1 132136 132136 0 100% /media/05_04_2009** is displayed, it indicates that the name of the virtual media equipment is **/dev/sr1**. The equipment name varies according to the actual situation.

**----End**

## Follow-up Procedure

After the SUSE Linux OS installation is completed, you can enable the service to the remote login OS according to the requirements, for details, see **B.1.6 How to Log In to the OS Through the Remote Login Tools?**.

# F.2 Verifying the Installation and Configuration of the OS

This topic describes how to check the OS version, OS patch, the disk partitioning of the system and the language environment variable of the system.

## Procedure

**1** Run the following command to view the OS version:

```
# cat /etc/SuSE-release
```

If the following information is displayed, it indicates that the SUSE Linux version is correct:

```
SUSE Linux Enterprise Server 10 (x86_64)
VERSION = 10
PATCHLEVEL = 3
```

**2** Run the following command to view the OS kernel version:

```
# uname -rv
```

The information similar to **2.6.16.60-0.54.5** is displayed. Here, **2.6.16.60-0.54.5** indicates the kernel version of the OS.

If the kernel version is **2.6.16.60-0.54.5**, it indicates that the kernel version is correct.

**NOTE**

If the SUSE Linux version or the kernel version are not correct, obtain the correct installation DVD of OS and install the OS again.

**3** Ensure that the disk partitioning of the system is correctly.

1. Run the following command to log in to the **YaST2 Control Center**:

   ```
   # yast2
   ```

2. In the **YaST Control Center** dialog box, click **System** > **Partitioner**.
3. View the disk partitioning information in the dialog box of displayed.

   According to the displayed disk partitioning information, check whether the current disk partitioning of the system is consistent with the disk partition planning. If they are inconsistent, you need to reinstall the OS and then partition disks according to the disk partition planning. For the disk partitioning planning, see **I Planning Disk Partitions**.

**4** Ensure that the language environment variable of the system is **en_US**.

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

```
# echo $LANG
```

If **en_US** is not displayed, change the language environment variable description in the **/etc/sysconfig/language** file to **RC_LANG="en_US"**. Perform the following steps:

1. Run the following command to log in to the **YaST2 Control Center**:
   ```
   # yast2
   ```
2. Choose **System** > **/etc/sysconfig Editor**. The **/etc/sysconfig Editor** dialog box is displayed.
3. Choose **System** > **Environment** > **Language** > **RC_LANG**. In **Setting of: RC_LANG**, enter *en_US*.
4. Choose **System** > **Environment** > **Language** > **ROOT_USES_LANG**. Set **ROOT_USES_LANG** to *yes*.
5. Click **Finish**.
6. Run the following commands to restart the OS:
   ```
   # sync;sync;sync;sync
   # shutdown -r now
   ```

**----End**

# G Common Operations for the Blade Server

This topic describes common operations for the blade server. To learn more details and operations about the blade server, see the manual delivered with the blade server to access the official Web site of the blade server vendor.

# G.1 Logging In to the Management Console of an IBM Blade Server

You can log in to the management software of the IBM management module to manage a blade server remotely. This topic describes how to log in to the management software of the IBM management module.

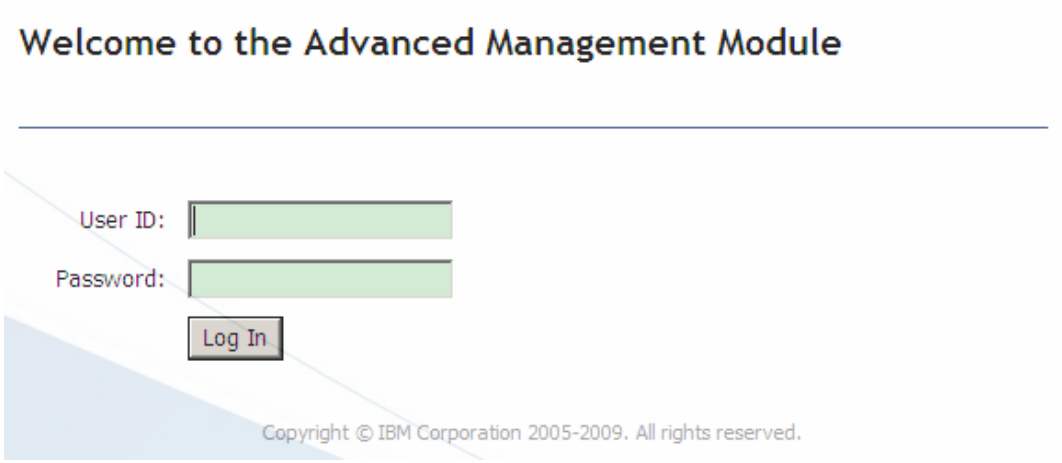
## Prerequisite

The JRE 1.4.2_08 or later must be installed on the Windows management terminal.

## Procedure

1. Log in to the Windows-based management terminal.
2. Open an Internet Explorer window. In the address bar, enter the IP address of the network port on the management module of an IBM blade server, and press **Enter**.

   The login dialog box is displayed.




3. Enter the user name and password of the management module.

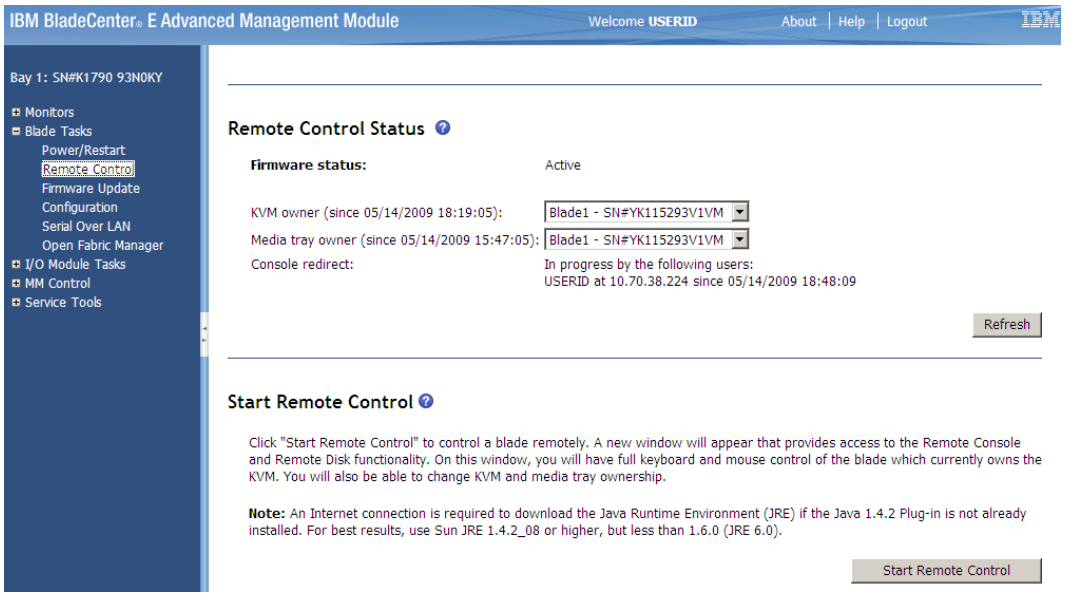
   By default, the login user of the management module of the IBM blade server is **USERID** and the password is **PASSW0RD**. Click **Log In**.

**CAUTION**

When you enter the initial password, note that the character after letter "W" is a number "0", but not a letter "O".

4. Click **Exit Wizard** in the **Advanced Management Module Configuration Wizard** dialog box, and the click **OK** and the management page is displayed.
5. In the left-hand pane, click **Blade Tasks** > **Remote Control**.

   The **Remote Control Status** dialog box is displayed.




6 Click **Start Remote Control**.

The **Warning-Security** dialog box is displayed.


**NOTE**

JRE 1.6.0 is used as an example in this topic. In the case of the JRE of another version, the displayed dialog box is different. Make selection according to the on-screen instructions.

7 Click **Run** to log in to the management console.

**----End**

# G.2 Mounting the Virtual Media on the IBM Blade Server

Mounting the virtual media refers to mounting the CD-ROM on the console to a blade server. In this way, the software can be installed remotely. This topic describes how to mount the virtual media on the IBM blade server.

## Prerequisite

The JRE1.5_08 or a later version must be installed on the Windows management terminal.

## Procedure

1. **Log in to the management console of the IBM blade server**.
2. In the remote management console window, click **Remote Drive**. The **Remote Disk** dialog box is displayed.
3. In the **Media Tray** field, select the board to be operated.
4. In the **Available Resources** pane, select the required installation mode.

   The installation by using the virtual CD-ROM drive is implemented in two ways: using the virtual CD-ROM drive and using image files.

   - If you use the virtual CD-ROM drive for the installation, do as follows:
     1. Click **CD-ROM (G:)** and then click **Add**.

        NOTE

        The drive letter after **CD-ROM** varies according to the actual situation.
     2. Click **Mount All**.

        NOTE

        For information on how to mount a CD-ROM, see the online help of the remote console. Specifically, click  to display the online help of the remote console.

        TIP

        You can run the **df -hk** command in the terminal window to query whether the virtual media is successfully mounted.

        Run the **df -hk** command in the terminal window repeatedly until the terminal displays **/dev/sr1 132136 132136 0 100% /media/05_04_2009**. This message indicates that the virtual media is successfully mounted. **/dev/sr1** indicates the device name. The device name varies according to the actual situation.
     3. Insert the installation CD-ROM of the SUSE Linux 10 Enterprise Server 10 SP3 to the CD-ROM drive of the computer where the management console resides.
   - If you use the image files for the installation, do as follows:
     1. Click **Select Image...** and then click **Add** .The **Open** dialog box is displayed.
     2. Select the location of the image files and then click **Open**.

        **CAUTION**

        Make sure that the name of the directory where the image files are saved is short and contains no space, punctuation or non-alphabetic characters.

**----End**

## Follow-up Procedure

To eject the CD-ROM, do as follows:

1. Run the following command to check the name of the virtual media device:
   ```
   # df -hk
   ```
   If the terminal displays **/dev/sr1 132136 132136 0 100% /media/05_04_2009**, it indicates that the name of the virtual media device is **/dev/sr1**. The device name varies according to the actual situation.
2. Run the following command to eject the CD-ROM:
   ```
   # eject Name of the virtual media device
   ```

# G.3 How to View the MAC Address of the External Communication NIC of an IBM Blade Server

## Question

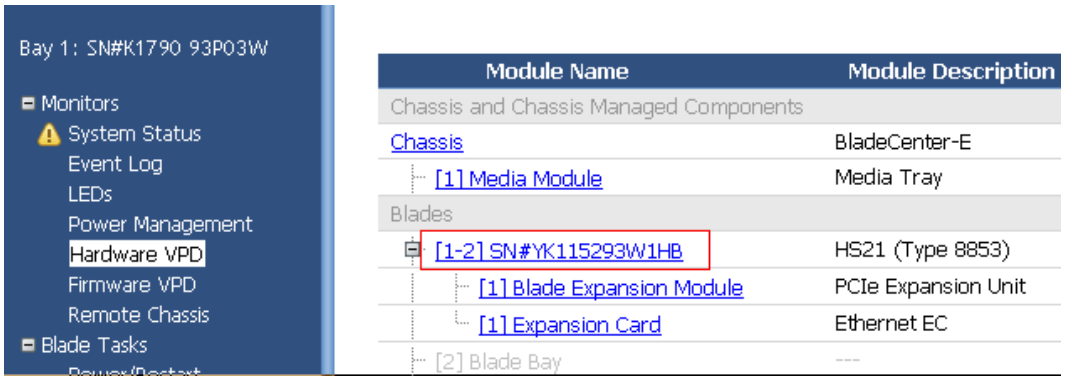
An IBM blade server is connected to the public network through I/O module 1 and I/O module 2. The system IP address of the IBM blade server must be set on the external communication NIC. When setting the system IP address, you need to select the NIC based on the MAC address.

## Answer

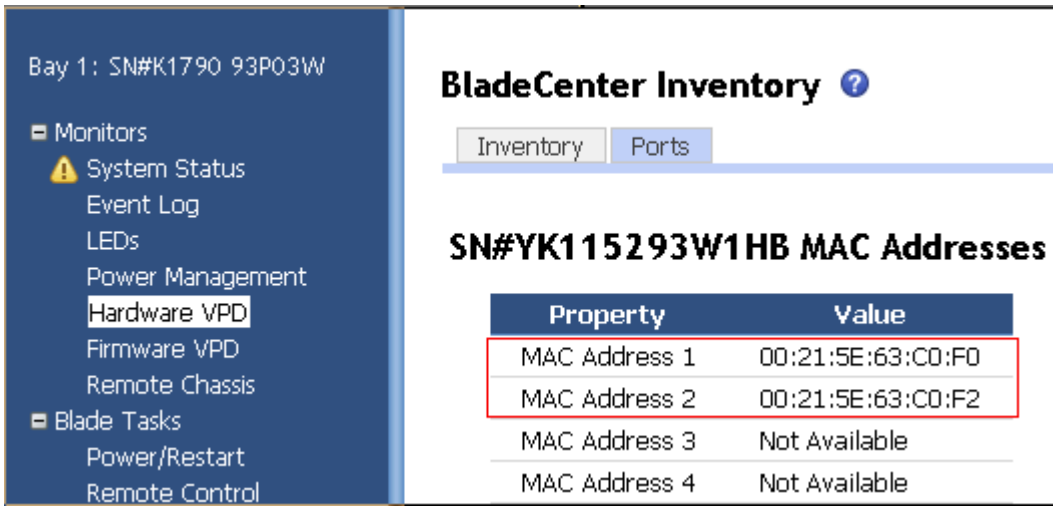
**1** Log in to the management console of the IBM blade server.

**2** Choose **Monitors** > **Hardware VPD**.

**3** On the **Hardware Topology** tab page of the **BladeCenter Hardware Information** window, search for the associated card by card number. Then, click SN number.




**4** In the **BladeCenter Inventory** window, click the **Ports** tab to view the MAC address of the external communication NIC.




**----End**

# G.4 Logging In to the Management Console of an ATAE Blade Server

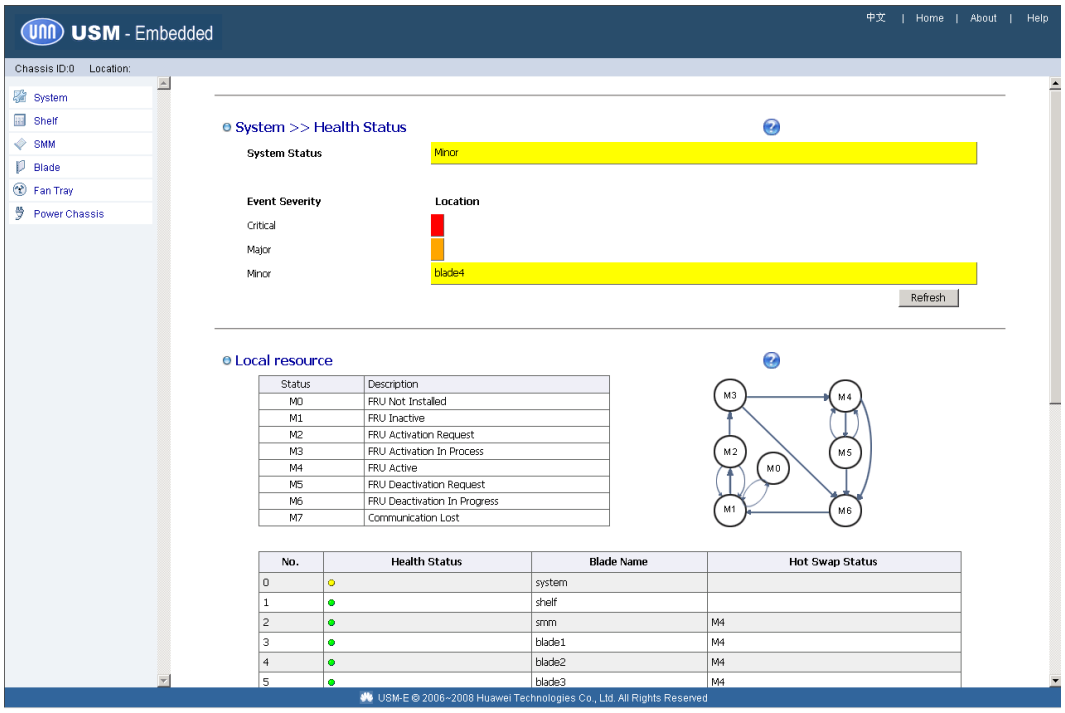
You can log in to the USM-E management software to manage an ATAE blade server remotely. This topic describes how to log in to the USM-E management software.

## Prerequisite

The JRE 1.5_08 or later must be installed on the Windows management terminal.

## Procedure

1. Log in to the Windows-based management terminal.
2. Open an Internet Explorer window. In the address bar, enter the IP address of the network port on the management unit of an ATAE blade server, and press **Enter**.
   The login dialog box is displayed.
3. Enter the user name **root** and the password **huaweiosta**, and click **OK**.



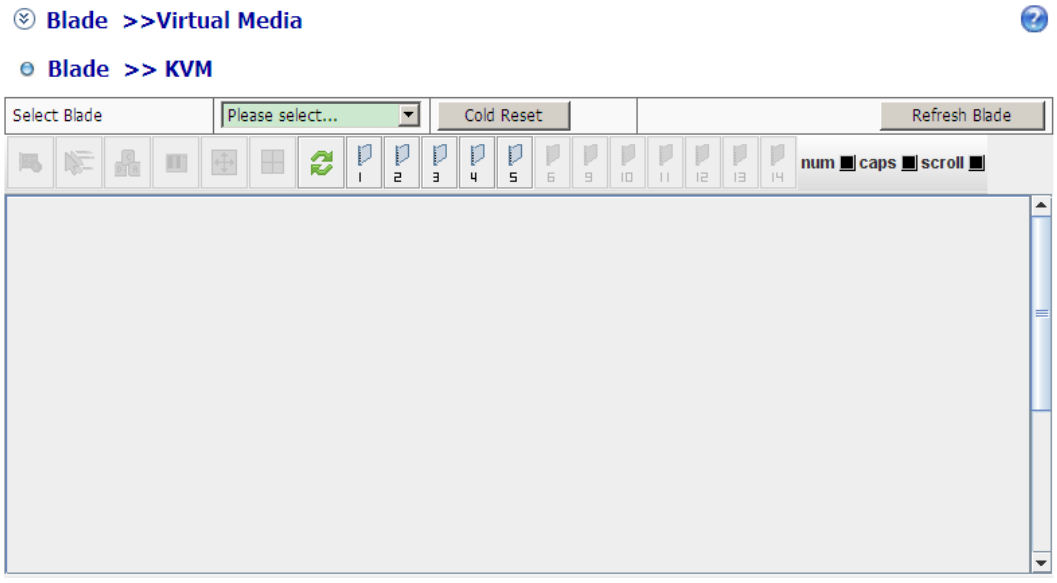

**4** In the left-hand pane, click **Blade** > **Remote Control**.

The **Warning-Security** dialog box is displayed.

**NOTE**

JRE 1.6.0 is used as an example in this topic. In the case of the JRE of another version, the displayed dialog box is different. Make selection according to the on-screen instructions.

**5** Click **Run** to log in to the management console.




**6** In the Blade >> KVM panel, select the required board.

**CAUTION**

Click the board number on the toolbar to select the required board.

**TIP**

- To enter the full screen mode, click  on the toolbar.
- To restore from the full screen mode to window, move the mouse to upper middle of the screen, press **Ctrl+Shift+Alt** and click  in the upper portion of the screen.

**----End**

# G.5 How to View the MAC Address of the Base Plane of an ATAE Blade Server

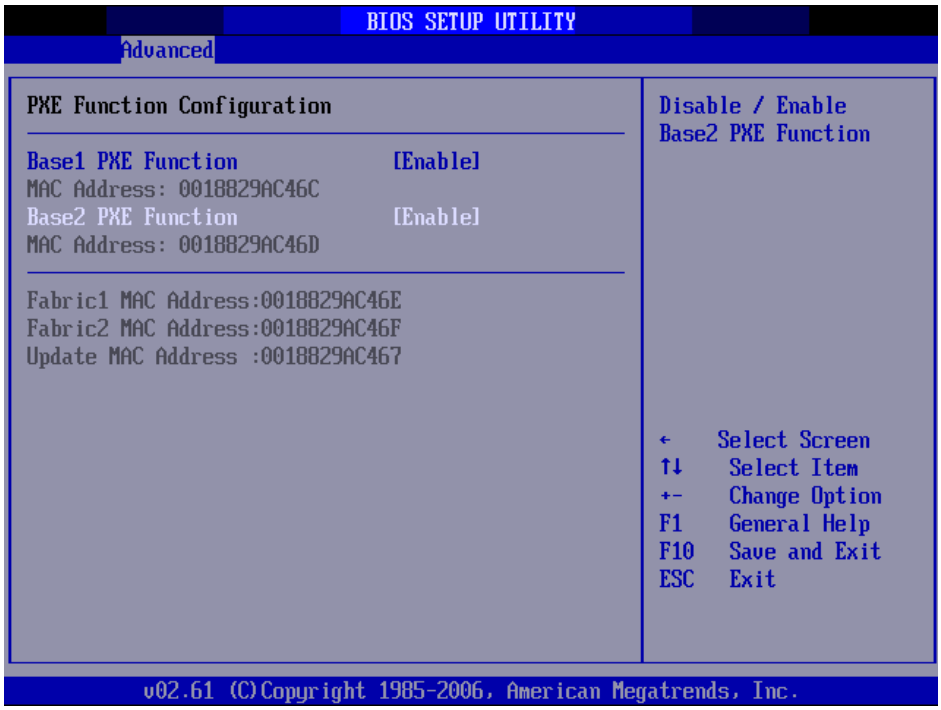
## Question

An ATAE blade server is connected to the public network through the base plane. The system IP address of an ATAE blade server must be set on the NIC of the base plane. When setting the system IP address, you need to select the NIC based on the MAC address.

## Answer

1. Log in to the management console of an ATAE blade server.
2. In the Blade >> KVM panel, select the required board from **Select Blade**, and click **Cold Reset** to restart the blade server.
3. In the process of restarting the blade server, when the **American Megatrends** window is displayed, press **Delete** to display the **BIOS SETUP UTILITY** window.
4. In the **BIOS SETUP UTILITY** window, press **Tab** to choose **Advanced** > **PXE Function Configuration** from the main menu.

   The **PXE Function Configuration** window is displayed. Record the MAC addresses of the base plane.




**TIP**

Record the MAC addresses of the base plane so that you can select the correct NICs for external communication when you set the network.

Press **Esc** to return to the main menu.

**----End**

# H 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**.<br>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**.<br>● Set the RAID Level to **RAID5**.<br>● Set the disk type to **SAS**.<br>● The first five disks serve as the RAID group. |
| LUN | Configure one LUN as follows:<br>● LUN information<br>– Name: LUN001<br>– Capacity: 1000 GB<br>– Stripe unit size: 32 KB<br>– Home controller: controller A<br>● Cache strategy<br>– Prefetch strategy: intelligent<br>– Write strategy: write back (mirroring)<br>● Mapping mode<br>Mapping object: host group name **HostGroup001** |
| Port | ● Set the type to **FC**.<br>● Set the name associated with the first identifier to **port1**.<br>● 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.

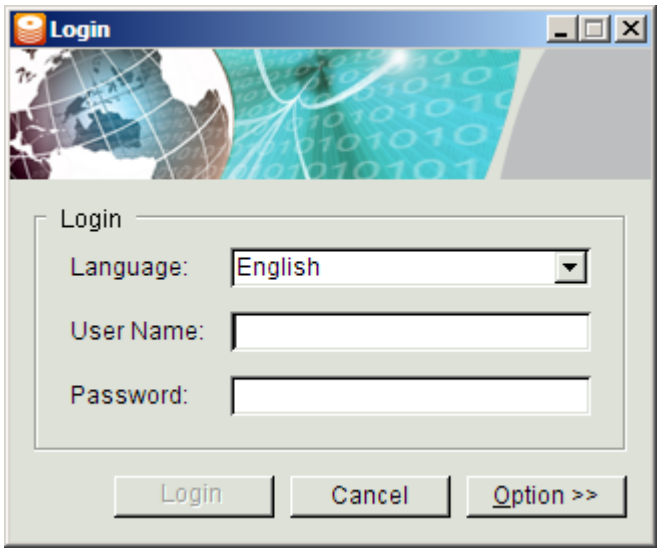
**CAUTION**

- 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**

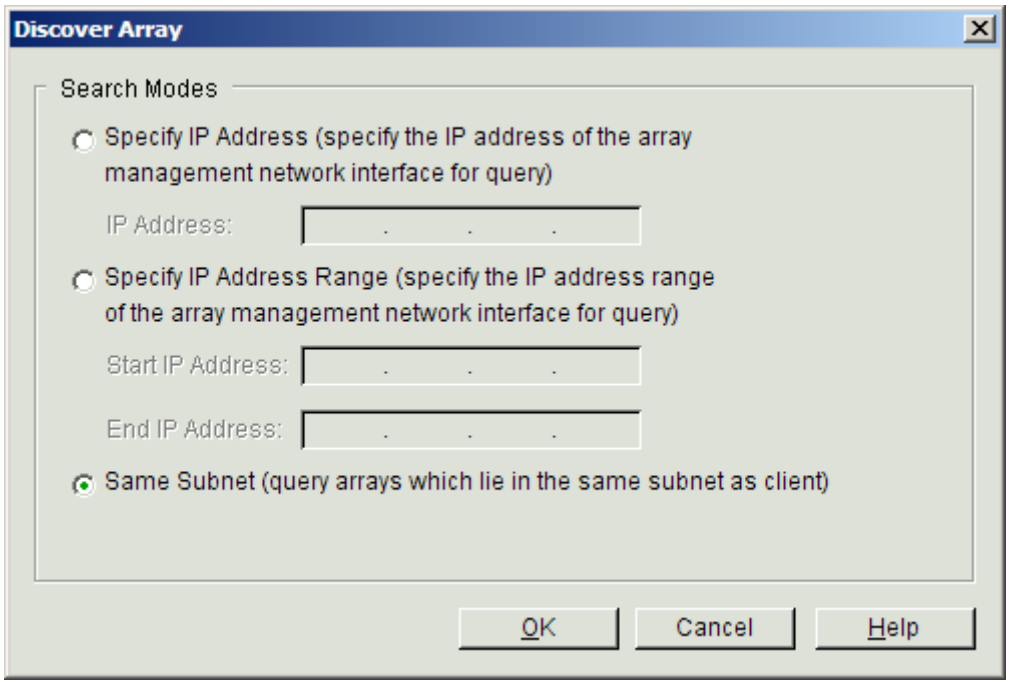
   - A disk array can be discovered only when the entered user name and password are the same as those of the disk array.
   - The default user name and password for logging in to the ISM are **admin** and **123456**. After login, change the password immediately and keep the password confidential.

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.



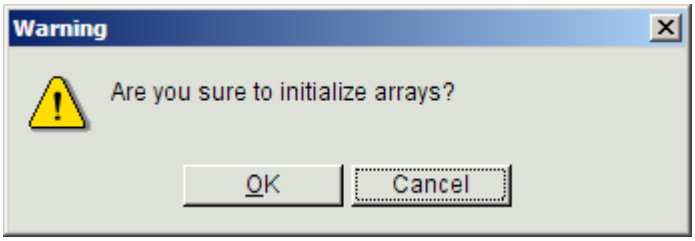

2. Select a mode for discovering disk arrays according to the conditions at your site. **Table H-1** describes the parameters for discovering disk arrays.

**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.<br>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:<br>● The discovery range is the IP subnet segment of the ISM client.<br>● 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.<br>● 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. |

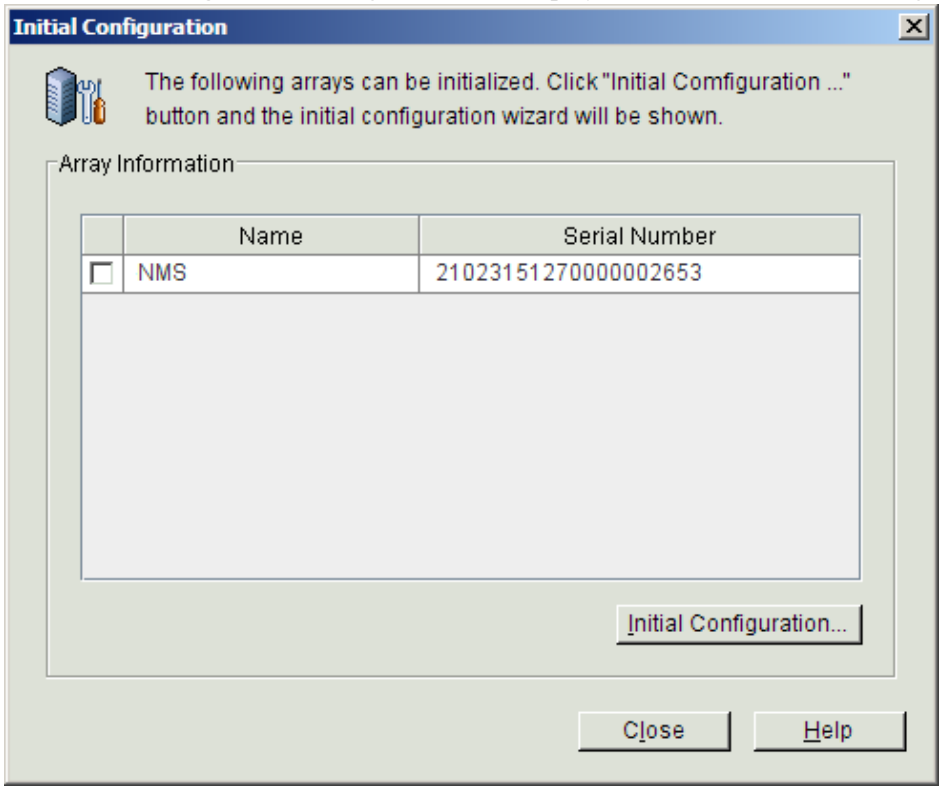
3. Click **OK**. After disk arrays are discovered, the **Info** dialog box will be displayed, prompting an operation success.

4. Click **OK**. The **Warning** dialog box will be displayed.

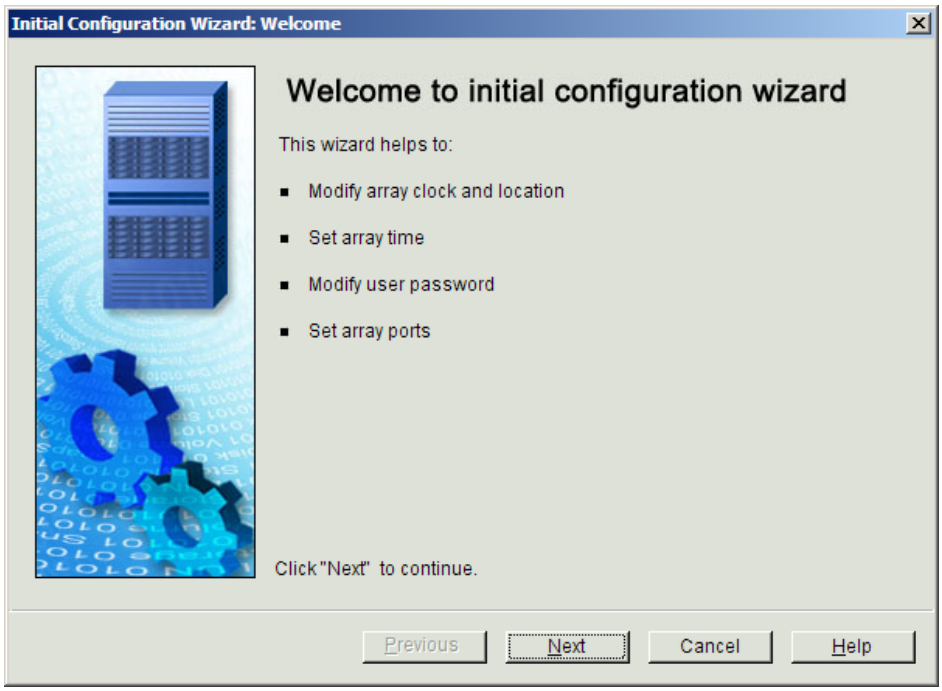



**3** Initialize the configuration.

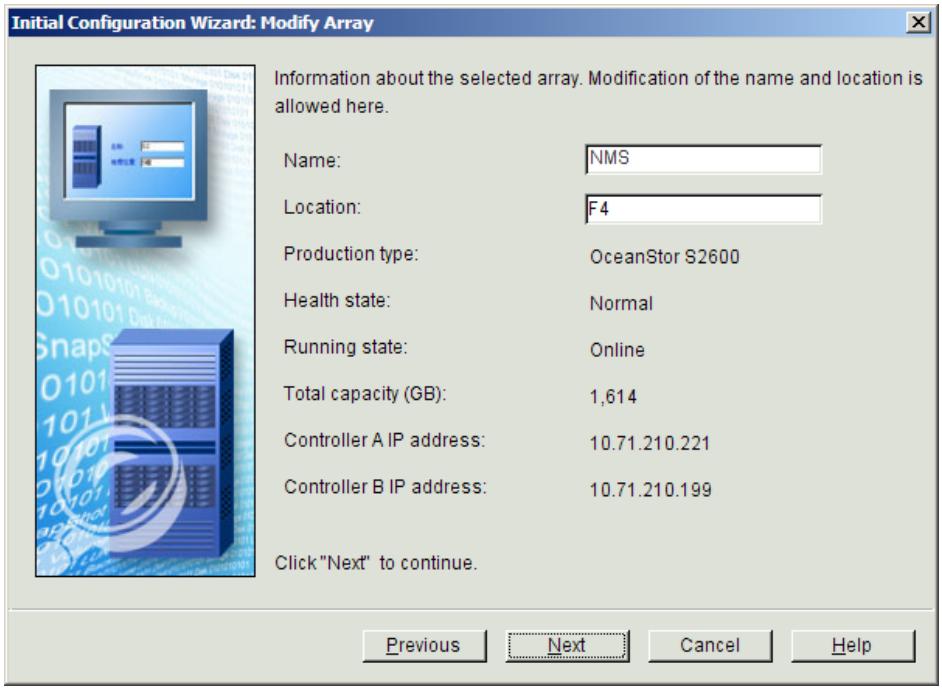
1. In the **Warning** dialog box, click **OK** to initialize the disk array.
   The **Initial Configuration** dialog box will be displayed, as shown in the following figure.




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.

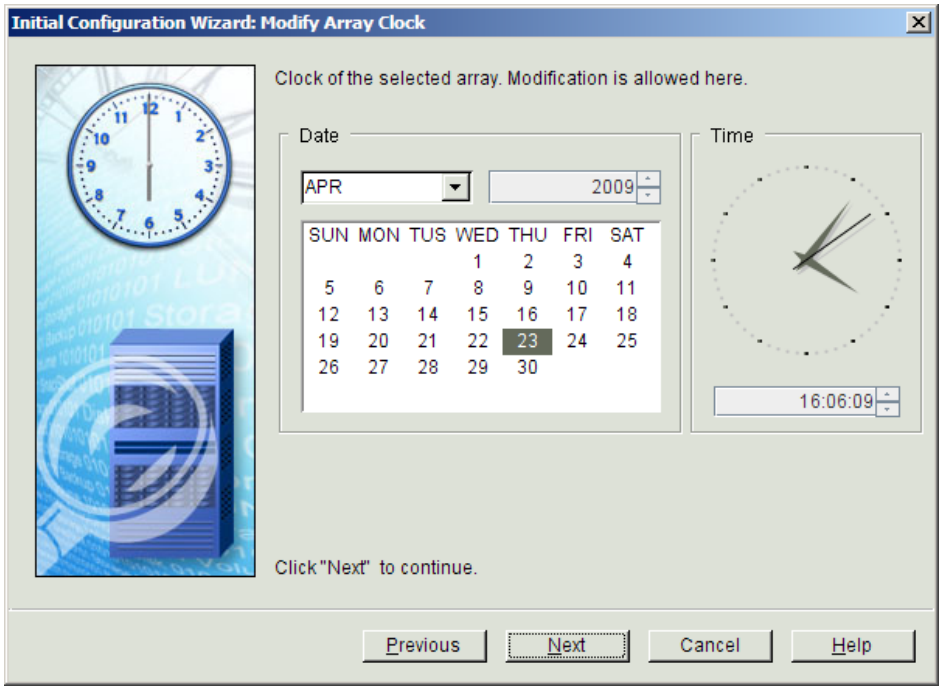



4. Enter the name of the disk array in the **Name** text box and the location information in the **Location** text box. **Table H-2** describes the parameters for modifying a disk array.

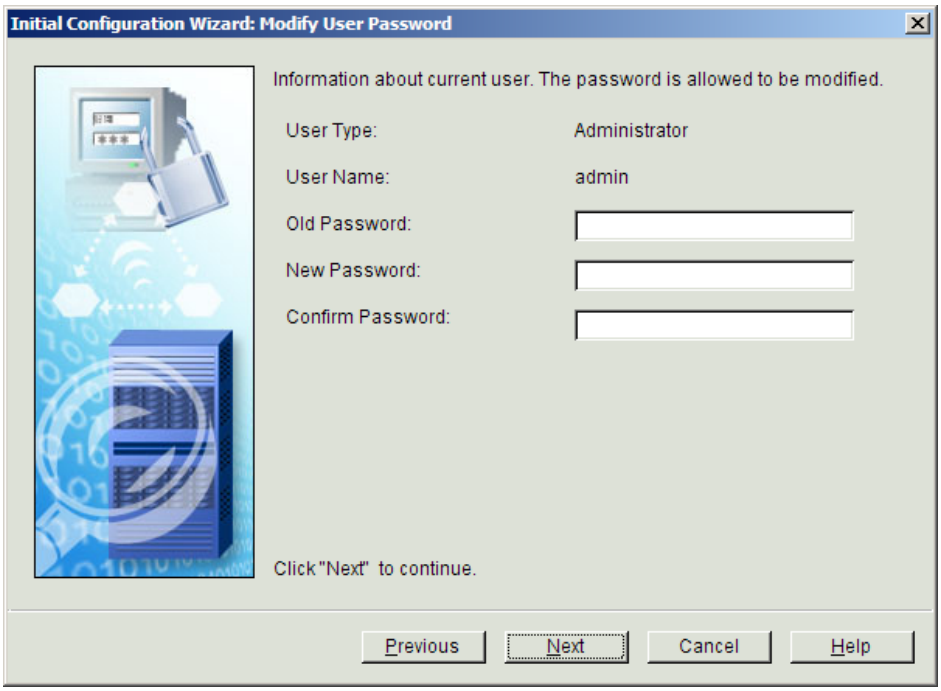
**Table H-2** Parameters for modifying a disk array

| Parameter | Description |
| --- | --- |
| Name | Specifies the name of the OceanStor S2600 disk array to be configured. When setting this parameter, note that:<br>● This parameter contains only the characters and numerals in DBC case, underscores (_), en-dash symbols (-), and simplified Chinese characters.<br>● 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:<br>● This parameter contains only the characters and numerals in DBC case, underscores (_), en-dash symbols (-), and simplified Chinese characters.<br>● 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.

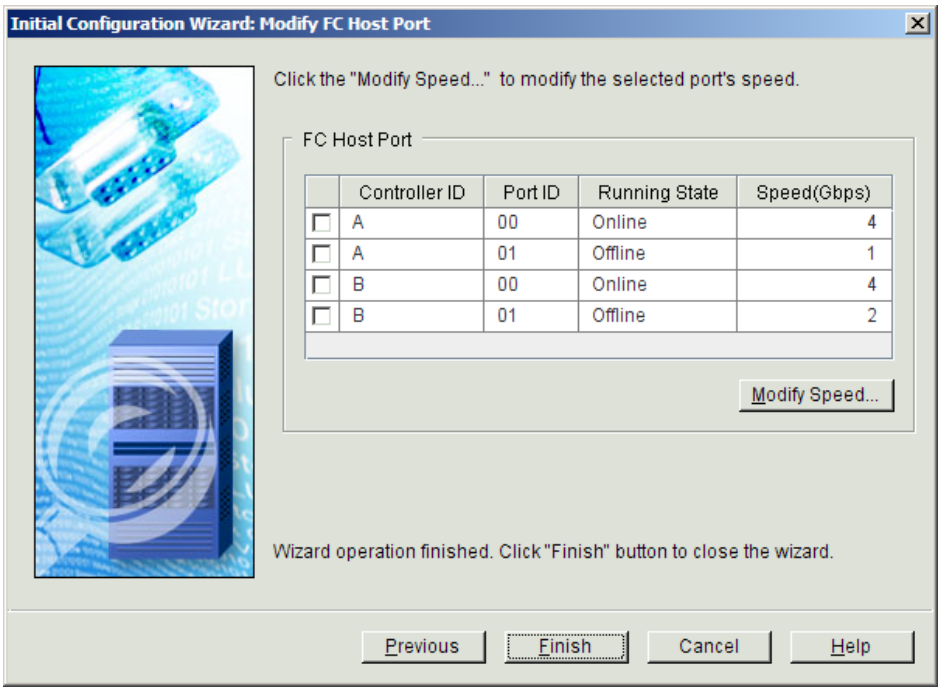
**Table H-3** Parameters for changing the user password

| 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:<br>● This parameter ranges from 6 to 16 characters.<br>● 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**

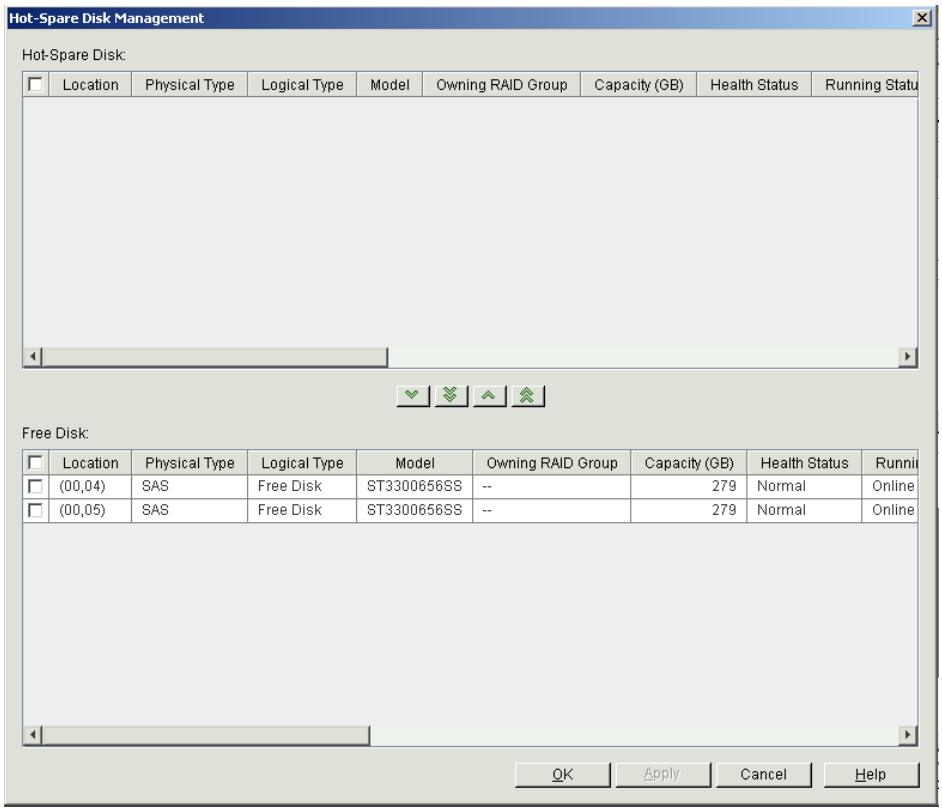
Click **Modify Speed** if the port rate needs to be changed. The default rate of an online port is 4 Gbit/s.



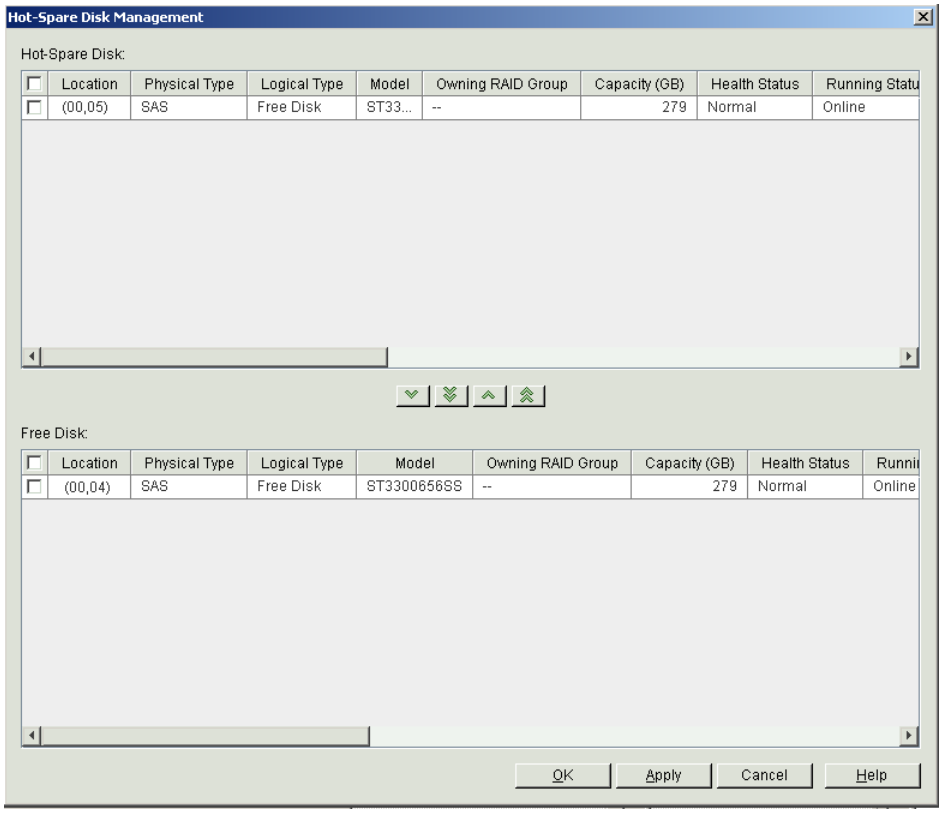

9. Click **Finish** to complete the initial configuration.
10. Click **Close** to exit.

**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.



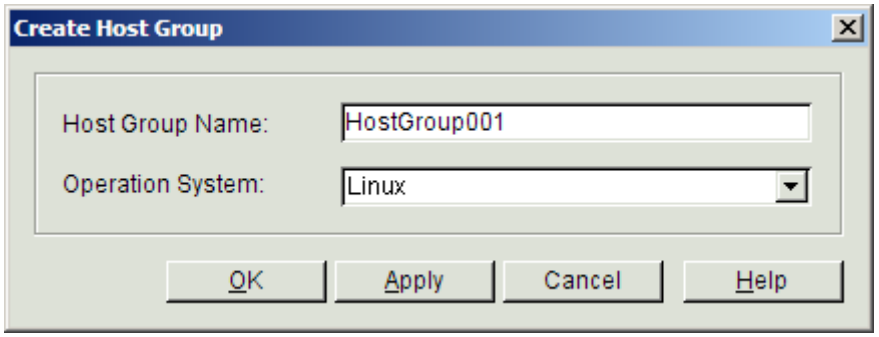

3. Select disk location **(00,05)** from the free disk list and click the third button (  ) in the middle portion of the dialog box to add the selected disk to the hot spare disk list.



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.



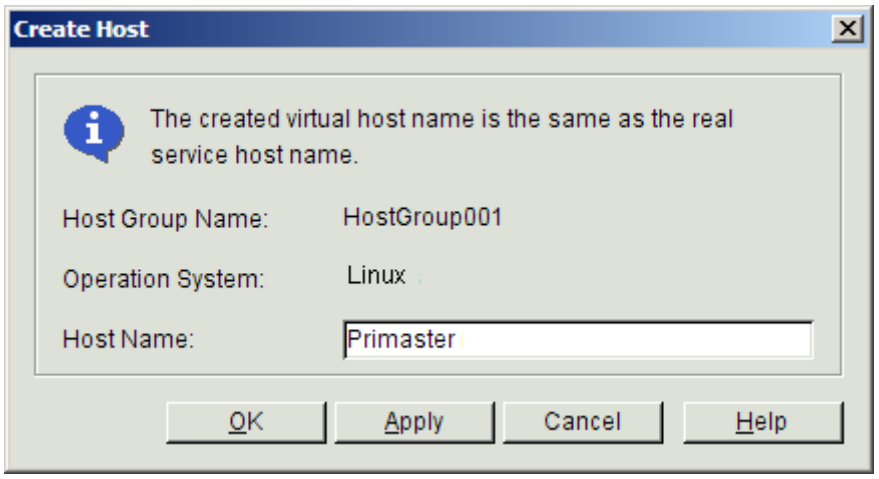

3. Select **Linux**, and then click **OK**.

   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

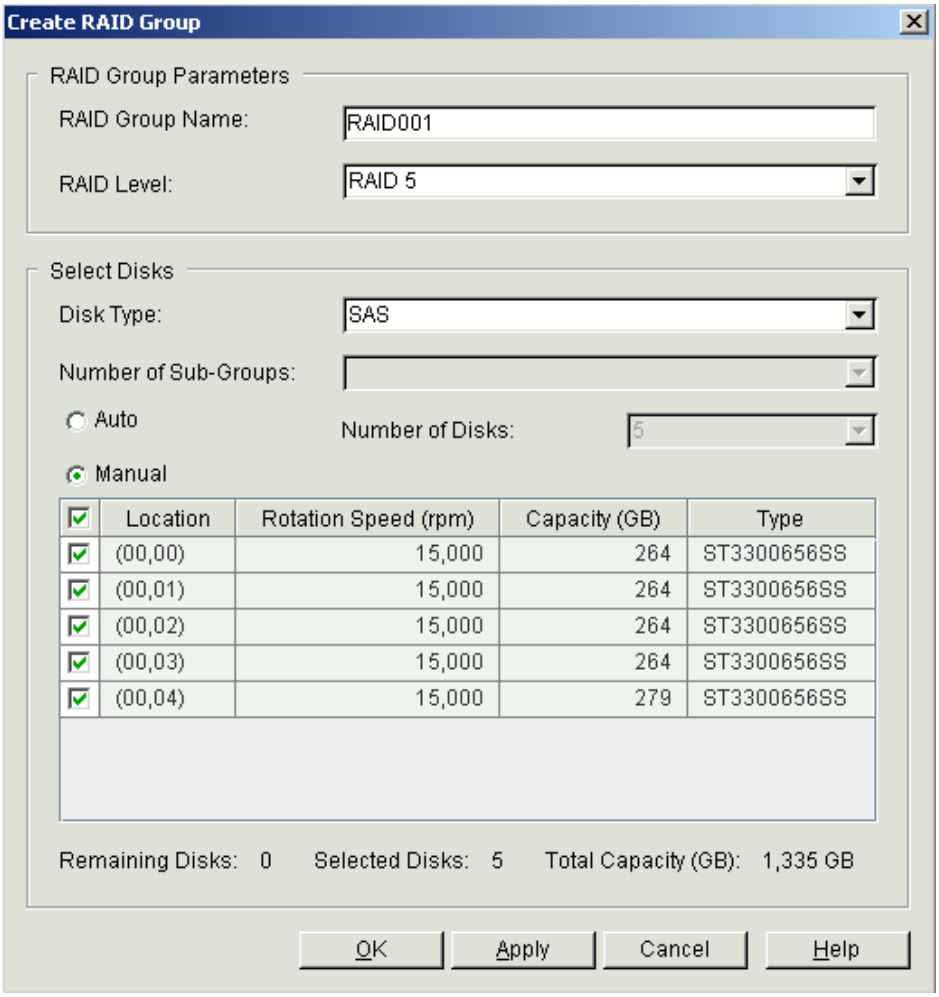
   It is recommended to enter the host name of the server connected to the disk array so that the host name is easy to remember.

   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.

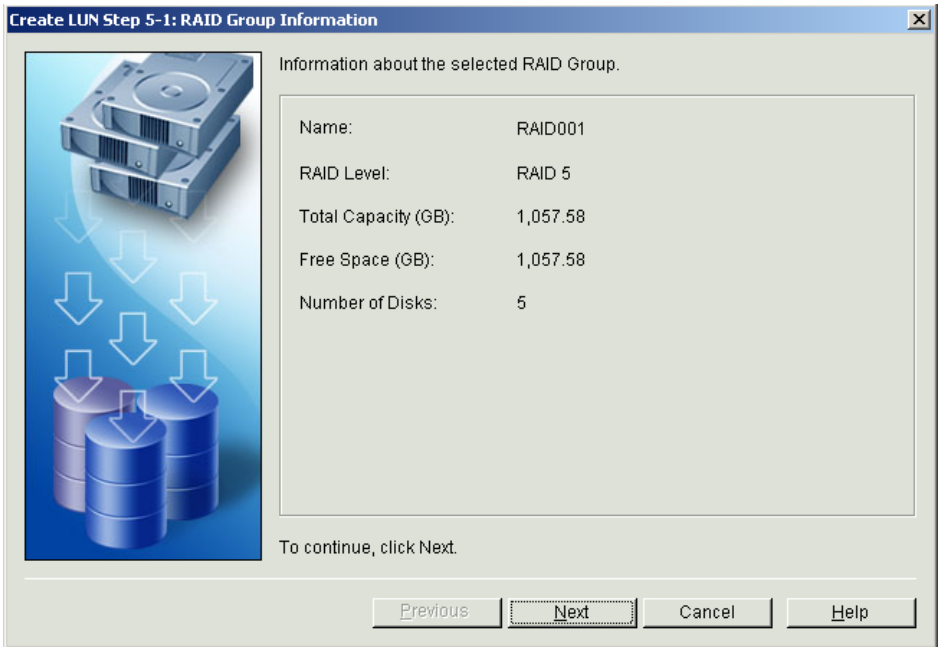
2. Choose **Configuration** > **Create RAID Group** from the main menu. In the **Create RAID Group** dialog box, modify the settings, as shown in the following figure.




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.

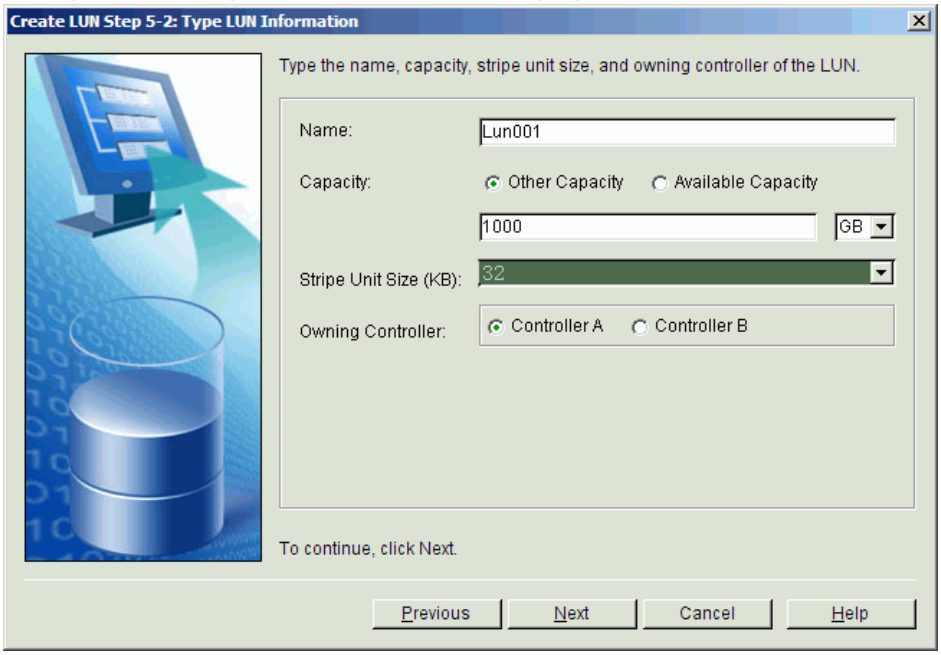
**7** Create Lun001.

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.



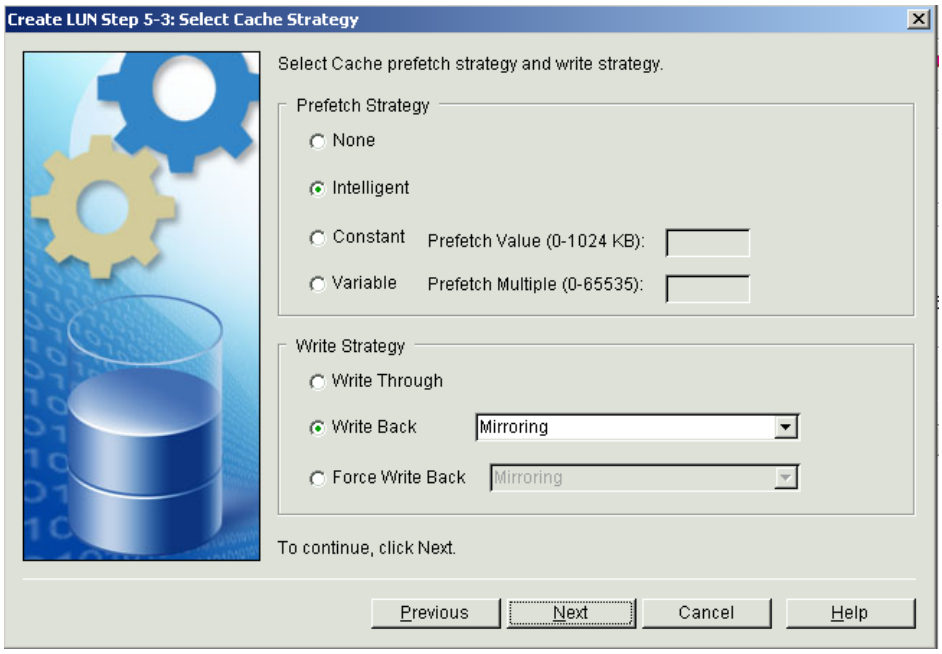

3. Click **Next**. The **Create LUN Step 5-2: Type LUN Information** dialog box will be displayed.

   Configure the settings as shown in the following figure.



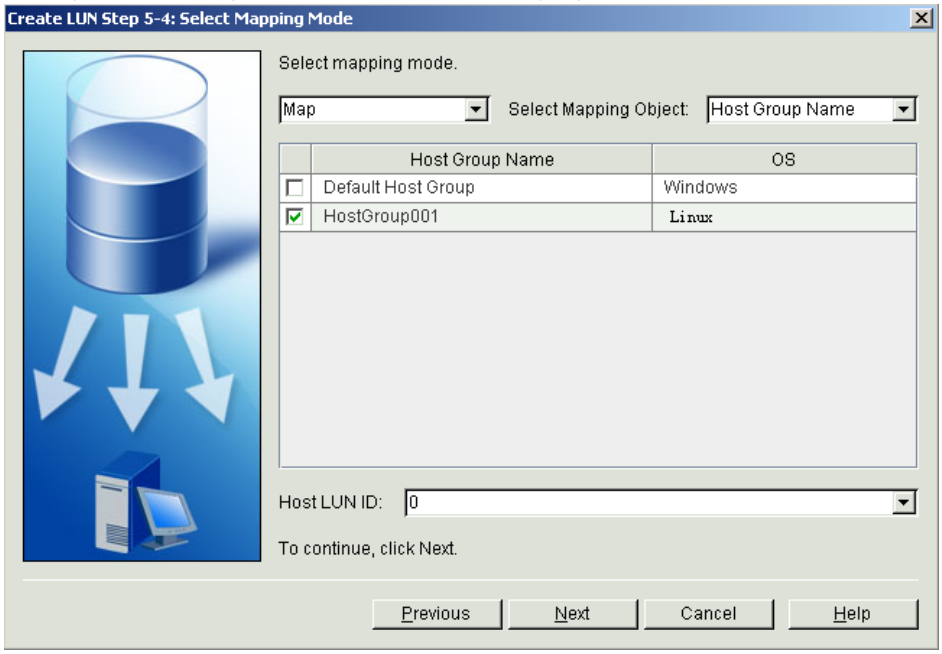

4. Click **Next**. The **Create LUN Step 5-3: Select Cache Strategy** dialog box will be displayed.

   Configure the settings as shown in the following figure.



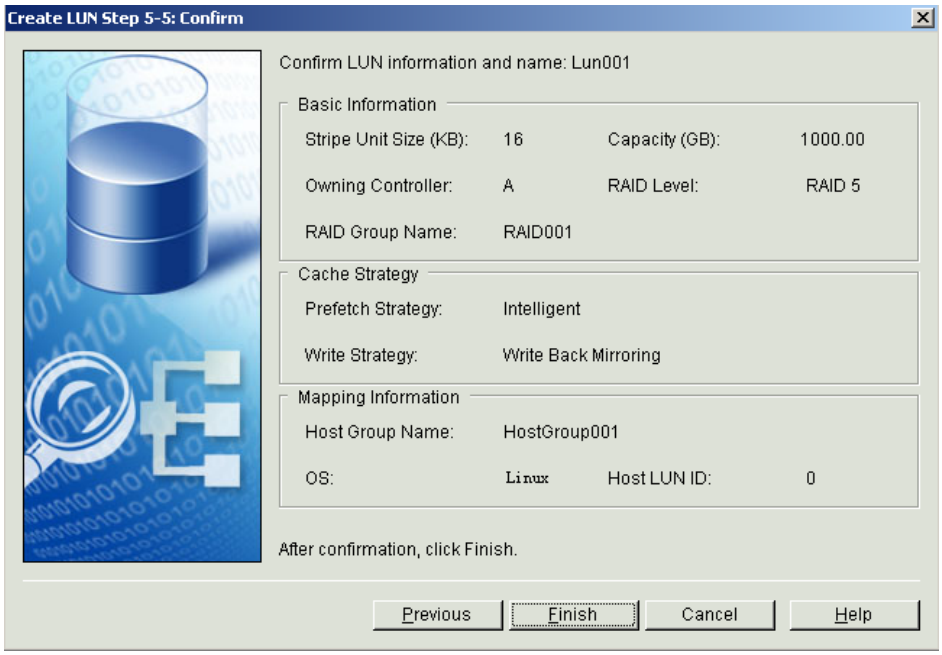

5. Click **Next**. The **Create LUN Step 5-4: Select Mapping Mode** dialog box will be displayed.

   Configure the settings as shown in the following figure.




6. Click **Next**. The **Create LUN Step 5-5: Confirm** dialog box will be displayed.

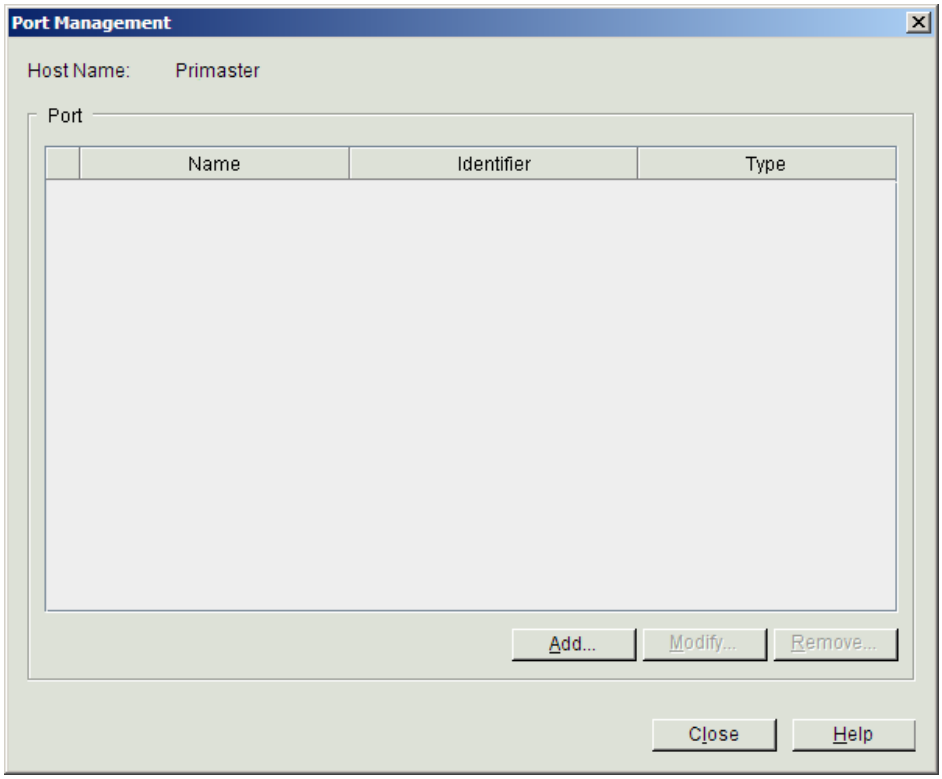
   Configure the settings as shown in the following figure.



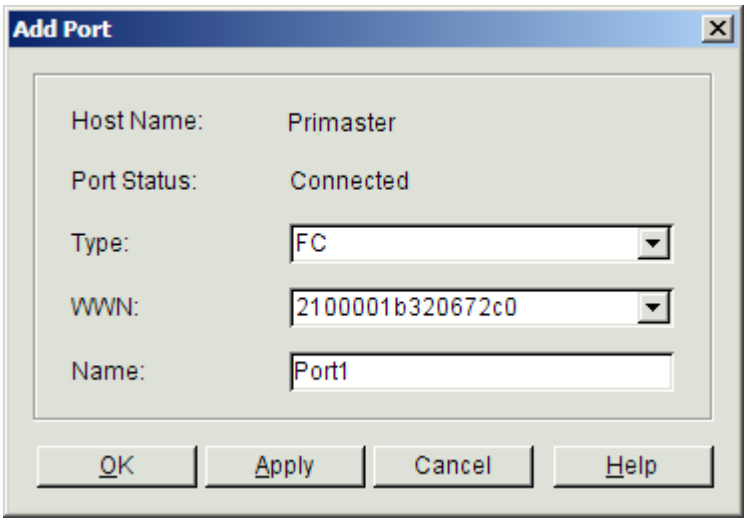

7. Click **Finish**. The **Info** dialog box will be displayed indicating that the operation was completed.
8. Click **OK**. Creation of Lun001 is complete.

**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:

```
# cd /sys/class/scsi_host/hostport ID
# cat state
```

**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:

```
# lssci
```

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:

```
Link Up - Loop
```

**NOTE**

If the fiber card is not in the **Link Up** 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 -r now
```

**----End**

# I Planning Disk Partitions

This topic describes the disk partitioning scheme that is determined according to the sizes and quantity of the server hard disks.

Before manually installing the OS, you need to specify the disk partitioning scheme. If the OS is installed through the rapid installation DVD, you can skip this part. The installation software automatically performs disk partitioning according to the disk size.

The standard configuration of an SUSE Linux server is two hard disks with the capacity of 146 GB. One of the disks functions as the mirrored disk that need not be partitioned.

**CAUTION**

In the high availability system (SUSE Linux-distributed), the partition schemes of the master server and slave server in primary and secondary sites are the same. For details, see **Table I-1**.

**Table I-1** Scheme for disk partition

| Partition Type | Path | Formatted or Not | Load Point | File System | Number of Hard Disks (146 GB) | Description |
|---|---|---|---|---|---|---|
| Primary partition | /dev/sda1 | Yes | / | Ext3 | 10 | It is the root partition. |
| | /dev/sda2 | Yes | swap | Swap | 16 | It is used for switching data in the system. |
| Extended partition | /dev/sda3 | Yes | | Ext3 | | In addition, the size of this partition is for reference and is allocated automatically by the system. Therefore, you need not set the size of this partition manually. |

| Partition Type | Path | Formatted or Not | Load Point | File System | Number of Hard Disks (146 GB) | Description |
|---|---|---|---|---|---|---|
| Logical partition | /dev/sda5 | Yes | /usr | Ext3 | 10 | It is a logical partition in the extended partition. This partition is used for storing programs or files of users. |
| | /dev/sda6 | Yes | /var | Ext3 | 10 | It is a logical partition in the extended partition. This partition is used for storing system logs. |
| | /dev/sda7 | Yes | /opt | Ext3 | 80 | It is a logical partition in the extended partition. |
| | /dev/sda8 | Yes | /export/home | Ext3 | 10 | It is a logical partition in the extended partition. |

# J 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 |