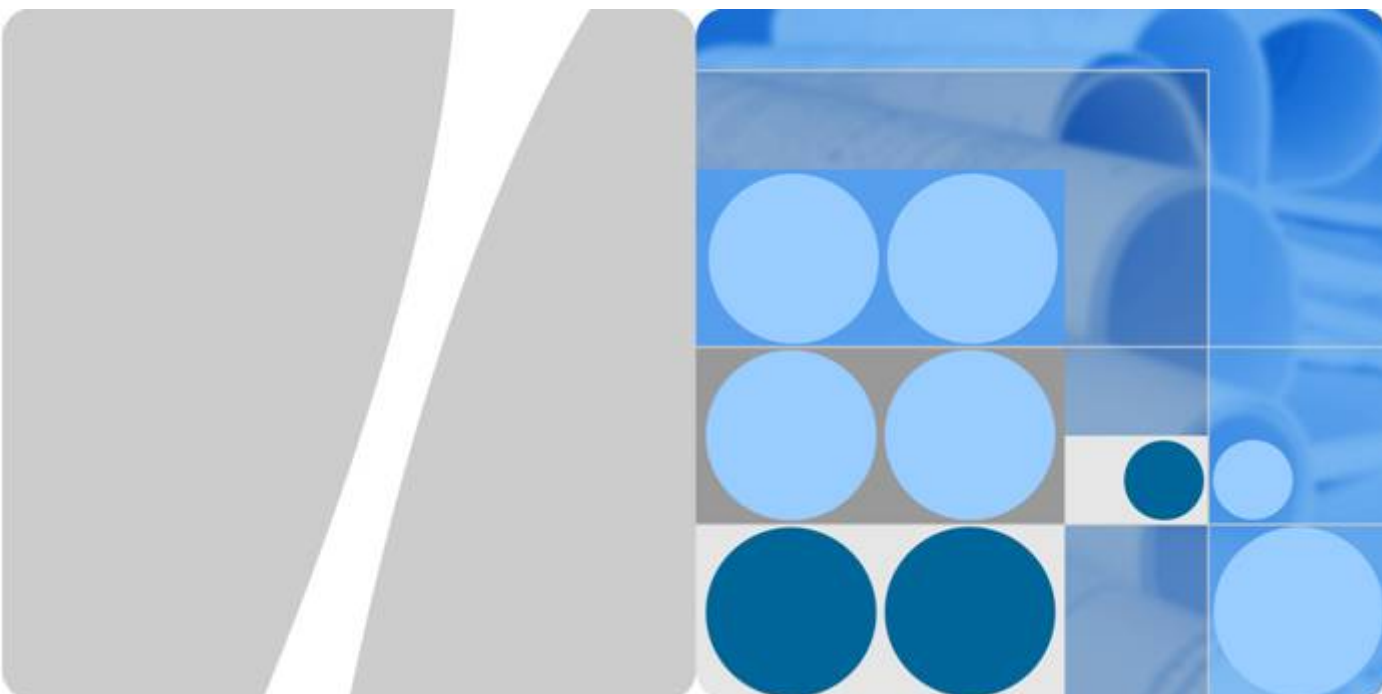




iManager U2000 Unified Network Management System

V100R002C01

Commissioning Guide

Issue **06**
Date **2010-11-19**

HUAWEI TECHNOLOGIES CO., LTD.



Copyright © Huawei Technologies Co., Ltd. 2010. All rights reserved.

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

Trademarks and Permissions



HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute 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 commission the U2000 and obtain the reference information required in the commissioning process.

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 .
<i>Italic</i>	Command arguments are in <i>italics</i> .
[]	Items (keywords or arguments) in brackets [] are optional.
{ x y ... }	Optional items are grouped in braces and separated by vertical bars. One item is selected.
[x y ...]	Optional items are grouped in brackets and separated by vertical bars. One item is selected or no item is selected.
{ x y ... }*	Optional items are grouped in braces and separated by vertical bars. A minimum of one item or a maximum of all items can be selected.
[x y ...]*	Optional items are grouped in brackets and separated by vertical bars. Several items or no item can be selected.

GUI Conventions

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

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

Change History

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

Changes in Issue 06 (2010-11-19)

The sixth commercial release has the following updates:

Fixed some bugs.

Changes in Issue 05 (2010-10-20)

The fifth commercial release has the following updates:

Fixed some bugs.

Changes in Issue 04 (2010-09-24)

The fourth commercial release has the following updates:

Fixed some bugs.

Changes in Issue 03 (2010-08-16)

The third commercial release has the following updates:

Fixed some bugs.

Changes in Issue 02 (2010-07-16)

The second commercial release has the following updates:

Fixed some bugs.

Changes in Issue 01 (2010-05-18)

Initial release.

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

About This Document.....	iii
1 Commissioning Overview.....	1-1
1.1 Commissioning Scenarios.....	1-2
1.2 Preparing for U2000 Commissioning.....	1-2
1.3 Commissioning Process.....	1-3
2 (Optional) Modifying System Parameters.....	2-1
2.1 Modifying Parameters for a Single-Server System (Windows).....	2-2
2.1.1 Preparing for System Parameter Modification.....	2-2
2.1.1.1 Networking Structure.....	2-3
2.1.1.2 Environment Requirements.....	2-3
2.1.1.3 Collecting Planning Information.....	2-4
2.1.1.4 Checking Hardware Connections.....	2-6
2.1.1.5 Powering On a Server.....	2-8
2.1.1.6 Applying for a U2000 License.....	2-9
2.1.1.7 Checking System Installation.....	2-10
2.1.2 Modifying System Parameters.....	2-10
2.1.3 Loading a U2000 License.....	2-11
2.1.4 Starting a Single-Server System (Windows).....	2-13
2.2 Modifying Parameters for a Single-Server System (Solaris).....	2-14
2.2.1 Preparing for System Parameter Modification.....	2-15
2.2.1.1 Networking Structure.....	2-16
2.2.1.2 Environment Requirements.....	2-17
2.2.1.3 Collecting Planning Information.....	2-17
2.2.1.4 Checking Hardware Connections.....	2-20
2.2.1.5 Powering On a Server.....	2-24
2.2.1.6 Applying for a U2000 License.....	2-26
2.2.1.7 Checking System Installation.....	2-28
2.2.2 Modifying System Parameters.....	2-28
2.2.3 Loading a U2000 License.....	2-29
2.2.4 Starting a Single-Server System (Solaris).....	2-32
2.3 Modifying Parameters for a Single-Server System (SUSE Linux-Distributed).....	2-35
2.3.1 Preparing for System Parameter Modification.....	2-36

2.3.1.1 Networking Structure.....	2-36
2.3.1.2 Environment Requirements.....	2-38
2.3.1.3 Collecting Planning Information.....	2-39
2.3.1.4 Checking Hardware Connections.....	2-42
2.3.1.5 Powering On a Server.....	2-45
2.3.1.6 Applying for a U2000 License.....	2-46
2.3.1.7 Checking System Installation.....	2-48
2.3.2 Modifying System Parameters.....	2-48
2.3.3 Loading a U2000 License.....	2-49
2.3.4 Starting the Single-Server System (SUSE Linux-Distributed).....	2-54
2.4 Modifying the Parameters of the High Availability System (Windows).....	2-57
2.4.1 Preparing for the Modification of System Parameters.....	2-58
2.4.1.1 Networking Structure.....	2-58
2.4.1.2 Environment Requirements.....	2-59
2.4.1.3 Collecting Planning Information.....	2-60
2.4.1.4 Checking Hardware Connections.....	2-63
2.4.1.5 Powering On a Server.....	2-65
2.4.1.6 Applying for a Veritas License.....	2-65
2.4.1.7 Applying for a U2000 License.....	2-66
2.4.1.8 Checking System Installation.....	2-67
2.4.2 Loading or Updating a License File.....	2-68
2.4.2.1 Updating a Veritas License.....	2-69
2.4.2.2 Loading a U2000 License.....	2-69
2.4.3 Modifying System Parameters.....	2-72
2.4.4 Starting the High Availability System (Windows).....	2-73
2.5 Modifying Parameters for a High Availability System (Solaris).....	2-75
2.5.1 Preparing for the Modification of System Parameters.....	2-75
2.5.1.1 Networking Structure.....	2-76
2.5.1.2 Environment Requirements.....	2-77
2.5.1.3 Collecting Planning Information.....	2-77
2.5.1.4 Checking Hardware Connections.....	2-88
2.5.1.5 Powering On a Server.....	2-91
2.5.1.6 Applying for a Veritas License.....	2-93
2.5.1.7 Applying for a U2000 License.....	2-94
2.5.1.8 Checking System Installation.....	2-96
2.5.2 Loading or Updating a License File.....	2-100
2.5.2.1 Updating a Veritas License.....	2-100
2.5.2.2 Loading a U2000 License.....	2-102
2.5.3 Modifying System Parameters.....	2-105
2.5.4 Starting a High Availability System (Solaris).....	2-106
2.6 Modifying the Parameters of the High Availability System (SUSE Linux-Distributed).....	2-109
2.6.1 Preparing for the Modification of System Parameters.....	2-109

2.6.1.1 Networking Structure.....	2-110
2.6.1.2 Environment Requirements.....	2-112
2.6.1.3 Collecting Planning Information.....	2-112
2.6.1.4 Checking Hardware Connections.....	2-117
2.6.1.5 Powering On a Server.....	2-121
2.6.1.6 Applying for a Veritas License.....	2-122
2.6.1.7 Applying for a U2000 License.....	2-123
2.6.1.8 Checking System Installation.....	2-125
2.6.2 Loading or Updating a License File.....	2-128
2.6.2.1 Updating a Veritas License.....	2-128
2.6.2.2 Loading a U2000 License.....	2-129
2.6.3 Modifying System Parameters.....	2-132
2.6.4 Starting the High Availability System (SUSE Linux-Distributed).....	2-134
3 Configuring System NTP Solutions.....	3-1
3.1 NTP Overview.....	3-2
3.1.1 Purpose of Time Synchronization.....	3-2
3.1.2 Overview of Time Synchronization.....	3-2
3.1.3 Time Synchronization Principle.....	3-3
3.2 NTP Configuration Schemes.....	3-6
3.2.1 Configuring the NTP Solution to the Installation Scheme of the Single-Server System (Windows)	3-7
3.2.2 Configuring the NTP Solution to the Installation Scheme of the Single-Server System (Solaris).....	3-9
3.2.3 Configuring the NTP Solution to the Installation Scheme of the Single-Server System (SUSE Linux-Distributed).....	3-10
3.2.4 Configuring the NTP Solution to the Installation Scheme of the High Availability System (Solaris)	3-12
3.2.5 Configuring the NTP Solution to the Installation Scheme of the High Availability System (Windows)	3-13
3.2.6 Configuring the NTP Solution to the Installation Scheme of the High Availability System (SUSE Linux - Distributed).....	3-14
3.3 NTP Configuration Task Set.....	3-16
3.3.1 Configuring the NTP Service by Using the NMS Maintenance Suite.....	3-16
3.3.2 Manually Configuring the NTP Service by Using Commands (Windows).....	3-17
3.3.2.1 Configuring the Windows OS as the NTP Client.....	3-18
3.3.2.2 Starting the NTP Service in the Windows OS.....	3-19
3.3.2.3 Stopping the NTP Service in the Windows OS.....	3-19
3.3.3 Manually Configuring the NTP Service by Using Commands (Solaris).....	3-20
3.3.3.1 Setting the Solaris system as the Top-Level Time Server.....	3-20
3.3.3.2 Setting the Solaris system to the Secondary Time Server.....	3-21
3.3.3.3 Setting the Solaris system to the NTP Client.....	3-21
3.3.3.4 Starting the NTP Service on the Solaris system.....	3-22
3.3.3.5 Checking the Conditions of the NTP Service in the Solaris OS.....	3-23
3.3.3.6 Stopping the NTP Service in the Solaris OS.....	3-24

3.3.4 Manually Configuring the NTP Service by Using Commands (SUSE Linux).....	3-25
3.3.4.1 Setting the SUSE Linux system as the Top-Level Time Server.....	3-25
3.3.4.2 Setting the SUSE Linux system to the Secondary Time Server.....	3-26
3.3.4.3 Setting the SUSE Linux to the NTP Client.....	3-26
3.3.4.4 Starting the NTP Service on the SUSE Linux.....	3-27
3.3.4.5 Checking the Conditions of the NTP Service in the SUSE Linux OS.....	3-27
3.3.4.6 Stopping the NTP Service in the SUSE Linux OS.....	3-28
4 Configuring NMS System Security.....	4-1
4.1 Configuring System Security Policies.....	4-2
4.2 U2000 Application Security.....	4-2
4.2.1 OS User Security.....	4-3
4.2.2 Database User Security.....	4-5
4.2.3 Security of the Database System Files.....	4-6
4.2.4 User Security Policy.....	4-6
4.2.5 Log Management Policy.....	4-9
4.2.6 Security of the System Data	4-10
4.2.7 NE Security Management.....	4-10
4.3 Configuring Communications Security.....	4-11
4.3.1 Communication Security.....	4-12
4.3.1.1 Southbound Communication Security.....	4-12
4.3.1.2 Northbound Communication Security.....	4-13
4.3.1.3 Communication Security Among Distributed Nodes.....	4-15
4.3.1.4 Client Communication Security.....	4-15
4.3.2 Enabling a Device to Communicate with the Server through the SSH Protocol.....	4-15
4.3.3 Setting the Communications Between the Server and the Client Through the SSL Protocol.....	4-17
4.4 Setting Security Policies of U2000 Users.....	4-18
4.4.1 Changing the admin User Password.....	4-19
4.4.2 Setting the U2000 Login Mode.....	4-19
4.4.3 Setting the Access Control List.....	4-20
4.4.4 Setting the Password Policy.....	4-22
4.4.5 Setting the Account Policy.....	4-23
5 Commissioning the Communication Between the Server and an Independent Client	5-1
6 Commissioning the Communication Between the NMS and NEs.....	6-1
6.1 Pre-configuration Requirements on the NE Side.....	6-3
6.2 Setting the Parameters for the Communication Between the U2000 and NEs.....	6-3
6.2.1 Protocols for Communications Between the U2000 and NEs.....	6-4
6.2.2 Setting SNMPv1/v2c Parameters on NEs.....	6-5
6.2.3 Setting SNMPv3 Parameters on NEs.....	6-6
6.2.4 Configuring the Default SNMP Parameters Template.....	6-8
6.3 Creating a Topology Subnet.....	6-9

6.4 Creating a Single NE.....	6-9
6.4.1 Creating a Single Transport NE.....	6-10
6.4.2 Creating a Single PTN NE.....	6-12
6.4.3 Creating a Single Router NE.....	6-14
6.4.4 Creating a Single Switch NE.....	6-15
6.4.5 Creating a Single Security Gateway NE.....	6-16
6.4.6 Creating a Single Access NE.....	6-17
6.5 Creating Optical NEs.....	6-18
6.6 Creating NEs In Batches.....	6-19
6.6.1 Creating Transport/PTN NEs in Batches.....	6-19
6.6.2 Creating SNMP/ICMP NEs in Batches.....	6-21
6.7 Viewing an NE in the Topology View.....	6-24
7 Commissioning the Communication Between the NMS and the OSS.....	7-1
7.1 Commissioning a CORBA NBI.....	7-2
7.2 Commissioning an XML NBI.....	7-3
7.3 Commissioning an SNMP NBI.....	7-5
7.4 Commissioning an TL1 NBI.....	7-6
7.5 Commissioning an FTP Performance NBI.....	7-7
8 Commissioning the Alarm Function.....	8-1
8.1 Alarm Reporting Process.....	8-2
8.2 Setting Trap Parameters on the NE.....	8-5
8.3 Setting Automatic Alarm Reporting.....	8-6
8.3.1 Setting Automatic Reporting Status for Alarms of an NE.....	8-6
8.3.2 Setting Automatic Reporting Status for Alarms of a Board.....	8-7
8.4 Monitoring Alarms.....	8-8
8.4.1 Monitoring Alarms Through the Topology View.....	8-8
8.4.2 Monitoring Alarms Through the Alarm Panel.....	8-9
8.4.3 Browsing the Current Alarm.....	8-10
A FAQs.....	A-1
A.1 Windows OS.....	A-2
A.1.1 How to Add a Static Route.....	A-2
A.1.2 How to Change the Password of the OS Administrator?.....	A-3
A.1.3 How to Configure the FTP Server in the Windows OS.....	A-3
A.1.4 How to Verify That the Video Driver Is Correctly Installed.....	A-6
A.1.5 How to Configure the Remote Login to the Windows OS.....	A-7
A.1.6 How to Forcibly End a Process.....	A-7
A.1.7 How to Configure the FTP, SFTP, or TFTP Service on Windows OS.....	A-7
A.1.8 How to Set the Virtual Memory to the System Managed Size.....	A-9
A.2 SUSE Linux OS.....	A-9
A.2.1 How to Start/Stop the FTP, TFTP, SFTP, and Telnet Services.....	A-9
A.2.2 How to Enable and Disable the FTP/Telnet Authority of the root User in the SUSE Linux OS?.....	A-11

A.2.3 How to Check the Remaining Space of a Disk.....	A-12
A.2.4 How to Monitor System Processes and Application Ports?.....	A-12
A.2.5 How to Log In to the OS Through the Remote Login Tools?.....	A-12
A.2.6 How to Query the Process Status.....	A-13
A.2.7 How to Forcibly End a Process.....	A-13
A.2.8 How to Use the vi Editor.....	A-13
A.2.9 How to Change the Time and Time Zone of the SUSE Linux OS?.....	A-15
A.3 Solaris OS.....	A-17
A.3.1 Network Configurations of the Workstation.....	A-17
A.3.1.1 How to Make the Devices Directly Connected to the two NICs of the Server Communicate with Each Other.....	A-17
A.3.1.2 How to Add the Default Route.....	A-18
A.3.1.3 How to Add a Static Route.....	A-18
A.3.1.4 How to Query the Gateway of a Sun Workstation.....	A-19
A.3.1.5 How to Configure the DNS on Solaris OS.....	A-20
A.3.1.6 How to Check the NIC Type of a Server.....	A-20
A.3.2 System Settings of the Workstation.....	A-20
A.3.2.1 How to Boot Up the Workstation from the CD-ROM Drive.....	A-21
A.3.2.2 How to Enable Input Modes on Solaris OS.....	A-21
A.3.2.3 How to Set the Interface Language of Solaris OS.....	A-21
A.3.2.4 How to Call the GUI Management Tool in Solaris 10 OS.....	A-22
A.3.2.5 How to Start the Snapshot Tool When It Is Unavailable.....	A-22
A.3.2.6 How to Switch to the Multi-user Mode or Single-user Mode.....	A-22
A.3.2.7 How to Open the Terminal Window on the Desktop in the JDS.....	A-23
A.3.2.8 How to Operate the CD-ROM.....	A-23
A.3.3 FTP and Telnet Service Configuration.....	A-24
A.3.3.1 How to Start/Stop the FTP, TFTP, SFTP, and Telnet Services.....	A-24
A.3.3.2 How to Enable and Disable the FTP/Telnet Authority of user root on Solaris OS.....	A-26
A.3.3.3 How to Transfer Files by Means of FTP.....	A-27
A.3.4 Usage and Maintenance of Workstation.....	A-27
A.3.4.1 How to View the Versions and Release Date of the Solaris OS.....	A-28
A.3.4.2 How to View Hardware Configurations for the Sun Workstation.....	A-28
A.3.4.3 How to Check Whether the Hard Disk of the Sun Workstation Is Damaged.....	A-31
A.3.4.4 How to Check the Partition of Solaris OS.....	A-31
A.3.4.5 How to Check the Remaining Space of a Disk.....	A-33
A.3.4.6 How to Decompress Files.....	A-33
A.3.4.7 How to Remotely Log In to the System as User root.....	A-34
A.3.4.8 How to Access the OS from the Controller.....	A-34
A.3.4.9 How to Switch Between the Console, OK Prompt, and # Prompt.....	A-35
A.3.4.10 How to Use the vi Editor.....	A-40
A.3.4.11 How to Use the Text Editor.....	A-42
A.3.4.12 How to Query the Process Status.....	A-42
A.3.4.13 How to Forcibly End a Process.....	A-43

A.3.4.14 How to Deploy a Solaris Single-Server System If Data Is Stored on Some Hard Disks.....	A-43
A.4 Veritas HA System.....	A-44
A.4.1 License Management.....	A-44
A.4.1.1 How to Check the Veritas License.....	A-44
A.4.1.2 How to Update the Veritas License (Windows).....	A-48
A.4.2 Disk Maintenance.....	A-48
A.4.2.1 How to Query the Disk Status.....	A-49
A.4.2.2 How to Query the Status of the Disk Group.....	A-49
A.4.2.3 How to Query the Status of the Disk Volume (Solaris & SUSE Linux).....	A-50
A.4.3 System Settings.....	A-51
A.4.3.1 What Are the Reasons for Automatic Switching.....	A-52
A.4.3.2 How to Log in and Exit the VCS (Veritas Cluster Server).....	A-52
A.4.3.3 How to Query the RVG Status (Solaris & SUSE Linux).....	A-54
A.4.3.4 How to Query the RVG Status (Windows).....	A-55
A.4.3.5 How to Query the Rlink Status (Solaris & SUSE Linux).....	A-57
A.4.3.6 How to Query the Rlink Status (Windows).....	A-59
A.4.3.7 How to Query the VVR Status (Solaris & SUSE Linux).....	A-61
A.4.3.8 How to Query the VVR Status (Windows).....	A-62
A.4.3.9 How to Manually Start the VCS Service (Solaris & SUSE Linux).....	A-63
A.4.3.10 How to Manually Start the VCS Service (Windows).....	A-63
A.4.3.11 How to Manually Start the VVR (Solaris & SUSE Linux).....	A-63
A.4.3.12 How to Manually Stop the VCS Service (Solaris & SUSE Linux).....	A-64
A.4.3.13 How to Manually Stop the VCS Service (Windows).....	A-64
A.4.3.14 How to Solve the Problem That the VMDg Node Icon Becomes Grayed out After the High Availability System Is Established (Windows HA System).....	A-64
A.4.3.15 How to Solve the Problem Where the Communications between the Primary Site and the Secondary Site Are Interrupted After the HA System Is Set Up.....	A-65
A.4.3.16 How to Rectify the Fault that Certain Menu Items on the VCS Client Are Dimmed.....	A-66
A.4.3.17 How to Start/Stop the NMS Before Synchronizing the Primary and Secondary Sites.....	A-66
A.4.3.18 How to Ensure Proper Connection of VVR Ports on Primary and Secondary Sites.....	A-69
A.4.3.19 How to Ensure Proper File Transfer Between Primary and Secondary Sites.....	A-69
A.5 SQL Server Database.....	A-70
A.5.1 How to Change the sa Password of the SQL Server.....	A-70
A.5.2 How to Expand the master Database.....	A-71
A.5.3 How to Shut Down the SQL Server Database.....	A-71
A.5.4 How to Start the SQL Server Database.....	A-73
A.5.5 How to Solve the Problem That the Password of User sa Is Forgotten.....	A-74
A.5.6 How to Check Whether the SQL Server Database Can Be Sorted in Binary Mode.....	A-74
A.5.7 How to Change the Database Sorting Mode to Binary.....	A-74
A.5.8 How to Check the Name of the SQL Server Database.....	A-75
A.6 Sybase Database.....	A-75
A.6.1 Startup and Shutdown of the Sybase Database.....	A-75
A.6.1.1 How to Disable the Sybase Database Service.....	A-76

A.6.1.2 How to Start the Sybase Database Service.....	A-77
A.6.1.3 How to Verify That the Sybase Process Is Running.....	A-78
A.6.2 Sybase Database Maintenance.....	A-78
A.6.2.1 How to Verify That the Sybase Database Has Been Installed.....	A-79
A.6.2.2 How to Check the Sybase Database Version.....	A-80
A.6.2.3 How to View the Server Name of the Sybase Database.....	A-80
A.6.2.4 How to Change the Password of User sa for the Sybase Database.....	A-81
A.6.2.5 How to Clear the Password of the Sybase Database.....	A-82
A.6.2.6 How to View the Bit Number of the Sybase Database.....	A-83
A.6.2.7 How to View the Details of the Sybase Database.....	A-83
A.6.2.8 How to View Data Tables.....	A-84
A.6.2.9 How to Query a Database Table if Only Part of the Table Name Is Remembered.....	A-84
A.6.2.10 How to Identify Database Errors Caused by Unexpected Powering-Off of the Workstation.....	A-85
A.6.2.11 How to Expand Space for the master Database.....	A-87
A.6.2.12 How to Set Up More User Connections to a Database.....	A-87
A.6.2.13 How to Check for Database Errors Using the dbcc Tool.....	A-88
A.6.2.14 How to Set the Network Transport Parameters of Databases.....	A-89
A.6.2.15 How to Delete a Suspect Database.....	A-92
A.6.2.16 How to Delete a Damaged User Database.....	A-93
A.6.2.17 How to Delete a Database from the Sybase Database?.....	A-94
A.6.2.18 How to View the Deadlock Information in the Database.....	A-95
A.7 Oracle Database.....	A-96
A.7.1 How to Check Whether the Oracle Database Has Been Installed.....	A-97
A.7.2 How to Check the Version of the Oracle Database.....	A-97
A.7.3 How to Check the Name of the Oracle Database.....	A-97
A.7.4 How to Start the Oracle Database in the High Availability System.....	A-98
A.7.5 How Can I Start the Oracle Database (Single-Server System)?.....	A-99
A.7.6 How to Shut Down the Oracle Database (High Availability System).....	A-100
A.7.7 How Can I Stop the Oracle Database (Single-Server System)?.....	A-101
A.7.8 How Can I Check Whether the Oracle Database Is Started?.....	A-102
A.7.9 How Can I Change the Password of an Oracle Database User?.....	A-102
A.7.10 How Can I Check Whether the Oracle Listener Is Started?.....	A-103
A.8 MSuite.....	A-103
A.8.1 How to Verify That The Process of the MSuite Server Is Started.....	A-104
A.8.2 How to Start the Process of the MSuite Server.....	A-104
A.8.3 How to End Processes on the MSuite Server.....	A-104
A.8.4 How to Start the MSuite Client.....	A-105
A.9 U2000 System.....	A-105
A.9.1 How to Verify That the U2000 Is Installed.....	A-108
A.9.2 How to Change the System Time and Time Zone of the Single-Server System on Windows.....	A-108
A.9.3 How to Change the System Time and Time Zone of the Single-Server System (Solaris).....	A-109
A.9.4 How to Change the System Time and Time Zone of the Single-Server System (SUSE Linux-Distributed)	A-110

A.9.5 How to Change the System Time and Time Zone of the High Availability System on Windows.	A-111
A.9.6 How to Change the System Time and Time Zone of the High Availability System (Solaris).....	A-112
A.9.7 How to Change the System Time and Time Zone of the High Availability System (SUSE Linux-Distributed).....	A-113
A.9.8 How to Change the IP Address of the Single-Server System on Windows.....	A-114
A.9.9 How to Change the Host Name of the Single-Server System on Windows.....	A-116
A.9.10 How to Change the IP Address and Host Name for the Single-Server System (Solaris).....	A-117
A.9.11 How to Change the IP Address and Host Name of the Single-Server System (SUSE Linux-Distributed).....	A-119
A.9.12 How to Modify the Server IP Address of High Availability System (Windows).....	A-121
A.9.13 How to Change the Host Name of the High Availability System (Windows).....	A-125
A.9.14 How to Change the IP Address and Host name for the High Availability System (Solaris).....	A-127
A.9.15 How to Change the IP Address and Host Name of the High Availability System (SUSE Linux-Distributed).....	A-133
A.9.16 How to Verify That the Processes of the U2000 Single-Server System Are Running on Windows.....	A-139
A.9.17 How to Start the Processes of the U2000 Single-Server System on Windows.....	A-139
A.9.18 How to End the Processes of the U2000 Single-Server System on Windows.....	A-140
A.9.19 How to Verify That the Processes of the U2000 Single-Server System Are Running on Solaris.	A-140
A.9.20 How to Start the Processes of the U2000 Single-Server System on Solaris.....	A-141
A.9.21 How to End the Processes of the U2000 Single-Server System on Solaris.....	A-142
A.9.22 How to Verify That the Processes of the U2000 Single-Server System (SUSE Linux-Distributed) Are Running.....	A-142
A.9.23 How to Start the Processes of the U2000 Single-Server System (SUSE Linux-Distributed).....	A-143
A.9.24 How to End the Processes of the U2000 Single-Server System (SUSE Linux-Distributed).....	A-143
A.9.25 How to Check Whether the U2000 Processes of the High Availability System (Windows) Are Started.....	A-144
A.9.26 How to Start the U2000 Processes of the High Availability System (Windows).....	A-145
A.9.27 How to End the U2000 Processes of the High Availability System (Windows).....	A-146
A.9.28 How to Check Whether the U2000 Processes of the High Availability System (Solaris) Are Started.....	A-147
A.9.29 How to Start the U2000 Processes of the High Availability System (Solaris).....	A-148
A.9.30 How to End the U2000 Processes of the High Availability System (Solaris).....	A-149
A.9.31 How to Check Whether the U2000 Processes of the High Availability System (SUSE Linux-Distributed) Are Started.....	A-150
A.9.32 How to Start the U2000 Processes of the High Availability System (SUSE Linux-Distributed). .	A-151
A.9.33 How to End the U2000 Processes of the High Availability System (SUSE Linux-Distributed). .	A-152
A.9.34 What Factors Affect the Response Speed of the NMS.....	A-153
A.9.35 How to Resolve the Problem Wherein Illegible Characters Occur in the NMS Window.....	A-153
A.9.36 How to Configure the ipmap.cfg Mapping File.....	A-154
A.9.37 How to Determine Which Types of Software Are Preinstalled.....	A-155
A.9.38 How to Check Whether the daem Process Is Started.....	A-155
A.9.39 How to Start the daem Process.....	A-156
A.9.40 How to End the daem Process.....	A-156

A.9.41 How to Rectify the Application GUI Startup Failure Caused by User Switching.....	A-157
A.9.42 How to Rectify the U2000 Startup Failure After the IP Address or Host Name of the Single-Server System (Solaris) Is Changed Manually.....	A-157
A.9.43 How to Rectify the U2000 Startup Failure Because the IP Address or Host Name of the Single-Server System (SUSE Linux-Distributed) Is Changed Manually.....	A-158
A.9.44 How to View the U2000 and Sybase Database Installation Paths.....	A-161
A.9.45 How to View Network Configurations for the Primary Site or Secondary Site Installed with a HA System	A-162
A.9.46 How to Rectify the Mouse Detection Failure and Open the GUI After the T5220 Is Connected to the KVM.....	A-164
A.9.47 How to Check Downloaded Software Packages by Using MD5 Software.....	A-165
A.9.48 How to Rectify the Failure to Connect to the Sybase Database During U2000 Installation.....	A-166
A.9.49 Reinstalling the U2000 on or Migrating the U2000 to Another Computer.....	A-167
A.9.50 How to Set the Communication Mode on the U2000 server for the Single-Server System (Windows)	A-167
A.9.51 How to Set the Communication Mode on the U2000 server for the Single-Server System (Solaris)	A-168
A.9.52 How to Configure the Communication Mode for a Linux-based U2000 Server?.....	A-169
A.9.53 How to Set the Communication Mode on the U2000 Server for the High Availability System (Windows)	A-170
A.9.54 How to Set the Communication Mode of the Server in a High Availability System (Solaris)?....	A-173
A.9.55 How to Set the Communication Mode of the Server in a High Availability System (SUSE Linux-Distributed).....	A-175
B Configuring Controller IP Addresses for Workstation.....	B-1
B.1 Configuring the IP Address for a System Controller on a T5220 Server.....	B-2
B.2 Configuring the IP Address for a System Controller on an M4000 Server.....	B-4
C Configuring the Management Console.....	C-1
C.1 Configuring the Remote Management Console of an ATAE Blade Server.....	C-2
C.2 Configuring the Remote Management Console of an IBM Blade Server.....	C-3
D MSuite.....	D-1
D.1 Overview.....	D-2
D.1.1 Basic Concepts.....	D-2
D.1.2 System Architecture of the MSuite.....	D-4
D.1.3 Function Overview.....	D-5
D.1.4 Graphical User Interface.....	D-8
D.1.5 Command Line Interface.....	D-10
D.2 Starting and Stopping the MSuite.....	D-11
D.2.1 Starting the Process of the MSuite Server.....	D-12
D.2.2 Logging In to the MSuite Client.....	D-12
D.2.3 Exiting from the MSuite client.....	D-13
D.2.4 Ending the Process of the MSuite Server.....	D-14
D.3 System Management.....	D-14
D.3.1 Refreshing the NMS Information.....	D-14

D.3.2 Synchronizing the NMS Information.....	D-15
D.3.3 Synchronizing the NMS Information (High Availability System).....	D-16
D.3.4 Changing the Password of the MSuite.....	D-17
D.3.5 Logging Out of the MSuite Client.....	D-18
D.4 U2000 Deployment.....	D-18
D.4.1 Adding a Component.....	D-19
D.4.2 Deleting a Component.....	D-20
D.4.3 Adding an Instance.....	D-21
D.4.4 Deploying instances by License.....	D-22
D.4.5 Deleting an Instance.....	D-23
D.4.6 Changing the Name and Remarks of an Instance.....	D-24
D.4.7 Setting the System Time and Time Zone.....	D-25
D.4.8 Changing the Password of the Administrator of the Database.....	D-26
D.4.9 Changing the Password of the User of the Database.....	D-27
D.4.10 Configuring the NTP Service.....	D-28
D.5 Adjusting the NMS.....	D-29
D.5.1 Changing the Host Name and IP Address.....	D-29
D.5.1.1 How to Change the IP Address of the Single-Server System on Windows.....	D-31
D.5.1.2 How to Change the Host Name of the Single-Server System on Windows.....	D-33
D.5.1.3 How to Change the IP Address and Host Name for the Single-Server System (Solaris).....	D-34
D.5.1.4 How to Change the IP Address and Host Name of the Single-Server System (SUSE Linux-Distributed).....	D-36
D.5.1.5 How to Modify the Server IP Address of High Availability System (Windows).....	D-38
D.5.1.6 How to Change the Host Name of the High Availability System (Windows).....	D-41
D.5.1.7 How to Change the IP Address and Host name for the High Availability System (Solaris).....	D-44
D.5.1.8 How to Change the IP Address and Host Name of the High Availability System (SUSE Linux-Distributed).....	D-49
D.5.2 Configuring Routes.....	D-55
D.5.3 Synchronizing Network Configurations.....	D-56
D.6 Management of the High Availability System (Veritas hot standby).....	D-57
D.6.1 Establishing the HA Relationship Between the Primary and Secondary Sites.....	D-58
D.6.2 Deleting the HA Relationship Between the Primary and Secondary Sites.....	D-59
D.6.3 Deleting Replication Relations.....	D-60
D.6.4 Configuring the Current Server as the Active Server Forcibly.....	D-61
D.6.5 Performing the Dual-Active Operation.....	D-61
D.7 Maintaining a Distributed System.....	D-62
D.7.1 Adding a Slave Server.....	D-62
D.7.2 Deleting a Slave Server.....	D-63
D.7.3 Migrating an Instance.....	D-64
D.8 Configuring the Northbound Interface Instance.....	D-64
D.9 Managing Databases.....	D-65
D.9.1 Backing Up the System Database.....	D-65
D.9.1.1 Immediately Backing Up the U2000 Database to a Local Server Through the MSuite.....	D-66

D.9.1.2 Immediately Backing Up the U2000 Database to a Remote Server Through the MSuite.....	D-68
D.9.2 Restoring Data of a U2000 Single-Server System (Windows).....	D-70
D.9.2.1 Restoring U2000 Single-Server System (Windows) Data from a Local Server.....	D-70
D.9.2.2 Restoring U2000 Single-Server System (Windows) Data from a Remote Server.....	D-72
D.9.3 Restoring U2000 Single-Server System (Solaris) Data.....	D-74
D.9.3.1 Restoring U2000 Single-Server System (Solaris) Data from a Local Server.....	D-75
D.9.3.2 Restoring U2000 Single-Server System (Solaris) Data from a Remote Server.....	D-77
D.9.4 Restoring U2000 Single-Server System (SUSE Linux-Distributed) Data.....	D-80
D.9.4.1 Restoring U2000 Single-Server System (SUSE Linux-Distributed) Data from a Local Server	D-80
D.9.4.2 Restoring U2000 Single-Server System (SUSE Linux-Distributed) Data from a Remote Server	D-82
D.9.5 Restoring U2000 High Availability System (Windows) Data.....	D-85
D.9.5.1 Restoring U2000 High Availability System (Windows) Data from a Local Server.....	D-85
D.9.5.2 Restoring U2000 High Availability System (Windows) Data from a Remote Server.....	D-87
D.9.6 Restoring U2000 High Availability System (Solaris) Data.....	D-90
D.9.6.1 Restoring U2000 High Availability System (Solaris) Data from a Local Server.....	D-90
D.9.6.2 Restoring U2000 High Availability System (Solaris) Data from a Remote Server.....	D-93
D.9.7 Restoring U2000 High Availability System (SUSE Linux-Distributed) Data.....	D-96
D.9.7.1 Restoring U2000 High Availability System (SUSE Linux-Distributed) Data from a Local Server	D-96
D.9.7.2 Restoring U2000 High Availability System (SUSE Linux-Distributed) Data from a Remote Server	D-98
D.9.8 Restoring Data of a U2000 High Availability System (Cross-U2000).....	D-101
D.9.9 Initializing the U2000 Database.....	D-102
E Shutting Down the U2000.....	E-1
E.1 Shutting Down the U2000 Client.....	E-2
E.2 Shutting Down the Single-Server System (Windows).....	E-2
E.3 Shutting Down the Single-Server System (Solaris).....	E-3
E.4 Shutting Down the Single-Server System (SUSE Linux-Distributed).....	E-4
E.5 Shutting Down the High Availability System (Windows).....	E-5
E.6 Shutting Down the High Availability System (Solaris).....	E-6
E.7 Shutting Down the High Availability System (SUSE Linux-Distributed).....	E-8
F U2000 Port List.....	F-1
F.1 U2000 Service Port Overview.....	F-2
F.2 Ports Between the U2000 Server and the NEs.....	F-4
F.3 Ports Between the U2000 Server and the Clients.....	F-11
F.4 Ports Between the U2000 Server and the OSS.....	F-19
F.5 Ports on Primary and Secondary Sites of the Veritas HA System.....	F-25
F.6 Ports for Internal Processes of the U2000 Server.....	F-29
F.7 Ports for Remote Maintenance.....	F-37
F.8 Ports for Other Connections.....	F-40

G Abbreviations.....G-1

Figures

Figure 1-1 Commissioning flowchart.....	1-3
Figure 2-1 Networking diagram for a Windows single-server system.....	2-3
Figure 2-2 Hardware connection between the DL380 server.....	2-7
Figure 2-3 Hardware connection between the DL580 server.....	2-8
Figure 2-4 Position of the power button of the DL580G5 server.....	2-9
Figure 2-5 Network diagram for a centralized system.....	2-16
Figure 2-6 Hardware connections between the T5220 server and the OceanStor S2600 disk array.....	2-21
Figure 2-7 Hardware connections between the T5220 server and the OceanStor S3100 disk array.....	2-21
Figure 2-8 Hardware connections between the T5220 server and the StorageTek 2540 disk array.....	2-22
Figure 2-9 Hardware connections between the M4000 server and the OceanStor S2600 disk array.....	2-22
Figure 2-10 Hardware connections between the M4000 server and the OceanStor S3100 disk array.....	2-23
Figure 2-11 Hardware connections between the M4000 server and the StorageTek 2540 disk array.....	2-23
Figure 2-12 Power button of the T5220 server.....	2-24
Figure 2-13 Power button of the M4000 server.....	2-25
Figure 2-14 Networking diagram for a distributed system.....	2-37
Figure 2-15 Cable connection for an IBM blade server.....	2-43
Figure 2-16 Cable connection for an ATAE blade server.....	2-44
Figure 2-17 Diagram of the connection between the ATAE server card and the USB drive.....	2-44
Figure 2-18 Networking structure of the high availability system (Veritas hot standby).....	2-59
Figure 2-19 Hardware connection between the DL380 server.....	2-64
Figure 2-20 Hardware connection between the DL580 server.....	2-64
Figure 2-21 Position of the power button of the DL580G5 server.....	2-65
Figure 2-22 Networking structure of a high availability system (Solaris).....	2-76
Figure 2-23 Networking example (single-NIC scheme).....	2-79
Figure 2-24 Networking example (double-NIC scheme (without IPMP)).....	2-81
Figure 2-25 Networking example (double-NIC scheme (with IPMP)).....	2-84
Figure 2-26 Hardware connection between the T5220 server and the OceanStor S2600.....	2-88
Figure 2-27 Hardware connection between the T5220 server and the OceanStor S3100.....	2-89
Figure 2-28 Hardware connection between the T5220 server and the StorageTek 2540.....	2-89
Figure 2-29 Hardware connection between the M4000 server and the OceanStor S2600.....	2-90
Figure 2-30 Hardware connection between the M4000 server and the OceanStor S3100.....	2-90
Figure 2-31 Hardware connection between the M4000 server and the StorageTek 2540.....	2-91
Figure 2-32 Power button of the T5220 server.....	2-92

Figure 2-33 Power button of the M4000 server.....	2-92
Figure 2-34 Networking structure of the high availability system (SUSE Linux-distributed).....	2-110
Figure 2-35 Connecting the ATAE blade server to the public network through the switching board.....	2-118
Figure 2-36 Connecting the IBM blade server to the public network through the switching board.....	2-118
Figure 2-37 Diagram of the connection between the ATAE blade server and a disk array.....	2-119
Figure 2-38 Diagram of the connection between the IBM blade server and a disk array.....	2-120
Figure 2-39 Diagram of the connection between the ATAE server card and the USB drive.....	2-120
Figure 3-1 NTP synchronization principle.....	3-4
Figure 3-2 NTP hierarchical networking.....	3-5
Figure 3-3 Basic process of configuring NTP.....	3-6
Figure 6-1 Topology for communications between the U2000 and NEs in the IP/access domain.....	6-4
Figure 6-2 Topology for communications between the U2000 and NEs in the transport domain.....	6-5
Figure 8-1 Alarm reporting flow chart 1.....	8-3
Figure 8-2 Alarm reporting flow chart 2.....	8-4
Figure 8-3 Alarm panel.....	8-9
Figure A-1 Starting the FTP, TFTP, and Telnet services.....	A-10
Figure A-2 Selecting the service path.....	A-90
Figure A-3 Selecting the database service.....	A-90
Figure A-4 Selecting available network transport settings.....	A-91
Figure A-5 Modifying the transport type.....	A-91
Figure A-6 High Availability System (Solaris) resources.....	A-128
Figure A-7 High Availability System (Solaris) resources.....	A-131
Figure A-8 High Availability System (SUSE Linux-Distributed) resources.....	A-134
Figure A-9 High Availability System (SUSE Linux-Distributed) resources.....	A-136
Figure B-1 Connections between the T5220 server and the controller.....	B-2
Figure B-2 Connections between the M4000 server and the controller.....	B-5
Figure C-1 Diagram of the connection between the SMM board and the controller.....	C-2
Figure D-1	D-3
Figure D-2 System architecture of the MSuite.....	D-4
Figure D-3 GUI of the MSuite client.....	D-9
Figure D-4 High Availability System (Solaris) resources.....	D-45
Figure D-5 High Availability System (Solaris) resources.....	D-47
Figure D-6 High Availability System (SUSE Linux-Distributed) resources.....	D-50
Figure D-7 High Availability System (SUSE Linux-Distributed) resources.....	D-53
Figure F-1 Relationship between the U2000 server and peripherals.....	F-3

Tables

Table 1-1 Topics for reference for commissioning a U2000.....	1-4
Table 2-1 Installation environment requirements.....	2-4
Table 2-2 Host name list.....	2-4
Table 2-3 System IP address list.....	2-5
Table 2-4 Time zone and time list.....	2-5
Table 2-5 User and password list.....	2-5
Table 2-6 Server disk partition list (146 GB disk).....	2-5
Table 2-7 Server disk partition list (80 GB disk).....	2-6
Table 2-8 Installation path list.....	2-6
Table 2-9 Quantity list of configured components and instances.....	2-6
Table 2-10 Installation environment requirements.....	2-17
Table 2-11 Host name list.....	2-17
Table 2-12 Controller IP address list.....	2-18
Table 2-13 System IP address list.....	2-18
Table 2-14 Route list.....	2-19
Table 2-15 Time zone and time list.....	2-19
Table 2-16 User and password list.....	2-19
Table 2-17 Quantity list of configured components and instances.....	2-20
Table 2-18 Installation path list.....	2-20
Table 2-19 Installation environment requirements.....	2-38
Table 2-20 Host name list.....	2-39
Table 2-21 Controller IP address list.....	2-39
Table 2-22 System IP address list.....	2-40
Table 2-23 Private network segment list.....	2-40
Table 2-24 Route list.....	2-40
Table 2-25 Time zone and time list.....	2-41
Table 2-26 List of users and passwords.....	2-41
Table 2-27 Quantity list of configured components and instances.....	2-42
Table 2-28 Installation environment requirements.....	2-59
Table 2-29 Host name list.....	2-60
Table 2-30 IP address planning of the single-networking-interface scheme.....	2-61
Table 2-31 Time zone and time list.....	2-62
Table 2-32 List of users and passwords	2-62

Table 2-33 Server disk partition list (4*146GB disk).....	2-63
Table 2-34 Installation path list.....	2-63
Table 2-35 Quantity list of configured components and instances.....	2-63
Table 2-36 Installation environment requirements.....	2-77
Table 2-37 Host name list.....	2-78
Table 2-38 Example of IP address planning of the single-NIC scheme.....	2-80
Table 2-39 Example of IP address planning of the double-NIC scheme (without IPMP).....	2-82
Table 2-40 Example of IP address planning of the two-NIC scheme (with IPMP).....	2-85
Table 2-41 Route list.....	2-86
Table 2-42 Time zone and time list.....	2-87
Table 2-43 User and password list.....	2-87
Table 2-44 Quantity list of configured components and instances.....	2-87
Table 2-45 Installation environment requirements.....	2-112
Table 2-46 Host name list.....	2-113
Table 2-47 Controller IP address list.....	2-114
Table 2-48 Planning of system IP addresses of the master and slave server.....	2-115
Table 2-49 Route list.....	2-115
Table 2-50 Time zone and time list.....	2-116
Table 2-51 User and password list.....	2-116
Table 2-52 Quantity list of configured components and instances.....	2-117
Table 2-53 Installation path list.....	2-117
Table 4-1 Solaris OS users related to the U2000 and their rights.....	4-3
Table 4-2 Linux OS users related to the U2000 and their rights.....	4-4
Table 4-3 Windows OS users related to the U2000 and their rights.....	4-5
Table 4-4 Database users and their rights.....	4-5
Table 4-5 Database users and their rights.....	4-5
Table 4-6 Database users and their rights.....	4-6
Table 5-1 Server parameter settings.....	5-2
Table 7-1 Serving ports of the CORBA NBI.....	7-3
Table 7-2 Serving ports of the XML NBI.....	7-4
Table 7-3 Serving ports of the SNMP NBI.....	7-6
Table A-1 Commands for quitting the vi editor.....	A-15
Table A-2 Commands for quitting the vi editor.....	A-42
Table A-3 Fields about the disk volume status.....	A-50
Table A-4 RVG status of the primary site.....	A-54
Table A-5 RVG status of the primary site.....	A-56
Table A-6 Rlink status on the primary site.....	A-57
Table A-7 Rlink status on the primary site.....	A-59
Table A-8 Mapping relationship between U2000 IP addresses and NAT server IP addresses.....	A-154
Table C-1 Parameter settings.....	C-5
Table D-1 Functions of the MSuite.....	D-5
Table D-2 Common CLI commands for the MSuite.....	D-10

Table F-1 Ports on the NEs for connecting the U2000.....F-4

Table F-2 Ports on the U2000server for connecting NEs.....F-7

Table F-3 Ports on the U2000 server for connecting the clients.....F-11

Table F-4 Ports on the U2000 server for connecting the OSS.....F-19

Table F-5 Ports on the OSS for connecting the U2000 server.....F-25

Table F-6 Veritas on primary and secondary sites of the HA system ports.....F-26

Table F-7 Ports for internal processes of the U2000 server.....F-30

Table F-8 Ports for remote maintenance.....F-38

Table F-9 Ports for other connections.....F-40

1 Commissioning Overview

About This Chapter

This topic describes the commissioning scenario, preparations for commissioning, and commissioning process.

[1.1 Commissioning Scenarios](#)

This topic describes the scenarios where a U2000 is commissioned. To enable a U2000 to manage networks, you must commission the U2000 before using it to manage equipment and configure services.

[1.2 Preparing for U2000 Commissioning](#)

This topic describes how to prepare for U2000 commissioning. Before commissioning a U2000, you must make ready the planning for the U2000 system scheme, hardware installation, and software installation.

[1.3 Commissioning Process](#)

This topic describes the commissioning process. Before commissioning a U2000, you must get familiar with the flowchart for commissioning a U2000 and the topics for reference.

1.1 Commissioning Scenarios

This topic describes the scenarios where a U2000 is commissioned. To enable a U2000 to manage networks, you must commission the U2000 before using it to manage equipment and configure services.

The items to be commissioned in a U2000 are as follows:

1. System parameters

If parameter settings for the system do not meet the on-site requirements, you must modify the system parameters. The servers delivered by Huawei have been pre-installed and you must modify parameters for these servers. The parameters to be modified vary according to the deployment scheme.

2. System NTP solution

By configuring the system NTP solution, you must ensure that the time for the U2000 server is consistent with the time for a U2000 client.

3. U2000 security

By configuring U2000 security, you must ensure network and data security to protect networks against illegitimate logins or incorrect operations.

4. Communications between the server and an independent client

By logging in to an independent client, you must ensure that the independent client properly communicates with the server. Log in to a U2000 using the client, and then perform management operations in the GUI of the U2000 client.

5. Communications between a U2000 and NEs

By commissioning the communications between a U2000 and NEs, you must ensure that the U2000 can manage all added NEs. For the details about NE management, see the Help.

6. Communications between a U2000 and OSSs

The U2000 supports NBIs including CORBA NBI, XML NBI, SNMP NBI, TL1 NBI, and FTP performance NBI. By commissioning the communications between a U2000 and OSSs according to the NBI to be used, you must ensure that the NBI function is available for the U2000.

7. Alarm function

As an important information source for learning the equipment running status and locating faults, alarms need to be obtained and managed in an effectively manner. By setting alarm parameters, you must ensure that equipment alarms can be reported to a U2000. In this manner, the U2000 can monitor and manage the live network in real time. For details about alarm management, see the Help. For details about how to commission the alarm box, see the associated documents delivered with the alarm box.

1.2 Preparing for U2000 Commissioning

This topic describes how to prepare for U2000 commissioning. Before commissioning a U2000, you must make ready the planning for the U2000 system scheme, hardware installation, and software installation.

1. For the planning for the U2000 system scheme, see the *iManager U2000 Planning Guide*.

2. For details about hardware installation, see the *iManager U2000 Hardware Installation Guide (N610E)* or *iManager U2000 Hardware Installation Guide (ATAE)* according to the purchased racks and servers.
3. The servers delivered by Huawei have been pre-installed and can be commissioned directly. If a server is purchased from other suppliers, install the server software according to the planned U2000 system deployment scheme. For details about U2000 deployment schemes, see the **Software Installation Guide**.
4. For details about how to install a client, see the *iManager U2000 Client Software Installation Guide*.

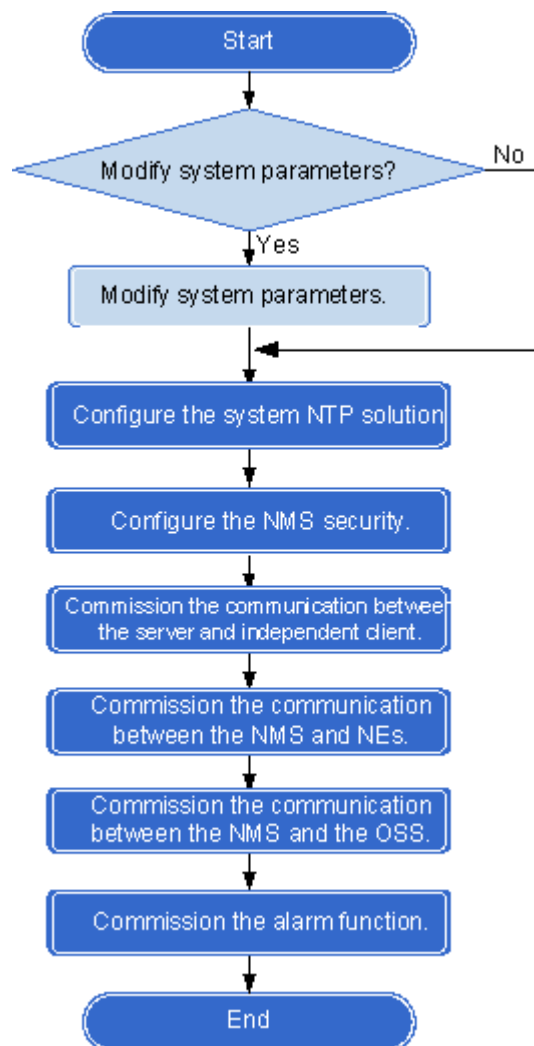
1.3 Commissioning Process

This topic describes the commissioning process. Before commissioning a U2000, you must get familiar with the flowchart for commissioning a U2000 and the topics for reference.

Commissioning Flowchart

The following figure shows the process of commissioning a U2000.

Figure 1-1 Commissioning flowchart



Chapters for Reference

The following table shows the topics for reference for commissioning a U2000.

Table 1-1 Topics for reference for commissioning a U2000

No.	Description	Topics for Reference
1	If parameter settings for the system do not meet the on-site requirements, you must modify the system parameters. The servers delivered by Huawei have been pre-installed and you must modify parameters for these servers. The parameters to be modified vary according to the deployment scheme.	See the associated topics according to the selected deployment scheme. ● 2.1 Modifying Parameters for a Single-Server System (Windows) ● 2.2 Modifying Parameters for a Single-Server System (Solaris) ● 2.3 Modifying Parameters for a Single-Server System (SUSE Linux-Distributed) ● 2.4 Modifying the Parameters of the High Availability System (Windows) ● 2.5 Modifying Parameters for a High Availability System (Solaris) ● 2.6 Modifying the Parameters of the High Availability System (SUSE Linux-Distributed)
2	By configuring the system NTP solution, you must ensure that the time for the U2000 server is consistent with the time for a U2000 client.	3 Configuring System NTP Solutions
3	By configuring U2000 security, you must ensure network and data security to protect networks against illegitimate logins or incorrect operations.	4 Configuring NMS System Security
4	By logging in to an independent client, you must ensure that the independent client properly communicates with the server. Log in to a U2000 using the client, and then perform management operations in the GUI of the U2000 client.	5 Commissioning the Communication Between the Server and an Independent Client
5	By commissioning the communications between a U2000 and NEs, you must ensure that the U2000 can manage all added NEs. For the details about NE management, see the Help.	6 Commissioning the Communication Between the NMS and NEs

No.	Description	Topics for Reference
6	The U2000 supports NBIs including CORBA NBI, XML NBI, SNMP NBI, TL1 NBI, and FTP performance NBI. By commissioning the communications between a U2000 and OSSs according to the NBI to be used, you must ensure that the NBI function is available for the U2000.	7 Commissioning the Communication Between the NMS and the OSS
7	As an important information source for learning the equipment running status and locating faults, alarms need to be obtained and managed in an effectively manner. By setting alarm parameters, you must ensure that equipment alarms can be reported to a U2000. In this manner, the U2000 can monitor and manage the live network in real time. For details about alarm management, see the Help. For details about how to commission the alarm box, see the associated documents delivered with the alarm box.	8 Commissioning the Alarm Function

2 (Optional) Modifying System Parameters

About This Chapter

If parameter settings for the system do not meet the on-site requirements, you must modify the system parameters. The servers delivered by Huawei have been pre-installed and you must modify parameters for these servers. The parameters to be modified vary according to the deployment scheme.

[2.1 Modifying Parameters for a Single-Server System \(Windows\)](#)

This topic describes how to modify parameters for a Windows single-server system, including the host name and IP address, route, time and time zone, subsystem, instance, and user password.

[2.2 Modifying Parameters for a Single-Server System \(Solaris\)](#)

This topic describes how to modify parameters for a centralized system, including the host name and IP address, route, time and time zone, subsystem, instance, and user password.

[2.3 Modifying Parameters for a Single-Server System \(SUSE Linux-Distributed\)](#)

This topic describes how to modify parameters for a distributed system, including the host name and IP address, route, time and time zone, subsystem, instance, and user password.

[2.4 Modifying the Parameters of the High Availability System \(Windows\)](#)

This topic describes how to modify the parameters of the High Availability System (Windows), including the host name and IP address, route, time and time zone, subsystem, instance, and user password.

[2.5 Modifying Parameters for a High Availability System \(Solaris\)](#)

This topic describes how to modify parameters for a centralized system, including the host name and IP address, route, time and time zone, subsystem, instance, and user password.

[2.6 Modifying the Parameters of the High Availability System \(SUSE Linux-Distributed\)](#)

This topic describes how to modify the parameters of the high availability system (SUSE Linux-distributed), including the host name and IP address, route, time and time zone, subsystem, instance, and user password.

2.1 Modifying Parameters for a Single-Server System (Windows)

This topic describes how to modify parameters for a Windows single-server system, including the host name and IP address, route, time and time zone, subsystem, instance, and user password.

2.1.1 Preparing for System Parameter Modification

This topic describes how to prepare for system parameter modification. Before modifying system parameters, you must get familiar with the networking structure and environment requirements, collect planning information, check hardware connections, power on a server, apply for a U2000 license, and check system installation.

2.1.2 Modifying System Parameters

This topic describes how to modify the host names, IP addresses, time, time zone and DST, components, instances, and user passwords for the OS and database according to the collected planning information.

2.1.3 Loading a U2000 License

This topic describes how to load a U2000 license. This topic describes how to install a U2000 license. Before using a U2000, you must load a U2000 license.

2.1.4 Starting a Single-Server System (Windows)

This topic describes how to start a Windows single-server system. After the U2000 server is started, you must start the U2000. Then, log in to the U2000 to manage networks.

2.1.1 Preparing for System Parameter Modification

This topic describes how to prepare for system parameter modification. Before modifying system parameters, you must get familiar with the networking structure and environment requirements, collect planning information, check hardware connections, power on a server, apply for a U2000 license, and check system installation.

2.1.1.1 Networking Structure

This topic describes the networking structure for a single-server system. Before commissioning a Windows single-server system, you must get familiar with the networking structure for the single-server system.

2.1.1.2 Environment Requirements

This topic describes the environment conditions, such as the telecommunications room environment, cable condition, and networking condition of the telecommunications room, that you must get familiar with before you commission a U2000.

2.1.1.3 Collecting Planning Information

This topic describes how to collect planning information. Before commissioning, collect required information, including the host name, IP address, time zone and time, user password, components and instance number, and installation path.

2.1.1.4 Checking Hardware Connections

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

2.1.1.5 Powering On a Server

This topic describes how to power on a server.

2.1.1.6 Applying for a U2000 License

This topic describes how to apply for a U2000 license.

2.1.1.7 Checking System Installation

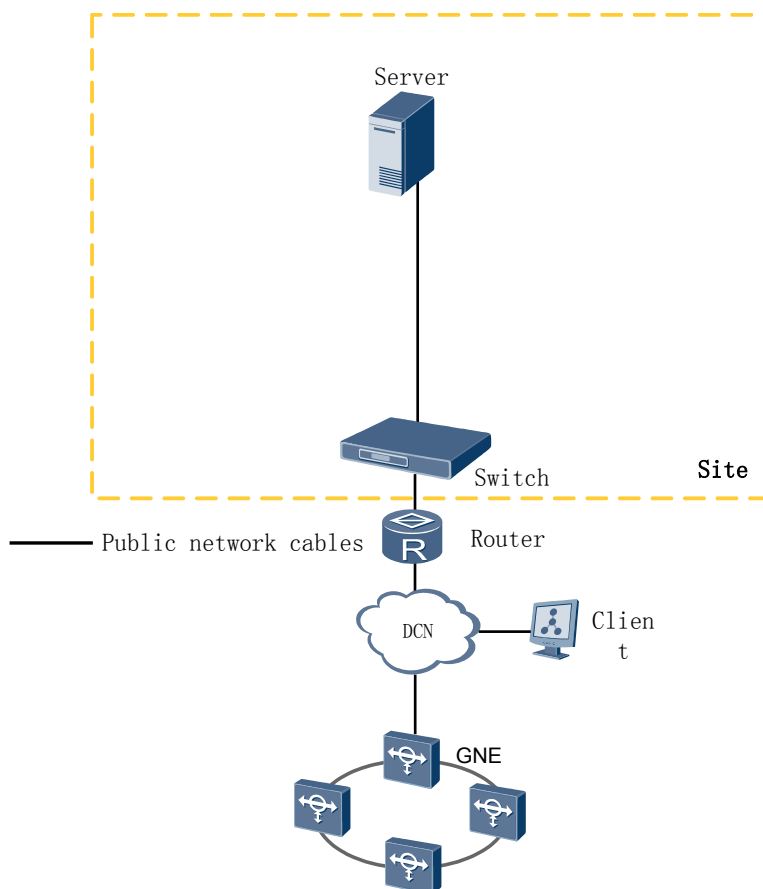
This topic describes how to check installation of a U2000. Before modifying system parameters, you must ensure that the U2000 has been installed and its version is correct.

2.1.1.1 Networking Structure

This topic describes the networking structure for a single-server system. Before commissioning a Windows single-server system, you must get familiar with the networking structure for the single-server system.

The following figure shows the networking structure for a Windows single-server system.

Figure 2-1 Networking diagram for a Windows single-server system



The U2000 client and U2000 MSuite communicate with the server using a data communication network (DCN).

NEs and the upper-layer NMS (OSS) communicate with the server using a DCN.

2.1.1.2 Environment Requirements

This topic describes the environment conditions, such as the telecommunications room environment, cable condition, and networking condition of the telecommunications room, that you must get familiar with before you commission a U2000.

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

Table 2-1 Installation environment requirements

Check Item	Requirement
Temperature	The required temperature range is from 15°C to 30°C in long-term working conditions and from 0°C to 45°C in short-term working conditions.
Humidity	The required humidity range is 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 is larger than 5 µm is less than or equal to 3×104/m3.
Floor	The floor is anti-static movable and must be grounded.
Space	The telecommunication room must have good ventilation and enough space for operation and maintenance.
Power supply	The power supply should 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 is normal and can be accessed successfully.
Network	The routers connecting each server are 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 are connected, including routers and the DCNs.

2.1.1.3 Collecting Planning Information

This topic describes how to collect planning information. Before commissioning, collect required information, including the host name, IP address, time zone and time, user password, components and instance number, and installation path.

Complete planning for the information listed in the following tables according to the *iManager U2000 Planning Guide*. Collect and record the planning 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 2-2 Host name list

Item	Example	Plan
Server	NMSServer	

Table 2-3 System IP address list

Item	Example	Plan
System IP address	129.9.1.1/255.255.255.0/129.9.1.254	

 NOTE

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

Table 2-4 Time zone and time list

Item	Example	Plan
Time zone	GMT+08:00	
Time	14:00	

Table 2-5 User and password list

User	Example	Plan
OS super user administrator	admin123	
Database super user sa	changeme	
Database user NMSuser	NMSuser	
U2000 user admin	admin123	
network management system maintenance suite user admin	admin	

Table 2-6 Server disk partition list (146 GB disk)

Partition	Size (GB)	Description
Disk C	40	It is used to install the OS and database software.
Disk D	100	It is used to install the U2000 software and store the database data.
Disk E	Size of the remaining space	It is used to store the backup data for the U2000.

Table 2-7 Server disk partition list (80 GB disk)

Partition	Size (GB)	Description
Disk C	80	It is used to install the OS, database and U2000 software.

 NOTE

You must specify the principles and scheme for disk partitioning before installing the U2000 server. For details about how to set the Windows virtual memory to the system managed size, see [A.1.8 How to Set the Virtual Memory to the System Managed Size](#).

The basic principles for disk partitioning are as follows:

- Disk C, as the system disk, is used to install the OS and database software.
- Disk D is used to install the U2000 software and store the database data.
- The remaining space is allocated for free use. It can be used for NMS data backup.

Table 2-8 Installation path list

Software	Installation Path
Windows OS	C:\
SQL Server database software	C:\MSSQL2000
U2000 software	D:\U2000

 NOTE

An installation path name consists of the installation package path name and U2000 installation path name. It can contain only the letter, digit, and underscore (_). It cannot contain the space or brackets; otherwise, the installation fails.

Table 2-9 Quantity list of configured components and instances

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

2.1.1.4 Checking Hardware Connections

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

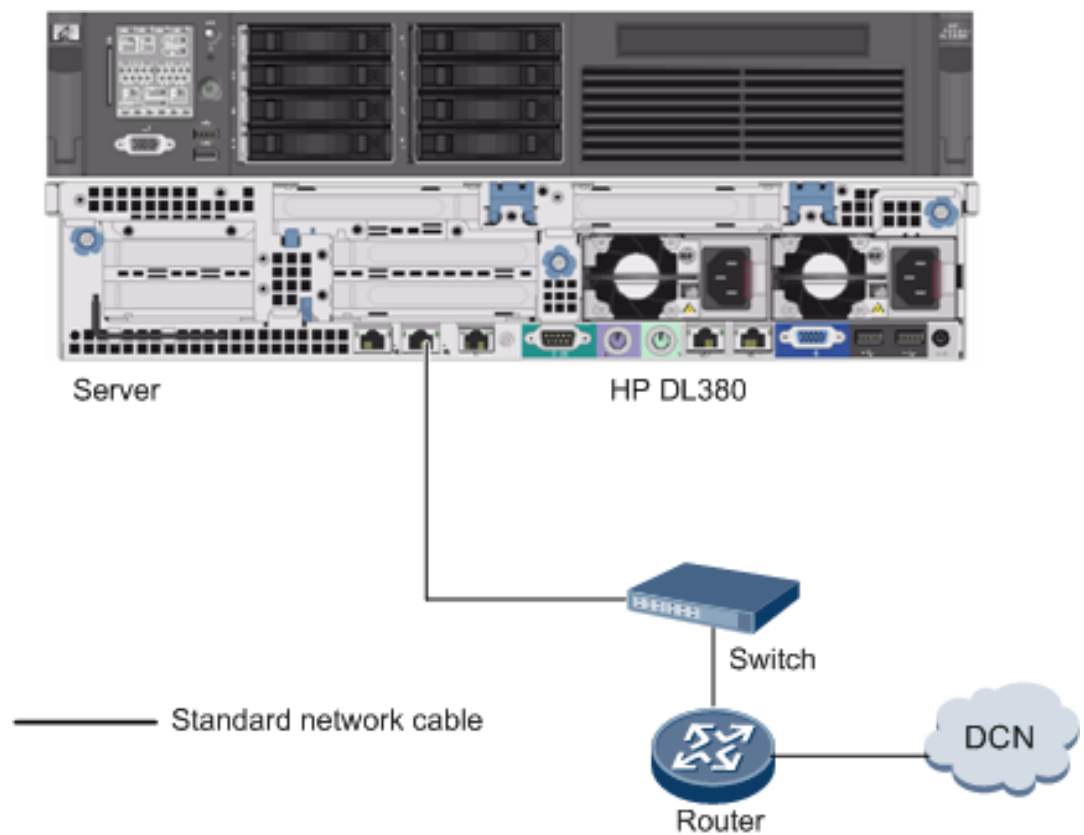
Prerequisite

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

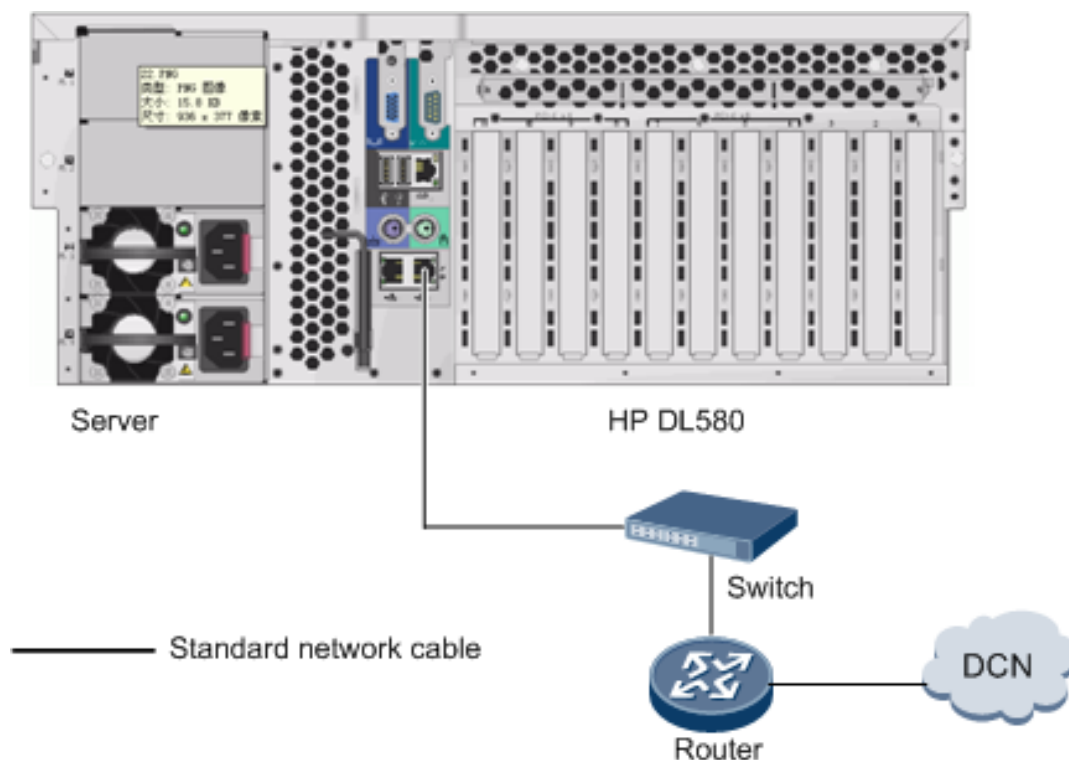
Procedure

- 1 Ensure that the power cables and ground wires for all components are tightly connected and in good contact and that the polarities are properly placed.
- 2 Ensure that all cables are bundled and free of visible damage.
- 3 Check hardware connections and network cables according to the hardware connection diagram.
 - The following figures show hardware connections for the DL380 server.

Figure 2-2 Hardware connection between the DL380 server



- The following figures show hardware connections for the DL580 server.

Figure 2-3 Hardware connection between the DL580 server**4** Check the plugs and sockets.

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

5 Ensure that all debris (cable straps, stubs, or moisture-absorbent packets) are picked up.**6** Remove unnecessary items from the telecommunications room. The workbench must be neat and the movable floor must be level and clean.

----End

2.1.1.5 Powering On a Server

This topic describes how to power on a server.

1. Press the power buttons of the peripherals connected to a server and the monitor to power on the peripherals and monitor.
2. Press the power button on the chassis of the server to power on the server. Take the HP DL580G5 server as an example. In the following figure, the power button is marked in a red frame.

Figure 2-4 Position of the power button of the DL580G5 server



2.1.1.6 Applying for a U2000 License

This topic describes how to apply for a U2000 license.

Context

- The license file is not delivered to customers along with a U2000 installation DVD. Contact Huawei engineers to apply for a license according to the contract number and the equipment serial number (ESN) of the U2000 server.
- 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.

- A license needs to be bound to an ESN of the server.

Procedure

- 1 Obtain the contract number.
- 2 Before installing a U2000, obtain the ESN tool from <http://support.huawei.com> to generate ESNs. The ESN tool is named U2000version_ESN_win32_x86.zip.

Decompress the ESN tool package, and then double-click the **esn.exe** file to view ESNs.

A message similar to the following will be displayed:

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

- 3 Send the contract number and the ESNs of the server to Huawei engineers or a Huawei local office.

NOTE

Huawei engineers access the <http://license.huawei.com> Web site according to the information you provide to apply for a license file. For details about how to apply for a license file, see the *iManager U2000 V100R002C01 License Instructions* archived at <http://support.huawei.com>.

- 4 Huawei engineers send the license file to you after obtaining it.

The license file delivered along with the U2000 is in .dat format.

----End

2.1.1.7 Checking System Installation

This topic describes how to check installation of a U2000. Before modifying system parameters, you must ensure that the U2000 has been installed and its version is correct.

Procedure

- 1 Log in to the OS as a user with **administrator** rights. The system automatically starts the database and U2000 service.

Check whether the shortcut icons for the U2000 client, U2000 System Monitor, and U2000 network management system maintenance suite are available on the desktop. If the shortcut icons are available, the U2000 has been installed; otherwise, install the U2000 according to the *iManager U2000 Single-Server Software Installation Guide (Windows)*.

- 2 Start the U2000 System Monitor client.
 1. Choose **Start > Programs > Network Management System > U2000 System Monitor** or double-click the associated shortcut icon on the desktop to start the System Monitor.
 2. In the **Login** dialog box, enter a user name and password to access the System Monitor window. The user name is **admin** and the initial password is blank by default. When you log in to the System Monitor for the first time, you must change the initial password.
 3. Choose **Help > About** from the main menu. The **About** dialog box is displayed. Check the U2000 version.

NOTE

If the version information does not meet the actual requirement, uninstall the U2000 and then obtain the correct software version to reinstall the U2000. For details, see the *iManager U2000 Single-Server Software Installation Guide (Windows)*.

----End

2.1.2 Modifying System Parameters

This topic describes how to modify the host names, IP addresses, time, time zone and DST, components, instances, and user passwords for the OS and database according to the collected planning information.

Modify the associated parameters according to the difference between the planning information and system parameters.

Parameter	Operation Method
Host name and IP address (Including route)	● For details about how to modify a host name, see A.9.9 How to Change the Host Name of the Single-Server System on Windows. ● For details about how to modify an IP address, see A.9.8 How to Change the IP Address of the Single-Server System on Windows.

Parameter	Operation Method
Time and time zone	● Modifying the time 1. Access the Control Panel window. Then, double-click the Date and Time icon. 2. In the dialog box that is displayed, click the Date and Time tab to set the current system date and time. Then, click OK. ● Modifying the time zone and DST 1. Access the Control Panel window. Then, double-click the Date and Time icon. 2. In the dialog box that is displayed, click the Time Zone tab. Select a time zone where the server resides from the drop-down list. 3. If you require the server to automatically adjust the time according to the DST, click the Internet Time tab, and then select the Automatically synchronize with an Internet time server check box. 4. Click OK.
Component and instance	● To add a component, see D.4.1 Adding a Component. ● To delete a component, see D.4.2 Deleting a Component. ● To add a instance, see D.4.3 Adding an Instance. ● To delete a instance, see D.4.5 Deleting an Instance. ● To modify an instance name or a piece of remarks, see D.4.6 Changing the Name and Remarks of an Instance.
Password for the database supper user	D.4.8 Changing the Password of the Administrator of the Database
Password for the database user NMSuser	D.4.9 Changing the Password of the User of the Database
Password for the MSuite	D.3.4 Changing the Password of the MSuite
Password for the super user administrator of the OS	A.1.2 How to Change the Password of the OS Administrator?

2.1.3 Loading a U2000 License

This topic describes how to load a U2000 license. This topic describes how to install a U2000 license. Before using a U2000, you must load a U2000 license.

Prerequisite

- The OS and database must run properly.

If the database has not been started, choose **Start > Programs > Microsoft SQL Server > Service Manager**, and then click **Start/Continue** to start the database.

- The processes of the U2000 must be properly started.

If U2000 services have not been started, run the **startnms.bat** file in the U2000 installation path **\server\bin** to start U2000 services manually.

Context

If you have selected the license installation method during installation, the installation script automatically copies the license file of a U2000 to the **license** folder in the U2000 installation path. Manual operation is not required.

Procedure

- **Method one: Use commands to load the license.**

1. Copy the authorized license file to the U2000 server. Directly copying and pasting the license file to the **D:\U2000\server\etc\conf\license** path is prohibited.

NOTE

- Do not modify the contents in the license file.
- Check whether a temporary license file exists in the **D:\U2000\server\etc\conf\license** folder. If the file exists, create a backup folder and then copy and paste the temporary license file to it.

2. Update the U2000 license.

(1) Log in to the OS of the server.

(2) Run the following command to update the U2000 license file:

```
> updateLicense -file License_file_name
```

NOTE

In the command, *License_file_name* indicates a file name or the combination of an absolute path and a 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)

(3) Enter **Y**, and then press **Enter**.

NOTE

After the preceding operations are performed, the license file is automatically loaded to the **D:\U2000\server\etc\conf\license** path and renamed.

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

1. Copy and paste the authorized license to the server where the U2000 client is installed. If the U2000 and server are on the same computer, directly copying and pasting the license file to the **D:\U2000\server\etc\conf\license** path is prohibited.

 NOTE

- Do not modify the contents in the license file.
- Check whether a temporary license file exists in the **D:\U2000\server\etc\conf\license** folder. If the file exists, create a backup folder and then copy and paste the temporary license file to it.

2. Update the U2000 license.

- (1) On the OS desktop, double-click the **U2000 Client** shortcut icon. The **Login** dialog box is displayed.
- (2) In the **Server** drop-down list, select the server to be logged in to. Then, set **User Name** and **Password** to the valid values, and click **Login**. 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 when you log in to the U2000 client, select the license to be updated as prompted.
- If **Installation by license** or 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 that is displayed, select the new license file and click **Open**.

----End

2.1.4 Starting a Single-Server System (Windows)

This topic describes how to start a Windows single-server system. After the U2000 server is started, you must start the U2000. Then, log in to the U2000 to manage networks.

Context

- U2000 services run as background processes. Maintain the U2000 services using a System Monitor client.
- The client is installed at the same time as the U2000 software. The client described in this topic is the one installed on the server.
- During installation of the U2000 software, only one default U2000 user, that is, the **admin** user, is provided. The **admin** user is the administrator of a U2000 and has the highest rights of the U2000.

Procedure

- 1 Log in to the OS as a user with **administrator** rights. The system automatically starts the database and U2000 service.

 NOTE

If the database has not been started, choose **Start > Programs > Microsoft SQL Server > Service Manager**, and then click **Start/Continue** to start the database. If the database has been started, the manual operation is not required.

If U2000 services have not been started, run the **startnms.bat** file in the U2000 installation path **\server\bin** to start U2000 services manually. If the U2000 has been started, the manual operation is not required.

- 2 Check the shortcut icons.

**CAUTION**

If you cannot log in to the server through the GUI, skip this step.

The following shortcut icons are displayed on the desktop:

- **U2000 Client**
- **U2000 System Monitor**
- **U2000 Server**
- **U2000 NMS Maintenance Suite**
- **NE Software Management**

- 3 Choose **Start > Programs > Network Management System > U2000 System Monitor** or double-click the associated shortcut icon on the desktop to start the System Monitor.
- 4 In the **Login** dialog box, enter a user name and password to access the System Monitor window. The user name is **admin** and the initial password is blank by default. When you log in to the System Monitor for the first time, you must change the initial password.
- 5 Check whether U2000 processes can be properly started. The processes whose startup mode is **manual** must be started manually.
- 6 Start a U2000 client.
 1. On the desktop, double-click the **U2000 Client** shortcut icon.
 2. In the dialog box that is displayed, enter a U2000 user name and password. If you have changed the password for the **admin** user when logging in to the System Monitor, enter the new password.

 NOTE

There are two data transmission modes, namely, **Common** and **Security(SSL)**. You can query data transmission modes on the server. The default data transmission mode is **Common**. For details, see [A.9.50 How to Set the Communication Mode on the U2000 server for the Single-Server System \(Windows\)](#).

----End

2.2 Modifying Parameters for a Single-Server System (Solaris)

This topic describes how to modify parameters for a centralized system, including the host name and IP address, route, time and time zone, subsystem, instance, and user password.

2.2.1 Preparing for System Parameter Modification

This topic describes how to prepare for centralized system parameter modification. Before modifying system parameters, you must get familiar with the networking structure and environment requirements, collect planning information, check hardware connections, power on the server, apply for a U2000 license, and check system installation.

2.2.2 Modifying System Parameters

This topic describes how to modify the host name and IP address, route, time and time zone, component, instance, and passwords of the OS and database users according to the collected planning information.

2.2.3 Loading a U2000 License

This topic describes how to load a U2000 license. This topic describes how to install a U2000 license. Before using a U2000, you must load a U2000 license.

2.2.4 Starting a Single-Server System (Solaris)

This topic describes how to start a Solaris single-server system. After the U2000 server is started, you must start the U2000. Then, log in to the U2000 to manage networks.

2.2.1 Preparing for System Parameter Modification

This topic describes how to prepare for centralized system parameter modification. Before modifying system parameters, you must get familiar with the networking structure and environment requirements, collect planning information, check hardware connections, power on the server, apply for a U2000 license, and check system installation.

2.2.1.1 Networking Structure

This topic describes the networking structure for a centralized system. Before commissioning a centralized system, installation engineers need to get familiar with the network structure of the centralized system prior to installation.

2.2.1.2 Environment Requirements

This topic describes the environment conditions, such as the telecommunications room environment, cable condition, and networking condition of the telecommunications room, that you must get familiar with before you commission a U2000.

2.2.1.3 Collecting Planning Information

This topic describes how to collect planning information. Before commissioning a centralized system, collect required information, including the host name, IP address, route, time zone and time, user password, installation path, component quantity, and instance quantity.

2.2.1.4 Checking Hardware Connections

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

2.2.1.5 Powering On a Server

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

2.2.1.6 Applying for a U2000 License

This topic describes how to apply for a U2000 license.

2.2.1.7 Checking System Installation

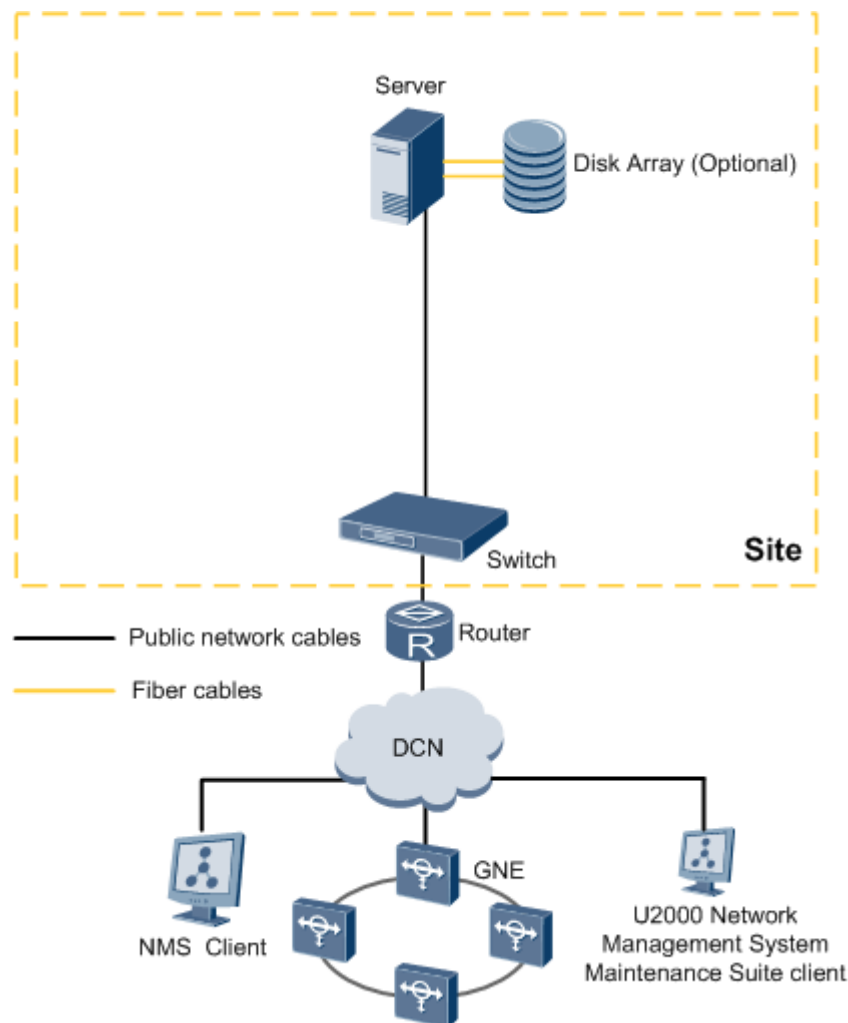
This topic describes how to check installation of a U2000. Before modifying system parameters, you must ensure that the U2000 has been installed and its version is correct.

2.2.1.1 Networking Structure

This topic describes the networking structure for a centralized system. Before commissioning a centralized system, installation engineers need to get familiar with the network structure of the centralized system prior to installation.

The following figure shows the network structure of the centralized system.

Figure 2-5 Network diagram for a centralized system



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

The U2000 client and network management system maintenance suite client communicate with the server using a DCN.

NEs and the OSS communicate with the centralized system using a DCN.

2.2.1.2 Environment Requirements

This topic describes the environment conditions, such as the telecommunications room environment, cable condition, and networking condition of the telecommunications room, that you must get familiar with before you commission a U2000.

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

Table 2-10 Installation environment requirements

Item	Requirement
Temperature	The required temperature range is 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 is from 40% to 65% for long-term working conditions and from 20% to 90% for short-term working conditions.
Dust	Dust density is less than or equal to 3 x 10 ⁴ /m ³ for particles with a diameter larger than 5 μm.
Floor	Flooring is anti-static movable and must be grounded.
Space	The telecommunications room has good ventilation and enough space for operation and maintenance.
Power supply	The power supply must be an independent external power supply system that provides stable electricity; UPS is recommended.
Circuit	The network where the server locates is functioning properly and is accessible.
Network	The routers connecting each server have been configured. For instructions on how to install routers, see the manuals delivered with the routers, or contact router suppliers. The networks of routers (including routers and the DCNs) in every telecommunications room are functioning properly.

2.2.1.3 Collecting Planning Information

This topic describes how to collect planning information. Before commissioning a centralized system, 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 planning 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 2-11 Host name list

Item	Example	Plan
Server	NMSserver	

Table 2-12 Controller IP address list

Item		Example	Plan
T5220	Controller IP address	129.9.1.20/255.255.255.0/129.9.1.254	
M4000	Primary controller IP address	129.9.1.21/255.255.255.0/129.9.1.254	
	Secondary controller IP address	129.9.2.21/255.255.255.0/129.9.2.254	
Disk array (optional)	Primary controller IP address	129.9.1.10/255.255.255.0/129.9.1.254	
	Secondary controller IP address	129.9.1.11/255.255.255.0/129.9.1.254	

 NOTE

The IP address is in the **IP address/subnet mask/gateway** format. The IP addresses for the primary and secondary controllers of the M4000 cannot be in the same network segment.

Table 2-13 System IP address list

Item	Example	Plan
System network interface	e1000g0	
System IP address	129.9.1.1/255.255.255.0/129.9.1.254	

 NOTE

Common network interface types include bge, ce, eri, ge0, and e1000g. You can check the physical network interfaces on the network card of the server.

To check the available physical network interfaces on the server, run the following command:

```
# more /etc/path_to_inst | grep network
```

Table 2-14 Route list

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

 NOTE

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

Table 2-15 Time zone and time list

Item	Example	Plan
Time zone	PRC Asia > Shanghai	
Time	14:00	

Table 2-16 User and password list

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

User	Example	Plan
network management system maintenance suite user admin	admin	

Table 2-17 Quantity list of configured components and instances

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

Table 2-18 Installation path list

Item	Installation Path
NMS software	/opt/U2000
Sybase database software	/opt/sybase

2.2.1.4 Checking Hardware Connections

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

Prerequisite

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

Procedure

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

Configuring disk arrays are optional. Skip this step if no disk array needs to be used.

- The following figures show the hardware connections between the T5220 server and three types of disk arrays.

Figure 2-6 Hardware connections between the T5220 server and the OceanStor S2600 disk array

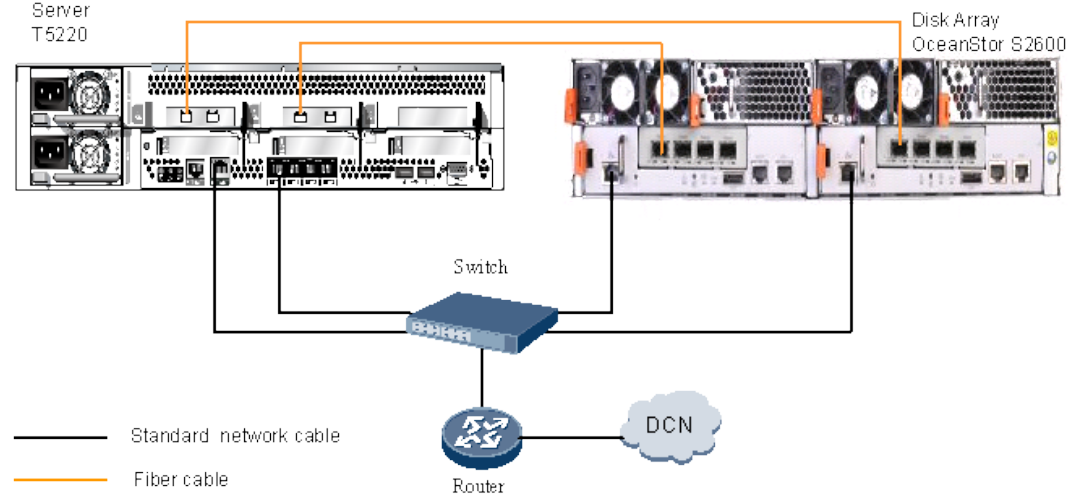


Figure 2-7 Hardware connections between the T5220 server and the OceanStor S3100 disk array

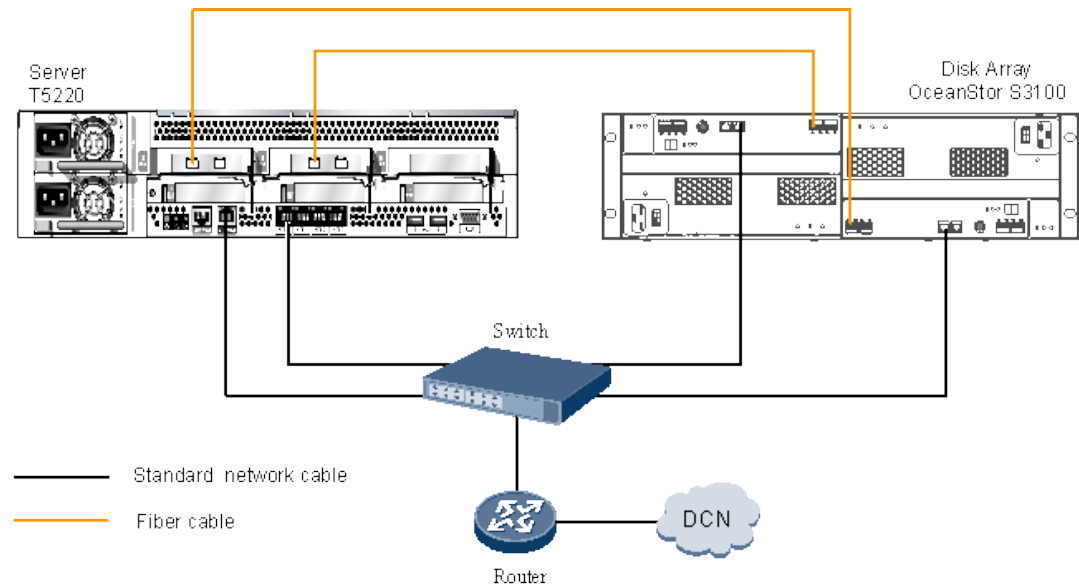
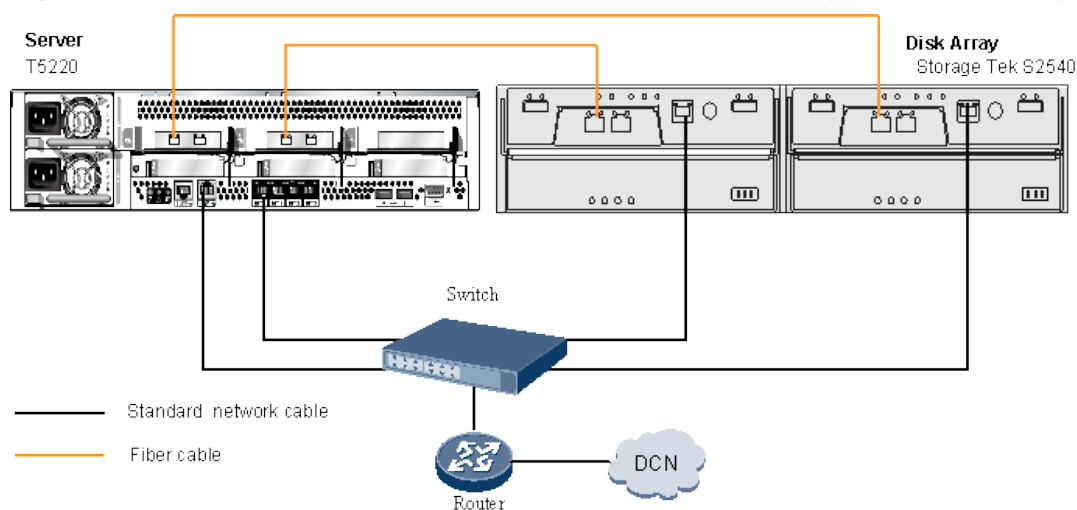


Figure 2-8 Hardware connections between the T5220 server and the StorageTek 2540 disk array

- The following figures show the hardware connections between the M4000 server and three types of disk arrays.

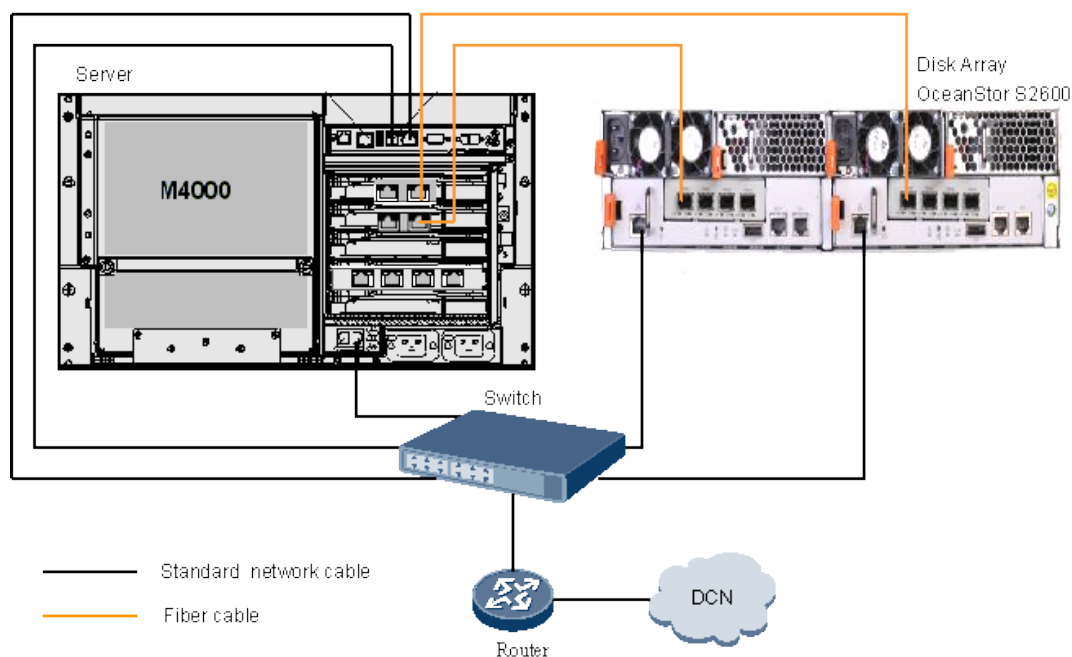
Figure 2-9 Hardware connections between the M4000 server and the OceanStor S2600 disk array

Figure 2-10 Hardware connections between the M4000 server and the OceanStor S3100 disk array

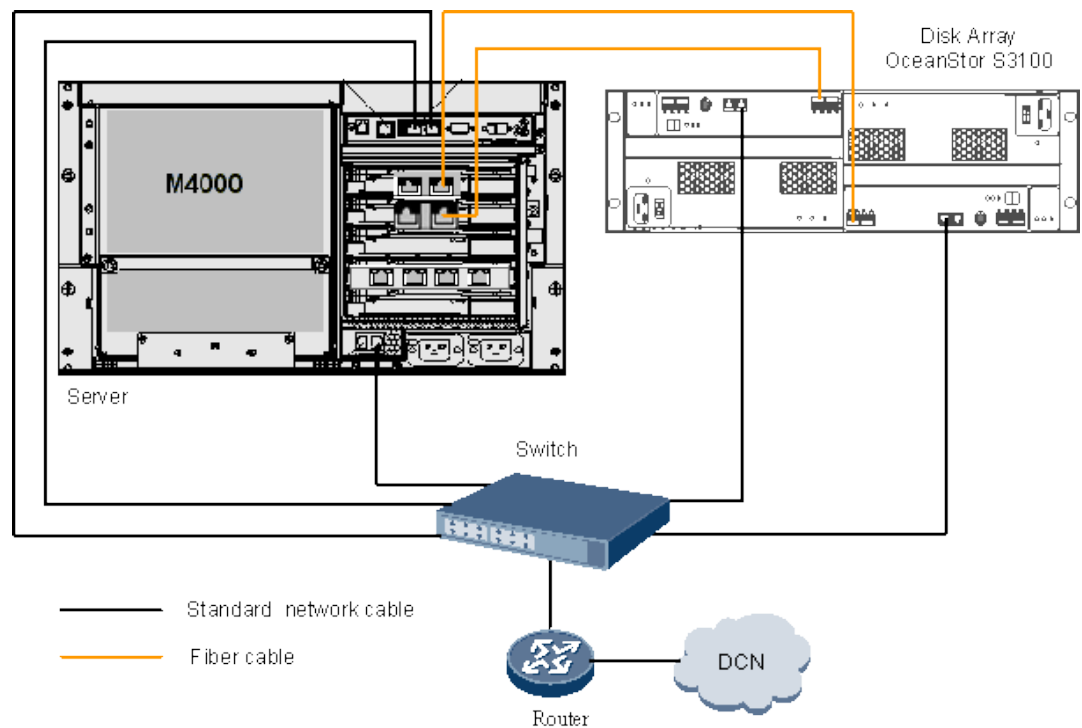
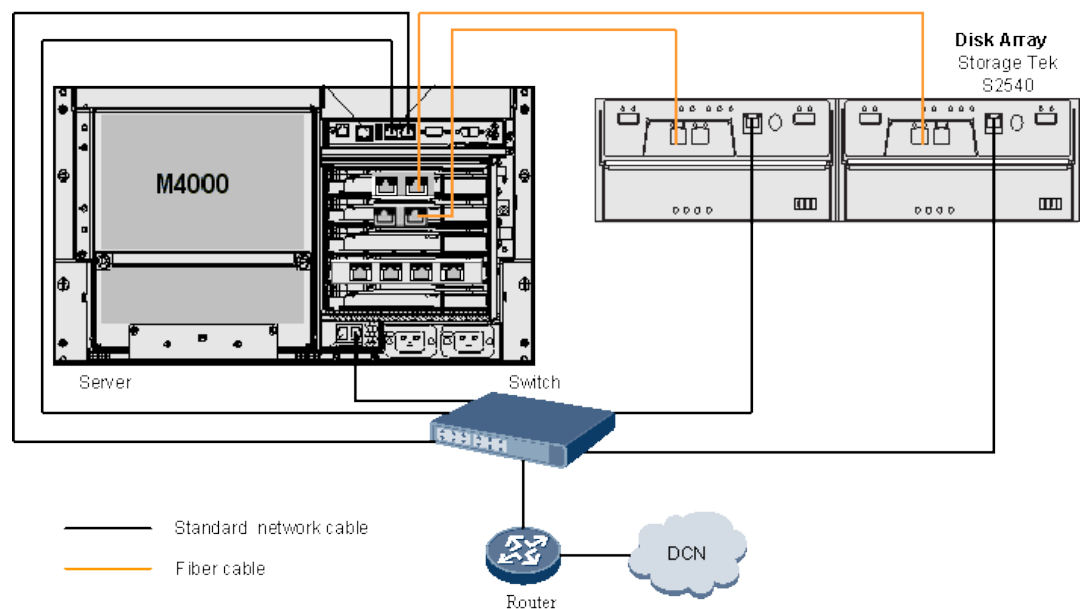


Figure 2-11 Hardware connections between the M4000 server and the StorageTek 2540 disk array



4 Check the plugs and sockets.

1. Ensure that the latches of cable plugs are locked fast and the plugs of coaxial cables are secured tightly.
 2. Ensure that the pins in each socket are complete and in good order. Curved pins may cause short circuits.
- 5 Ensure that all debris (cable straps, stubs, or moisture-absorbent packets) are picked up.
- 6 Remove unnecessary items from the telecommunications room. The workbench must be neat and the movable floor must be level and clean.

----End

2.2.1.5 Powering On a Server

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

T5220 Server

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

NOTE

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

Figure 2-12 Power button of the T5220 server



NOTE

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

M4000 Server

1. Connect the power supply to an M4000 server.

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

Figure 2-13 Power button of the M4000 server



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

 NOTE

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

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

Disk Arrays



CAUTION

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

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

2.2.1.6 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 to apply for a license according to the project contract number and the equipment serial number (ESN) of the U2000 server.
- 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.

Procedure

- 1 Obtain the contract number.
- 2 View ESNs.

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

NOTE

Make the following preparations:

- Obtain the ESN tool released with U2000 version from <http://support.huawei.com>. The ESN tool name is **U2000version_ESN_solaris_SPARC.tar**.
 - Copy the ESN tool package to the computer.
1. FTP the ESN tool to the U2000 server in binary mode. For example, upload the ESN tool to the **/opt** path. Details are as follows:
 - a. Log in to the computer where the ESN tool is stored.

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

Information similar to the following is displayed:

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

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

1. Log in to the OS as user **root**.
2. Run the following commands to view the ESN:
`# ./export/home/nmsuser/.profile`
`# cd /opt/U2000/server/lbin`
`# ./esn`

 NOTE

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

Information similar to the following is displayed:

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

- 3 Send the contract number and the server ESN to Huawei engineers or the local Huawei office.

 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

2.2.1.7 Checking System Installation

This topic describes how to check installation of a U2000. Before modifying system parameters, you must ensure that the U2000 has been installed and its version is correct.

Procedure

- 1 Log in to the OS as the **root** user.
- 2 To view the installation path **/opt/U2000** of the U2000 and the installation path **/opt/sybase** of the Sybase software, run the following commands:

```
# cd /opt
# ls
```

Information similar to the following is displayed:

```
HWENGR
HWICMR
sybase
U2000
...
```

- If the display information contains the U2000 and Sybase, the U2000 and Sybase database are installed.
- If the U2000 is not installed, install the U2000 according to the *iManager U2000 Single-Server Software Installation Guide (Solaris)*.

- 3 Check the U2000 version, run the following commands:

```
# cd /opt/U2000/server/etc/conf
# cat imap.cfg
```

Information similar to the following is displayed:

```
...
VER = U2000V100R002C01
```

The last line of the display 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 reinstall the U2000 according to the *iManager U2000 Single-Server Software Installation Guide (Solaris)*.

----End

2.2.2 Modifying System Parameters

This topic describes how to modify the host name and IP address, route, time and time zone, component, instance, and passwords of the OS and database users according to the collected planning information.

Modify the associated parameters according to the difference between the planning information and system parameters.

Parameter	Operation Method
Host name and IP address (Including route)	A.9.10 How to Change the IP Address and Host Name for the Single-Server System (Solaris)
Time and time zone	D.4.7 Setting the System Time and Time Zone
Component and instance	● To add a component, see D.4.1 Adding a Component. ● To delete a component, see D.4.2 Deleting a Component. ● To add a instance, see D.4.3 Adding an Instance. ● To delete a instance, see D.4.5 Deleting an Instance. ● To modify an instance name or a piece of remarks, see D.4.6 Changing the Name and Remarks of an Instance.
Password for the database supper user	D.4.8 Changing the Password of the Administrator of the Database
Password for the database user NMSuser	D.4.9 Changing the Password of the User of the Database
Password for the MSuite	D.3.4 Changing the Password of the MSuite
Password for the OS user root	In a CLI, run the following command to change the password for the root user: <pre># passwd root</pre> New Password: enter the new password of root Re-enter new Password: Re-enter new password of root
Password for the OS user nmsuser	In a CLI, run the following command to change the password for the nmsuser user: <pre># passwd nmsuser</pre> New Password: enter the new password of nmsuser Re-enter new Password: Re-enter new password of nmsuser

2.2.3 Loading a U2000 License

This topic describes how to load a U2000 license. This topic describes how to install a U2000 license. Before using a U2000, you must load 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

- During installation of the U2000 software, the OS user **nmsuser** is created automatically. The **nmsuser** user is used to regularly maintain a U2000.
- Two methods are available for loading a U2000 license.

– **Method one:**

Use commands to load the license. This method is applicable to users who cannot log in to GUI OSs.

Deployment scenario: The GUI is unavailable. Users cannot log in to the U2000 client but have to use commands for remote operations.

– **Method two:**

Load the license in the GUI. This method is applicable to users who are not familiar with common commands of the Solaris OS.

Deployment scenario: Loading the license in the GUI is recommended. If the GUI is available and the login to the U2000 client is successful, use this method.

Procedure

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

2 Ensure that the database is running.

Run the following command to check whether the Sybase database is running:

```
$ ps -ef | grep sybase
```

Information similar to the following is displayed:

```
sybase 4848 4847 0 May 18 ? 167:11 /opt/sybase/ASE-15_0/bin/data
server -sDBSVR -d/opt/sybase/data/lv_master -e/opt
sybase 5250 5248 0 May 18 ? 0:00 /opt/sybase/ASE-15_0/bin/back
upserver -sDBSVR_back -e/opt/sybase/ASE-15_0/insta
sybase 4847 1 0 May 18 ? 0:00 /usr/bin/sh /opt/sybase/ASE-1
5_0/install/RUN_DBSVR
sybase 5248 1 0 May 18 ? 0:00 /usr/bin/sh /opt/sybase/ASE-1
5_0/install/RUN_DBSVR_back
...
```

 NOTE

The database is running if the displayed information contains **/opt/sybase/ASE-15_0/install/RUN_DBSVR** and **/opt/sybase/ASE-15_0/install/RUN_DBSVR_back**.

Run the following commands to start the Sybase database if it is not running:

```
$ su - sybase
$ . /opt/sybase/SYBASE.sh
$ cd /opt/sybase/ASE-15_0/install
$ ./startserver -f ./RUN_DBSVR &
$ ./startserver -f ./RUN_DBSVR_back &
$ exit
```

 NOTE

Leave a space between the dot (.) and the command **/opt/sybase/SYBASE.sh**.

 NOTE

- **DBSVR** is the name of the database server and **DBSVR_back** is the name of the database backup server. These names must be consistent with the actual database names.
- View the database name and database backup server name by running the **more /opt/sybase/interfaces** command.

3 Ensure that the U2000 is running.

Run the following command to check whether the U2000 is running:

```
$ daem_ps
```


Information similar to the following is displayed:

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

NOTE

The U2000 is running if the displayed information contains **imap_sysmonitor -cmd start**.

To start the U2000 if it is not running, run the following commands:

```
$ cd /opt/U2000/server/bin
$ ./startnms.sh
```

- 4 Run the following commands to check whether a license file exists. If a license file 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
```

- 5 Load the U2000 license file.

Method one: Use commands to load the license.

1. Send the license file to the U2000 installation path **/export/home/nmsuser** in ASCII codes using FTP as the **nmsuser** user. Details are as follows:

- a. Log in to the PC where the license file is stored.
- b. Choose **Start > Run**. In the **Run** dialog box, enter **ftp system IP address of the server** and click **OK**. An FTP connection is established and a CLI is displayed.
- c. In the CLI, enter **nmsuser** as the name of the OS user.
User (IP_address: (none)) :**nmsuser**
- d. Enter the password for the **nmsuser** user.
Password:
- e. Set the format of the file to be transferred using FTP to ASCII.
ftp> **ascii**
- f. Navigate to the path on the computer where the license file is stored.
ftp> **lcd PC_directory**
- g. Navigate to the **/export/home/nmsuser** directory.
ftp> **cd /export/home/nmsuser**
- h. Run the **put** command to upload the license file to the server.
ftp> **put "License_file_name"**
- i. To exit the FTP program, run the following command:
ftp> **quit**

2. To activate the license file, run the following commands:

- a. Log in to the OS of the server as the **nmsuser** user.
- b. Run the following commands to update the U2000 license file:
\$ **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**.

Method two: Load the license in the GUI.

1. Save the license to be loaded to the server where the U2000 client is located.
2. Log in to the OS where the client program is installed.
 - In Windows, log in to the OS as the **administrator** user.
 - In Solaris, log in to the OS as the **nmsuser** user.
3. On the OS desktop, double-click the **U2000 Client** shortcut icon. The **Login** dialog box is displayed.
4. In the **Server** drop-down list, select the server 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 **Installation by license** or 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 that is displayed, select the new license file and click **Open**.

----End

Result

After the preceding operations are performed, the license file is automatically loaded to the **/opt/U2000/server/etc/conf/license** path.

2.2.4 Starting a Single-Server System (Solaris)

This topic describes how to start a Solaris single-server system. After the U2000 server is started, you must start the U2000. Then, log in to the U2000 to manage networks.

Prerequisite

The OS of the server must be started.

Context

- The client is installed at the same time as the centralized system. The client mentioned in this topic is the one installed on the server.
- 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 OS of the server as the **nmsuser** user.

2 Ensure that the database is running.

Run the following command to check whether the Sybase database is running:

```
$ ps -ef | grep sybase
```

Information similar to the following is displayed:

```
sybase 4848 4847 0 May 18 ? 167:11 /opt/sybase/ASE-15_0/bin/data
server -sDBSVR -d/opt/sybase/data/lv_master -e/opt
sybase 5250 5248 0 May 18 ? 0:00 /opt/sybase/ASE-15_0/bin/back
upserver -sDBSVR_back -e/opt/sybase/ASE-15_0/insta
sybase 4847 1 0 May 18 ? 0:00 /usr/bin/sh /opt/sybase/ASE-1
5_0/install/RUN_DBSVR
sybase 5248 1 0 May 18 ? 0:00 /usr/bin/sh /opt/sybase/ASE-1
5_0/install/RUN_DBSVR_back
...
```

NOTE

The database is running if the displayed information contains **/opt/sybase/ASE-15_0/install/RUN_DBSVR** and **/opt/sybase/ASE-15_0/install/RUN_DBSVR_back**.

Run the following commands to start the Sybase database if it is not running:

```
$ su - sybase
$ . /opt/sybase/SYBASE.sh
$ cd /opt/sybase/ASE-15_0/install
$ ./startserver -f ./RUN_DBSVR &
$ ./startserver -f ./RUN_DBSVR_back &
$ exit
```

NOTE

Leave a space between the dot (.) and the command **/opt/sybase/SYBASE.sh**.

NOTE

- **DBSVR** is the name of the database server and **DBSVR_back** is the name of the database backup server. These names must be consistent with the actual database names.
- View the database name and database backup server name by running the **more /opt/sybase/interfaces** command.

3 Ensure that the U2000 is running.

Run the following command to check whether the U2000 is running:

```
$ daem_ps
```

Information similar to the following is displayed:

```

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

```

 NOTE

The U2000 is running if the displayed information contains **imap_sysmonitor -cmd start**.

Run the following command to start the U2000 if it is not running:

```

$ cd /opt/U2000/server/bin
$ ./startnms.sh

```

4 Ensure that the network management system maintenance suite process is started.

Run the following command to switch to the **root** user:

```

$ su - root
password: password_of_the_root_user

```

Run the following command to check whether the network management system maintenance suite process is started:

```

# 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 -Dlanguage=en -Xverify:none -Xmx128m -Xm

```

 NOTE

If the displayed information contains **/opt/HWNMSJRE/jre_sol/bin/java -server**, it indicates that the network management system maintenance suite process is started.

If the network management system maintenance suite process is not started, run the following commands to start the network management system maintenance suite process:

```

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

```

Run the following command to switch back to the **nmsuser** user:

```

# exit

```

5 View the running status of each process through the System Monitor as user **nmsuser** to log in to the server GUI, as follows:

**CAUTION**

If you cannot log in to the GUI of the server, run the **svc_adm -cmd status** command to view the status of processes as user **nmsuser**.

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 [4.4.3 Setting the Access Control List](#).

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**.

For details about how to set the communication mode on the U2000 server for the single-server system (Solaris), see [A.9.51 How to Set the Communication Mode on the U2000 server for the Single-Server System \(Solaris\)](#).

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.

- 6 Start the U2000 client as user **nmsuser** to log in to the server GUI.



CAUTION

The U2000 should be logged in to through a standalone client in the event that login to the server through the GUI fails and login to the client on the server is not possible. For details, see [5 Commissioning the Communication Between the Server and an Independent Client](#).

1. On the desktop of the OS, double-click the **U2000 Client** shortcut icon.
2. In the dialog box that is displayed, enter the U2000 user name and password to open the main window of the client. The user name is **admin** and the password is the one changed in the previous step.

 NOTE

There are two data transmission modes, namely, **Common** and **Security(SSL)**. You can run the **ssl_adm -cmd query** command to query data transmission modes on the server. The **ssl_adm -cmd query** command must be run as user **nmsuser** in Solaris and SUSE Linux OS. The default data transmission mode is **Common**.

For details about how to set the communication mode on the U2000 server for the single-server system (Solaris), see [A.9.51 How to Set the Communication Mode on the U2000 server for the Single-Server System \(Solaris\)](#).

----End

2.3 Modifying Parameters for a Single-Server System (SUSE Linux-Distributed)

This topic describes how to modify parameters for a distributed system, including the host name and IP address, route, time and time zone, subsystem, instance, and user password.

2.3.1 Preparing for System Parameter Modification

This topic describes how to prepare for the modification of distributed system parameters. Before modifying parameters for a distributed system, you must get familiar with the networking structure and environment requirements, collect planning information, check hardware connections, power on the server, apply for a U2000 license, and check system installation..

[2.3.2 Modifying System Parameters](#)

This topic describes how to modify the host name and IP address, route, time and time zone, component, instance, and passwords of the OS and database users according to the collected planning information.

[2.3.3 Loading a U2000 License](#)

This topic describes how to load a U2000 license. You must install a U2000 license before using the U2000.

[2.3.4 Starting the Single-Server System \(SUSE Linux-Distributed\)](#)

This topic describes how to start the Single-Server System (SUSE Linux-Distributed). After the Single-Server System (SUSE Linux-Distributed) is started, you must start U2000 server processes before starting a U2000 client to monitor and manage the network.

2.3.1 Preparing for System Parameter Modification

This topic describes how to prepare for the modification of distributed system parameters. Before modifying parameters for a distributed system, you must get familiar with the networking structure and environment requirements, collect planning information, check hardware connections, power on the server, apply for a U2000 license, and check system installation..

[2.3.1.1 Networking Structure](#)

This topic describes the networking structure of a distributed system. Before commissioning a distributed system, you must get familiar with the networking structure.

[2.3.1.2 Environment Requirements](#)

This topic describes the environment conditions, such as the telecommunications room environment, cable condition, and networking condition of the telecommunications room, that you must get familiar with before you commission a U2000.

[2.3.1.3 Collecting Planning Information](#)

This topic describes how to collect planning information. Before commissioning a distributed system, collect required information, including the host name, IP address, route, time zone and time, user password, installation path, component quantity, and instance quantity.

[2.3.1.4 Checking Hardware Connections](#)

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

[2.3.1.5 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.

[2.3.1.6 Applying for a U2000 License](#)

This topic describes how to apply for a U2000 license.

[2.3.1.7 Checking System Installation](#)

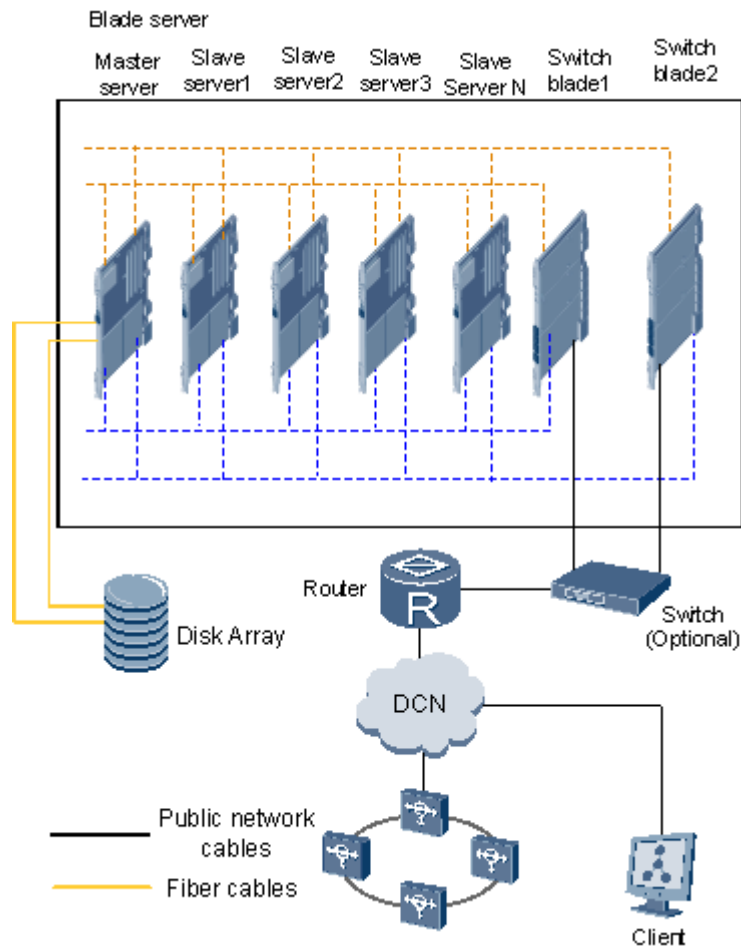
This topic describes how to check installation of a U2000. Before modifying system parameters, you must ensure that the U2000 has been installed and its version is correct.

2.3.1.1 Networking Structure

This topic describes the networking structure of a distributed system. Before commissioning a distributed system, you must get familiar with the networking structure.

The following figure shows the networking structure of a distributed system.

Figure 2-14 Networking diagram for a distributed system



Networking Diagram for a Distributed System

- 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.
- A distributed system communicates with an external network using a public network. For example, the connections to clients and equipment.
- A disk array is used to store database data to improve database performance.
- A maximum number of five slave servers are supported.

Connection Description of Communications in a Distributed System

- 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.
- The clients of both the U2000 and the network management system maintenance suite communicate with the master server and slave server using a DCN. That is, during the login to the client of either the U2000 or the network management system maintenance suite, the public IP address of the master server is selected. To ensure that the master server and slave server properly communicate with each other on an external network in the case of an NIC fault, the external probe is configured with bond by default.
- Both network elements (NEs) and the upper-layer NMS communicate with the distributed system (including the master server and slave server) through the DCN.

2.3.1.2 Environment Requirements

This topic describes the environment conditions, such as the telecommunications room environment, cable condition, and networking condition of the telecommunications room, that you must get familiar with before you commission a U2000.

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

Table 2-19 Installation environment requirements

Item	Requirement
Temperature	The required temperature range is 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 is from 40% to 65% for long-term working conditions and from 20% to 90% for short-term working conditions.
Dust	Dust density is less than or equal to $3 \times 10^4/\text{m}^3$ for particles with a diameter larger than 5 μm .
Floor	Flooring is anti-static movable and must be grounded.
Space	The telecommunications room has good ventilation and enough space for operation and maintenance.
Power supply	The power supply must be an independent external power supply system that provides stable electricity; UPS is recommended.
Circuit	The network where the server locates is functioning properly and is accessible.
Network	The routers connecting each server have been configured. For instructions on how to install routers, see the manuals delivered with the routers, or contact router suppliers. The networks of routers (including routers and the DCNs) in every telecommunications room are functioning properly.

2.3.1.3 Collecting Planning Information

This topic describes how to collect planning information. Before commissioning a distributed system, 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 planning 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 2-20 Host name list

Item	Example	Plan
Master server	Masterserver	
Slave serverN	SlaveserverN	

 NOTE

In the preceding table, N represents the serial number for a slave server. The host names for slave servers can be increased in sequence along with the increase of the number of slave servers. For example, the host name can be Slaveserver1. A maximum number of five slave servers are supported.

Table 2-21 Controller IP address list

Item		Example	Plan
Blade server	IP address for the network interface on the SMM	- ATAE blade server: 129.9.1.20/255.255.255.0/129.9.1.254 - IBM blade server: 129.9.1.30/255.255.255.0/129.9.1.254	
Disk array	Primary controller IP address	129.9.1.10/255.255.255.0/129.9.1.254	
	Secondary controller IP address	129.9.1.11/255.255.255.0/129.9.1.254	

 NOTE

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

Table 2-22 System IP address list

Item	Example	Plan
System network interface	eth0	
System IP address	● Master server: 129.9.1.30/255.255.255.0/129.9.1.254 ● Slave server: 129.9.1.31/255.255.255.0/129.9.1.254 ● ... ● slave server: 129.9.1.N/ 255.255.255.0/129.9.1.254	

 NOTE

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 2-23 Private network segment list

Item	Example	Plan
Private network segment 1	192.168.100.0	
Private network segment 2	192.168.101.0	
...	...	

Table 2-24 Route list

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

 NOTE

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

Table 2-25 Time zone and time list

Item	Example	Plan
Time zone	PRC Asia > Shanghai	
Time	14:00	

Table 2-26 List of users and passwords

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	PASSWORD NOTE When you enter the initial password, note that the character after letter "W" is a digit "0", but not a letter "O".	
Administrator admin for the OceanStor S2600 disk array	123456	
OS user root	root	
OS user oracle	oracle	
Database supper user	changeme	
Database user	NMSuser	
U2000 user admin	admin123	
network management system maintenance suite user admin	admin	

 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 2-27 Quantity list of configured components and instances

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

2.3.1.4 Checking Hardware Connections

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

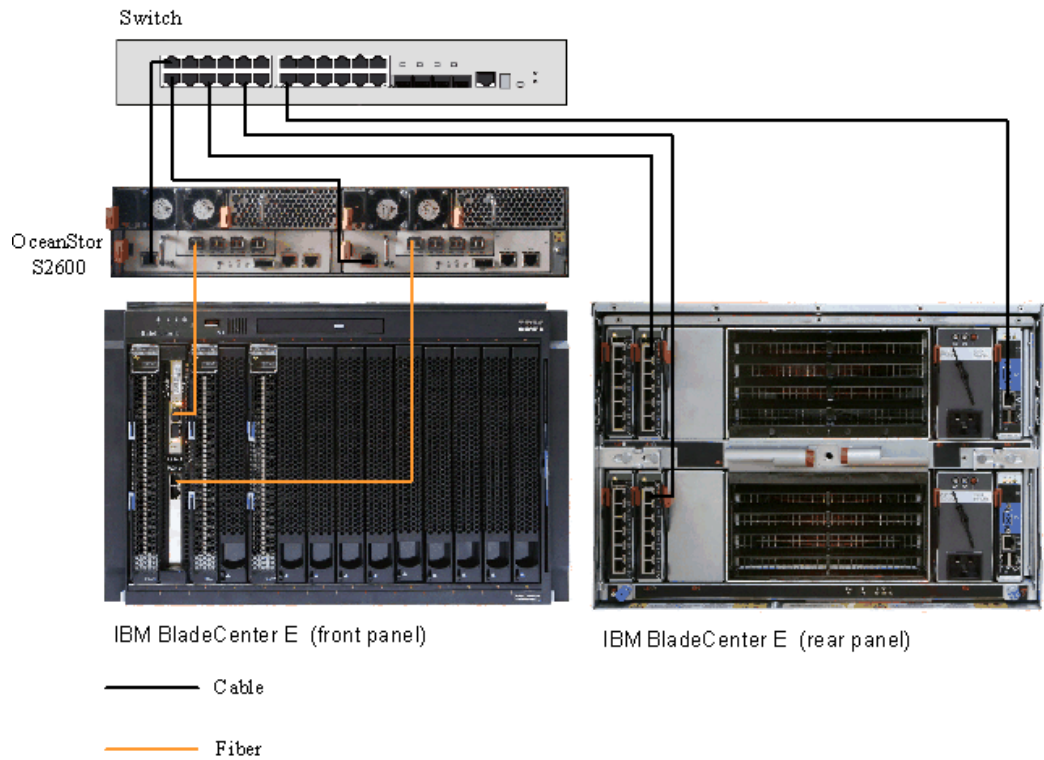
Prerequisite

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

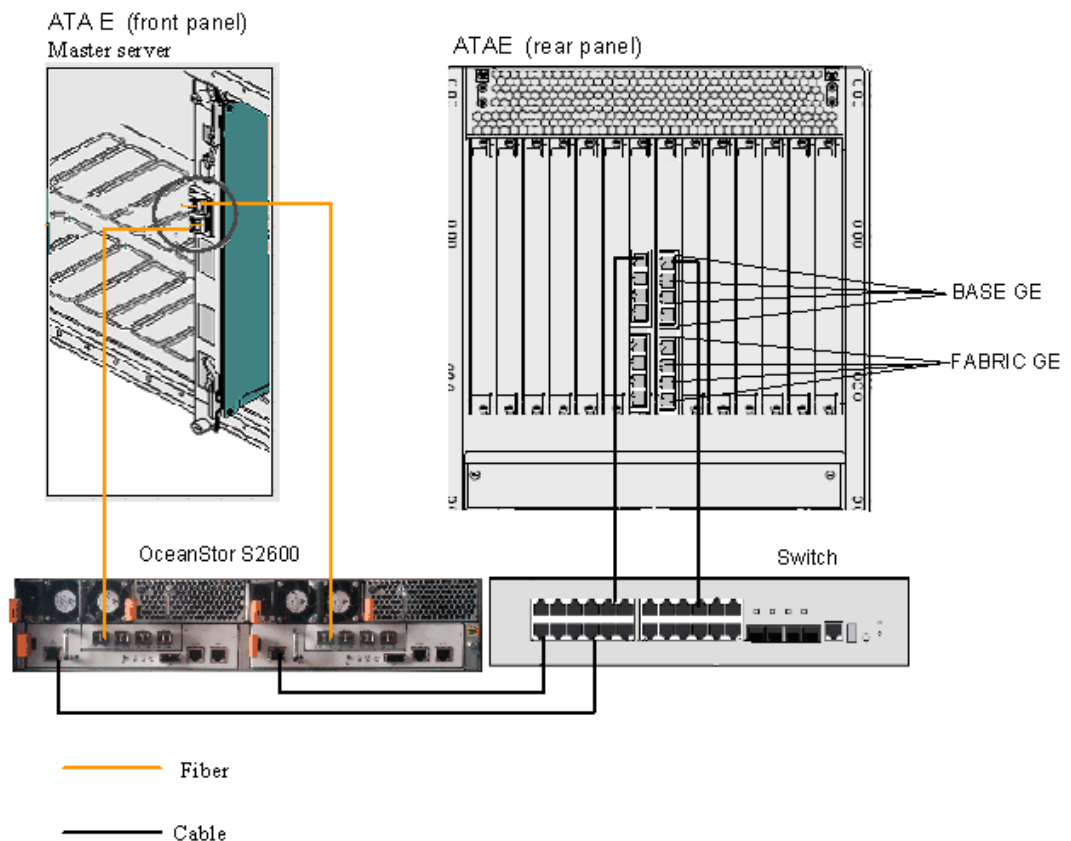
Procedure

- 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 card is in a correct slot of a subrack.
During U2000 installation, a label is attached to each card to identify the associated slot.
You must insert a card into a proper slot.
- 4 Check hardware connections and network cable connections according to the hardware connection diagram.
 - If an IBM blade server is used, connect cables according to the following figure.

Figure 2-15 Cable connection for an IBM blade server

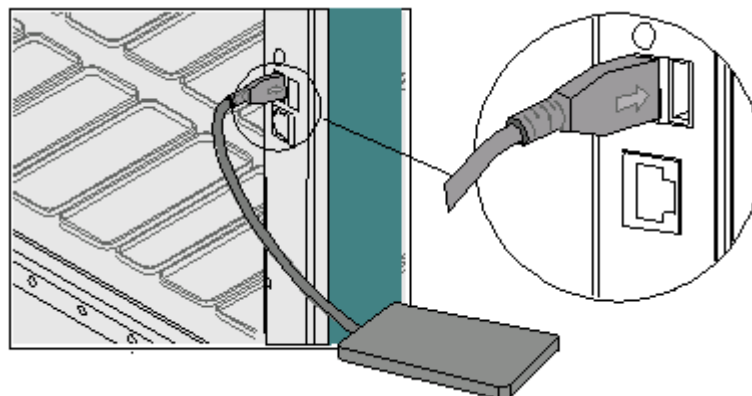


- In an ATAE blade server is used, connect cables according to the following figure. The blade server must be connected to an external network through the base plane of a switching board.

Figure 2-16 Cable connection for an ATAE blade server

- 5 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 2-17 Diagram of the connection between the ATAE server card and the USB drive

- 6 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.
 - 7 Ensure that all debris (cable straps, stubs, or moisture-absorbent packets) are picked up.
 - 8 Remove unnecessary items from the telecommunications room. The workbench must be neat and the movable floor must be level and clean.
- End

2.3.1.5 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.

2.3.1.6 Applying for a U2000 License

This topic describes how to apply for a U2000 license.

Context

- The license file is not delivered to customers along with a U2000 installation DVD. Contact Huawei engineers for the application of a master server license according to the contract number and ESNs of the server.
- 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.

Procedure

- 1 Obtain the contract number.
- 2 View ESNs of the master server.

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 OS as user **root**.
2. Run the following commands to view the ESN:
./export/home/nmsuser/.profile
cd /opt/U2000/server/lbin
./esn

 NOTE

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

Information similar to the following is displayed:

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

- 3 Send the contract number and the server ESN to Huawei engineers or the local Huawei office.

 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

2.3.1.7 Checking System Installation

This topic describes how to check installation of a U2000. Before modifying system parameters, you must ensure that the U2000 has been installed and its version is correct.

Procedure

- 1 Log in to the OS of the master server as the **root** user.
- 2 To view the U2000 installation path **/opt/U2000** and the Oracle software installation path **/opt/oracle**, run the following commands:

```
# cd /opt
# ls
```

Information similar to the following is displayed:

```
HWENGR
HWICMR
oracle
U2000
...
```

- If the displayed information contains U2000 and oracle, the U2000 and Oracle database have been installed.
- If the displayed information does not contain U2000, install a U2000. For details about how to install a U2000, see the *iManager U2000 Single-Server Software Installation Guide (SUSE Linux)*.

- 3 To check the U2000 version, run the following commands:

```
# cd /opt/U2000/server/etc/conf
# cat imap.cfg
```

Information similar to the following is displayed:

```
...
VER = U2000V100R002C01
```

The last line of the displayed information shows the U2000 version. If the version does not meet the actual requirement, uninstall the U2000 and then obtain the correct U2000 version to reinstall the U2000. For details about how to reinstall a U2000, see the *iManager U2000 Single-Server Software Installation Guide (SUSE Linux)*.

----End

2.3.2 Modifying System Parameters

This topic describes how to modify the host name and IP address, route, time and time zone, component, instance, and passwords of the OS and database users according to the collected planning information.

Modify the associated parameters according to the difference between the planning information and system parameters.

Parameter	Operation Method
Host name, IP address or route	A.9.11 How to Change the IP Address and Host Name of the Single-Server System (SUSE Linux-Distributed).
Time and time zone	D.4.7 Setting the System Time and Time Zone.

Parameter	Operation Method
Component and instance	● To add a component, see D.4.1 Adding a Component. ● To delete a component, see D.4.2 Deleting a Component. ● To add a instance, see D.4.3 Adding an Instance. ● To delete a instance, see D.4.5 Deleting an Instance. ● To modify an instance name or a piece of remarks, see D.4.6 Changing the Name and Remarks of an Instance.
Password for the database supper user	D.4.8 Changing the Password of the Administrator of the Database
Password for the database user NMSuser	D.4.9 Changing the Password of the User of the Database
Password for the MSuite	D.3.4 Changing the Password of the MSuite
Password for the OS user root	In a CLI, run the following command to change the password for the root user: <pre># passwd root</pre> New Password: enter the new password of root Re-enter new Password: Re-enter new password of root

2.3.3 Loading a U2000 License

This topic describes how to load a U2000 license. You must install a U2000 license before using the U2000.

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

Two methods are available for loading a U2000 license.

- Use commands to load the license. In this method, you must upload the license file to the specified path on the server and then run commands on the U2000 server to load the license.
- Load the license in the GUI. In this method, you only need to save the license file to the computer where the U2000 client is installed and use the U2000 client to load the license.



NOTE

You can select a method as required. No matter which method is selected, ensure that the U2000 server process has been started.

Procedure

- 1 Ensure that the network management system maintenance suite process and daem process on the slave server is started.

 NOTE

If there are multiple slave servers, check them respectively.

1. Log in to the OS of the slave server as the **root** user.
2. Do as follows to check whether the network management system maintenance suite process has been started:

```
# 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_linux/bin/java
-server -Dequinox.conf=engineering/conf/installE
```

 NOTE

If the displayed information contains **/opt/HWNMSJRE/jre_linux/bin/java -server**, it indicates that the network management system maintenance suite process is started.

If the network management system maintenance suite process has not been started, run the following commands to start it:

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

3. Do as follows to check whether the daem process of the slave server has been started:

```
# 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 imapmr
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.

If the daem process has not been started, run the following command to start it:

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

- 2 Ensure that the network management system maintenance suite process on the master server is started.

1. Log in to the OS of the master server as the **root** user.
2. Do as follows to check whether the network management system maintenance suite process has been started:

```
# 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_linux/bin/java
-server -Dequinox.conf=engineering/conf/installE
```

 NOTE

If the displayed information contains **/opt/HWNMSJRE/jre_linux/bin/java -server**, it indicates that the network management system maintenance suite process is started.

If the network management system maintenance suite process has not been started, run the following commands to start it:

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

3 Ensure that the database is running.

To check whether the Oracle database is running, run the following command:

```
> ps -ef | grep ora_
```

Information similar to the following is displayed:

```
oracle      4055          1  0  20:00 ?        00:00:00 ora_j000_U2KDB
oracle      4174      4107  0  20:00 pts/1    00:00:00 grep ora_
oracle     23333          1  0  Nov15 ?        00:00:20 ora_pmon_U2KDB
oracle     23335          1  0  Nov15 ?        00:00:00 ora_vktm_U2KDB
oracle     23339          1  0  Nov15 ?        00:00:00 ora_diag_U2KDB
oracle     23341          1  0  Nov15 ?        00:00:00 ora_dbrm_U2KDB
oracle     23343          1  0  Nov15 ?        00:00:01 ora_psp0_U2KDB
oracle     23347          1  0  Nov15 ?        00:03:35 ora_dia0_U2KDB
oracle     23349          1  0  Nov15 ?        00:00:00 ora_mman_U2KDB
oracle     23351          1  0  Nov15 ?        00:00:03 ora_dbw0_U2KDB
oracle     23353          1  0  Nov15 ?        00:00:13 ora_lgwr_U2KDB
oracle     23355          1  0  Nov15 ?        00:00:15 ora_ckpt_U2KDB
oracle     23357          1  0  Nov15 ?        00:00:06 ora_smon_U2KDB
```

...

NOTE

If the displayed information contains the following processes, the database service is started successfully:

- ora_pmon_U2KDB
- ora_dbw0_U2KDB
- ora_lgwr_U2KDB
- ora_ckpt_U2KDB
- ora_smon_U2KDB

To check whether the listener is started, run the following commands:

```
> su - oracle
password:password_of_oracle_user
> lsnrctl status
> exit
```

Information similar to the following is displayed:

```
...
STATUS of the LISTENER
-----
Alias                LISTENER
Version              TNSLSNR for Linux: Version 11.1.0.7.0 - Production
Start Date           17-DEC-2009 20:35:58
Uptime               0 days 0 hr. 5 min. 2 sec
Trace Level          off
Security             ON: Local OS Authentication
SNMP                 OFF
...
```

NOTE

If the displayed information contains **Alias LISTENER**, the listener is started successfully:

To start the Oracle database, run the following commands:

```
> su - oracle
```

```
password:password_of_oracle_user
> sqlplus / as sysdba
SQL> startup
ORACLE instance started.

Total System Global Area 1610612736 bytes
Fixed Size                2046264 bytes
Variable Size             385877704 bytes
Database Buffers          1207959552 bytes
Redo Buffers              14729216 bytes
Database mounted.
Database opened.
```

To exit the SQL Server database, run the following command:

```
SQL> exit
```

To start the listener, run the following command:

```
> lsnrctl start
```

To log out as the Oracle user, run the following command:

```
> exit
```

4 On the master server, start U2000 server processes.

1. To check whether U2000 server processes have been 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 27069      1    0 10:31:39 ?          1:39 imapmr
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

The U2000 is running if the displayed information contains **imap_sysmonitor -cmd start**.

2. If the U2000 processes are not started, run the following command to start U2000 processes:

```
# cd /opt/U2000/server/bin
# ./startnms.sh
```

5 Run the following commands to check whether a license file exists. If a license file 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
```

6 Do as follows to load the U2000 license.

Method one: Use commands to load the U2000 license.

1. Send the license file in ASCII codes by FTP to the U2000 installation path **/export/home/nmsuser** 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. On the server, open a CLI and run the following commands to make the license take effect:
cd /opt/U2000/server
. svc_profile.sh
cd /export/home/nmsuser
updateLicense -file License_file_name

 NOTE

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

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)

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

Method two: Load the U2000 license in the GUI.

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

 NOTE

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

----End

Result

After the preceding operations are performed, the license file is automatically loaded to the **/opt/U2000/server/etc/conf/license** path.

2.3.4 Starting the Single-Server System (SUSE Linux-Distributed)

This topic describes how to start the Single-Server System (SUSE Linux-Distributed). After the Single-Server System (SUSE Linux-Distributed) is started, you must start U2000 server processes before starting a U2000 client to monitor and manage the network.

Prerequisite

The OSs of the master server and slave server must be started.

Context

- In normal cases, the network management system maintenance suite process and the daem process of the slave server start along with the server OS.
- In normal cases, the network management system maintenance suite process and the database process of the master server start along with the server OS.

Procedure

- 1 Ensure that the network management system maintenance suite process and daem process on the slave server is started.

 NOTE

If there are multiple slave servers, check them respectively.

1. Log in to the OS of the slave server as the **root** user.
2. Do as follows to check whether the network management system maintenance suite process has been started:

```
# 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_linux/bin/java
-server -Dequinox.conf=engineering/conf/installE
```

 NOTE

If the displayed information contains **/opt/HWNMSJRE/jre_linux/bin/java -server**, it indicates that the network management system maintenance suite process is started.

If the network management system maintenance suite process has not been started, run the following commands to start it:

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



```
# ./startserver.sh
```

3. Do as follows to check whether the daem process of the slave server has been started:

```
# 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.

If the daem process has not been started, run the following command to start it:

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

2. Ensure that the network management system maintenance suite process on the master server is started.

1. Log in to the OS of the master server as the **root** user.
2. Do as follows to check whether the network management system maintenance suite process has been started:

```
# 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_linux/bin/java
-server -Dequinox.conf=engineering/conf/installE
```

NOTE

If the displayed information contains `/opt/HWNMSJRE/jre_linux/bin/java -server`, it indicates that the network management system maintenance suite process is started.

If the network management system maintenance suite process has not been started, run the following commands to start it:

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

3. On the master server, do as follows to ensure that the Oracle process and the database listening process have been started:

1. To check whether the Oracle process has been started, run the following command:

```
# su - oracle
> ps -ef | grep ora_
```

Information similar to the following is displayed:

```
oracle    4055      1  0 20:00 ?          00:00:00 ora_j000_U2KDB
oracle    4174    4107  0 20:00 pts/1      00:00:00 grep ora_
oracle    23333      1  0 Nov15 ?          00:00:20 ora_pmon_U2KDB
oracle    23335      1  0 Nov15 ?          00:00:00 ora_vktm_U2KDB
oracle    23339      1  0 Nov15 ?          00:00:00 ora_diag_U2KDB
oracle    23341      1  0 Nov15 ?          00:00:00 ora_dbrm_U2KDB
oracle    23343      1  0 Nov15 ?          00:00:01 ora_psp0_U2KDB
```

```

oracle 23347 1 0 Nov15 ? 00:03:35 ora_dia0_U2KDB
oracle 23349 1 0 Nov15 ? 00:00:00 ora_mman_U2KDB
oracle 23351 1 0 Nov15 ? 00:00:03 ora_dbw0_U2KDB
oracle 23353 1 0 Nov15 ? 00:00:13 ora_lgwr_U2KDB
oracle 23355 1 0 Nov15 ? 00:00:15 ora_ckpt_U2KDB
oracle 23357 1 0 Nov15 ? 00:00:06 ora_smon_U2KDB
...

```

 NOTE

- If the displayed information contains the following five processes, it indicates that the database service is started normally.
 - ora_pmon_U2KDB
 - ora_dbw0_U2KDB
 - ora_lgwr_U2KDB
 - ora_ckpt_U2KDB
 - ora_smon_U2KDB

- If the database process is not started, run the following commands to start the Oracle database process.

```

> sqlplus / as sysdba
SQL> startup
ORACLE instance started.

```

```

Total System Global Area 1610612736 bytes
Fixed Size                  2046264 bytes
Variable Size              385877704 bytes
Database Buffers          1207959552 bytes
Redo Buffers               14729216 bytes
Database mounted.
Database opened.

```

Run the following command to exit the SQL Server database.

```
SQL> exit
```

2. Run the following command to check whether the listener is started.

```
> lsnrctl status
```

Information similar to the following is displayed:

```

...
STATUS of the LISTENER
-----
Alias                LISTENER
Version              TNSLSNR for Linux: Version 11.1.0.7.0 - Production
Start Date           17-DEC-2009 20:35:58
Uptime                0 days 0 hr. 5 min. 2 sec
Trace Level           off
Security              ON: Local OS Authentication
SNMP                  OFF
...

```

 NOTE

- If the displayed information contains **Alias LISTENER**, it indicates that the listener is started normally.
- If the listen has not been started, run the following command to start it:


```
> lsnrctl start
```

3. Run the following command to log out the Oracle user:

```
> exit
```

- 4 On the master server, start U2000 server processes.

1. To check whether U2000 server processes have been 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 27069      1    0 10:31:39 ?          1:39 imapmr
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

The U2000 is running if the displayed information contains **imap_sysmonitor -cmd start**.

2. If the U2000 processes are not started, run the following command to start U2000 processes:

```
# cd /opt/U2000/server/bin
# ./startnms.sh
```

- 5 Start the U2000 client.

 NOTE

Because no U2000 client and System Monitor client are available in the SUSE Linux OS, log in to the independent U2000 client. For details, see [5 Commissioning the Communication Between the Server and an Independent Client](#).

----End

2.4 Modifying the Parameters of the High Availability System (Windows)

This topic describes how to modify the parameters of the High Availability System (Windows), including the host name and IP address, route, time and time zone, subsystem, instance, and user password.

2.4.1 Preparing for the Modification of System Parameters

This topic describes how to prepare for the modification of system parameters. Before modifying the parameters of the Windows High Availability System (Veritas Hot Standby), you must get familiar with the networking structure and environment requirements, collect planning information, check hardware connections, power on a server, apply for a Veritas license and U2000 license, and check system installation.

2.4.2 Loading or Updating a License File

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.

2.4.3 Modifying System Parameters

This topic describes how to modify the host name, IP address, time, DST of the time zone, component, instance, and passwords of the OS and database users according to the collected planning information.

2.4.4 Starting the High Availability System (Windows)

This topic describes how to start the high availability system. Starting the U2000 high availability system includes starting the U2000 server and logging in to the U2000 client.

2.4.1 Preparing for the Modification of System Parameters

This topic describes how to prepare for the modification of system parameters. Before modifying the parameters of the Windows High Availability System (Veritas Hot Standby), you must get familiar with the networking structure and environment requirements, collect planning information, check hardware connections, power on a server, apply for a Veritas license and U2000 license, and check system installation.

2.4.1.1 Networking Structure

This topic describes the networking structure of the high availability system (Veritas hot standby). Before commissioning the high availability system (Veritas hot standby), you need to familiarize yourself with the networking structure of the high availability system (Veritas hot standby).

2.4.1.2 Environment Requirements

This topic describes the environment conditions, such as the telecommunications room environment, cable condition, and networking condition of the telecommunications room, that you must get familiar with before you commission a U2000.

2.4.1.3 Collecting Planning Information

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

2.4.1.4 Checking Hardware Connections

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

2.4.1.5 Powering On a Server

This topic describes how to power on a server.

2.4.1.6 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.

2.4.1.7 Applying for a U2000 License

This topic describes how to apply for a U2000 license.

2.4.1.8 Checking System Installation

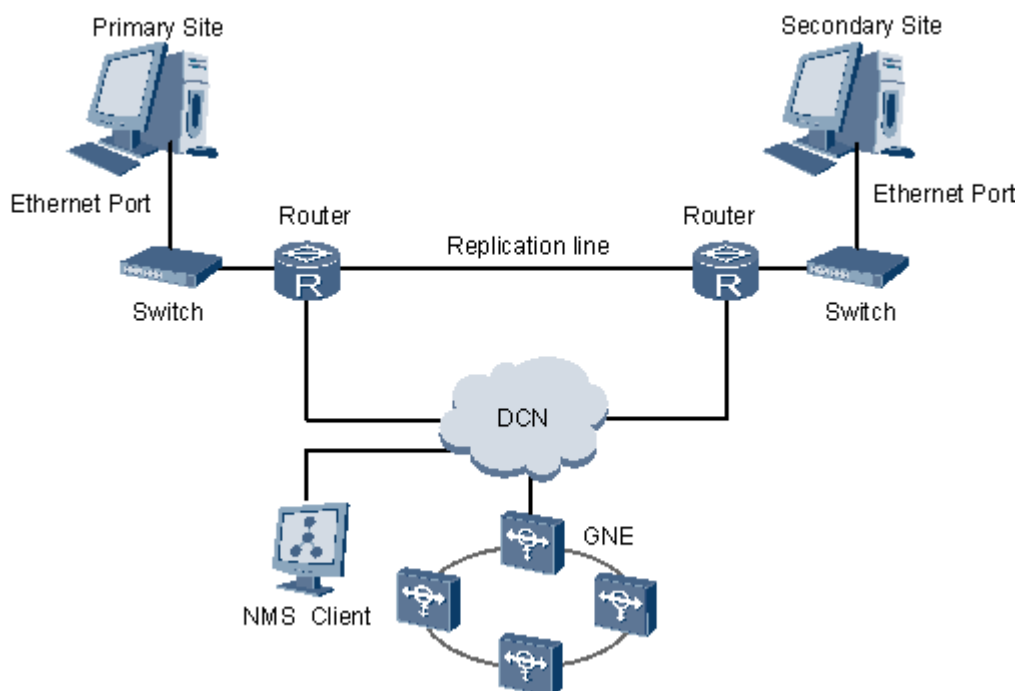
This topic describes how to check the installation of the high availability system (Solaris). Before modifying system parameters, you need to ensure that the Windows High Availability System (Veritas Hot Standby) is installed and its version is correct.

2.4.1.1 Networking Structure

This topic describes the networking structure of the high availability system (Veritas hot standby). Before commissioning the high availability system (Veritas hot standby), you need to familiarize yourself with the networking structure of the high availability system (Veritas hot standby).

The following figure shows the networking structure of the high availability system (Veritas hot standby).

Figure 2-18 Networking structure of the high availability system (Veritas hot standby)



Networking Description of the high availability system (Veritas hot standby)

- The high availability system (Veritas hot standby) consists of the primary site and the secondary site. Each site is composed of one workstation.
- The primary and secondary sites communicate through the DCN. The IPMP feature can be configured on the primary and secondary sites to prevent a single NIC from becoming invalid.
- The NMS client and the network management system maintenance suite client communicate with the server through the data communication network (DCN).
- NEs and the upper-layer NMS (OSS) communicate with the server through the DCN.

2.4.1.2 Environment Requirements

This topic describes the environment conditions, such as the telecommunications room environment, cable condition, and networking condition of the telecommunications room, that you must get familiar with before you commission a U2000.

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

Table 2-28 Installation environment requirements

Check Item	Requirement
Temperature	The required temperature range is from 15°C to 30°C in long-term working conditions and from 0°C to 45°C in short-term working conditions.

Check Item	Requirement
Humidity	The required humidity range is 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 is larger than 5 μm is less than or equal to $3 \times 10^4/\text{m}^3$.
Floor	The floor is anti-static movable and must be grounded.
Space	The telecommunication room must have good ventilation and enough space for operation and maintenance.
Power supply	The power supply should 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 is normal and can be accessed successfully.
Network	The routers connecting each server are 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 are connected, including routers and the DCNs.

2.4.1.3 Collecting Planning Information

This topic describes how to collect planning information. Before commissioning the high availability system (Veritas hot standby), 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 planning 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 2-29 Host name list

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

**CAUTION**

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

- The host name of the U2000 server must be unique on the network.
- The host name must be a string consisting of no more than 24 characters that can only be letters (A to Z), digits (0 to 9) and hyphen (-).
- The first character must be a letter and the last character cannot be a hyphen.
- The host name must be case-sensitive.
- The host name cannot contain any space.
- The host name cannot contain only one character.
- The host name cannot contain --.
- The host name cannot be any of the following keywords in the high availability system.
action false keylist static after firm local stop requires
remotecluster
system group resource global Start str temp set heartbeat
ArgListValues
System Group boolean hard Name soft before online condition
MonitorOnly
remote start cluster event VCSshm type Path offline Signaled
HostMonitor
Probed state Cluster IState int Type State VCSshm NameRule
ConfidenceLevel

Table 2-30 IP address planning of the single-networking-interface scheme

Site	Equipment Description	IP Planning	Sample IP Address/Subnet Mask
Primary site	System IP address	It is set during the OS installation. It is used for client and NE communication (optional and recommended) for heartbeat detection and data replication.	129.9.1.1/255.255.255.0
	Virtual IP address	It is used for client and NE communication (optional and not recommended; the virtual IP address is easy to be occupied, or the communication will fail if the virtual IP address is not enabled due to VCS abnormality). It is used to check NICs.	129.9.1.2/255.255.255.0

Site	Equipment Description	IP Planning	Sample IP Address/Subnet Mask
Secondary site	System IP address	It is set during the OS installation. It is used for client and NE communication (optional and recommended) for heartbeat detection and data replication.	129.9.1.3/255.255.255.0
	Virtual IP address	It is used for client and NE communication (optional and not recommended; the virtual IP address is easy to be occupied, or the communication will fail if the virtual IP address is not enabled due to VCS abnormality). It is used to check NICs.	129.9.1.4/255.255.255.0

Table 2-31 Time zone and time list

Item	Example	Plan
Time zone	PRC Asia > Shanghai	
Time	14:00	

Table 2-32 List of users and passwords

User	Example	Plan
Super user administrator of the OS	admin123	
DB Super User sa	changeme	
DB User NMSuser	NMSuser	
U2000 user admin	admin123	
network management system maintenance suite user admin	admin	
VCS Client User admin	password	

Table 2-33 Server disk partition list (4*146GB disk)

Partition	Size (GB)	Description
Disk C	40	It is used to install the OS and database software.
Disk D	100	It is used to install the U2000 software.
Disk S	50	It is used to store the database data. NOTE Disk S is not a physical disk assigned during the installation of the OS, but a file volume created during the installation of the Veritas software.

Table 2-34 Installation path list

Software	Installation Path
Windows OS	C:\
SQL Server database software	C:\MSSQL2000
SQL Server database data files	S:\data
U2000 software	D:\U2000

 NOTE

The installation directory, including the installation package path and the U2000 installation path, can contain only the letter, number, and underscore (_). It cannot contain the space or brackets; otherwise, the installation fails.

Table 2-35 Quantity list of configured components and instances

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

2.4.1.4 Checking Hardware Connections

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

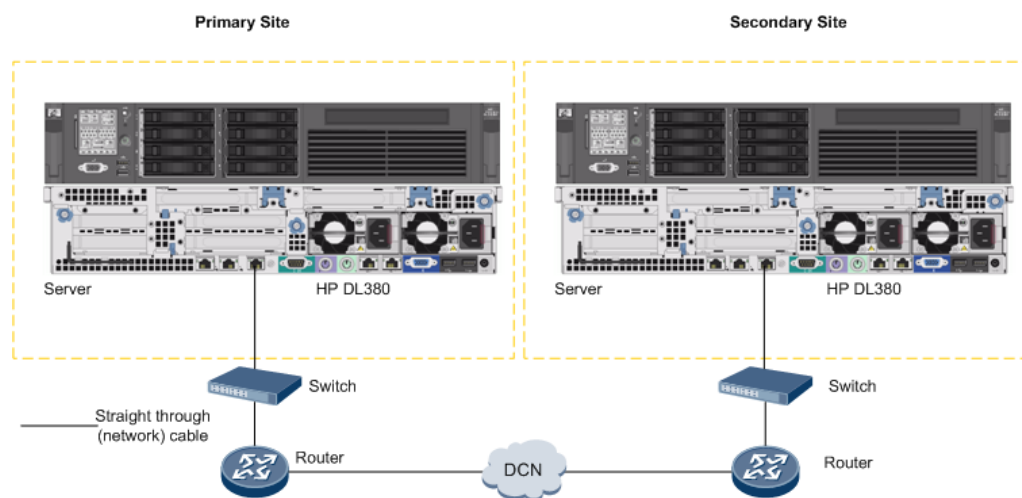
Prerequisite

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

Procedure

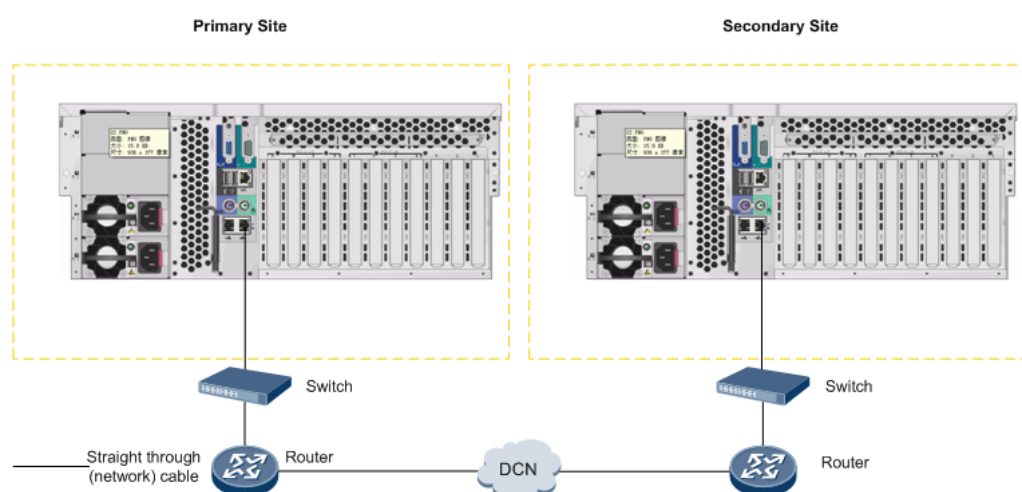
- 1 Ensure that the power cables and ground wires for all components are tightly connected and in good contact and that the polarities are properly placed.
- 2 Ensure that all cables are bundled and free of visible damage.
- 3 Check hardware connections and network cable connections according to the hardware connection diagram.
 - The following figures show the hardware connections of the DL380 server.

Figure 2-19 Hardware connection between the DL380 server



- The following figures show the hardware connections of the DL580 server.

Figure 2-20 Hardware connection between the DL580 server



- 4 Check the plugs and sockets.

1. Ensure that the latches of cable plugs are locked fast and the plugs of coaxial cables are secured tightly.
 2. Ensure that the pins in each socket are complete and in good order. Curved pins may cause short circuits.
- 5 Ensure that all debris (cable straps, stubs, or moisture-absorbent packets) are picked up.
- 6 Remove unnecessary items from the telecommunications room. The workbench must be neat and the movable floor must be level and clean.

----End

2.4.1.5 Powering On a Server

This topic describes how to power on a server.

1. Press the power buttons of the peripherals connected to a server and the monitor to power on the peripherals and monitor.
2. Press the power button on the chassis of the server to power on the server. Take the HP DL580G5 server as an example. In the following figure, the power button is marked in a red frame.

Figure 2-21 Position of the power button of the DL580G5 server



2.4.1.6 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

2.4.1.7 Applying for a U2000 License

This topic describes how to apply for a U2000 license.

Context

- The license file is not delivered to customers along with a U2000 installation DVD. Contact Huawei engineers to apply for a license according to the contract number and the equipment serial number (ESN) of the U2000 server.
- 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.
- The license needs to be bound to the ESNs of both the primary site server and the secondary site server.

Procedure

- 1 Obtain the contract number.
- 2 Before installing a U2000, obtain the ESN tool from <http://support.huawei.com> to generate ESNs. The ESN tool is named U2000~~version~~_ESN_win32_x86.zip.

Decompress the ESN tool package, and then double-click the **esn.exe** file to view ESNs.

A message similar to the following will be displayed:

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

- 3 Send the contract number and the ESNs of the server to Huawei engineers or a Huawei local office.

NOTE

Huawei engineers access the <http://license.huawei.com> Web site according to the information you provide to apply for a license file. For details about how to apply for a license file, see the *iManager U2000 V100R002C01 License Instructions* archived at <http://support.huawei.com>.

- 4 Huawei engineers send the license file to you after obtaining it.

The license file delivered along with the U2000 is in .dat format.

----End

2.4.1.8 Checking System Installation

This topic describes how to check the installation of the high availability system (Solaris). Before modifying system parameters, you need to ensure that the Windows High Availability System (Veritas Hot Standby) is installed and its version is correct.

Procedure

- 1 Check the shortcut icons.



CAUTION

If you cannot log in to the server through the GUI, skip this step.

The following shortcut icons are displayed on the desktop:

- U2000 Client
- U2000 System Monitor
- U2000 Server
- U2000 NMS Maintenance Suite
- NE Software Management

- 2 Run the following command on the primary site to check whether the replication between the primary and secondary sites is normal:

```
C:\> vxrlink -g datadg -i2 status datarlk
```

Information similar to the following is displayed:

```
2010-3-8 14:35:19  
RLINK is up to date.  
RLINK is up to date.
```

If **RLINK is up to date** is displayed, it indicates that the replication is normal.

3 Start the U2000 System Monitor client.

1. Choose **Start > Programs > Network Management System > U2000 System Monitor** or double-click the associated shortcut icon on the desktop to start the System Monitor.
2. In the **Login** dialog box, enter a user name and password to access the System Monitor window. The user name is **admin** and the initial password is blank by default. When you log in to the System Monitor for the first time, you must change the initial password.
3. Choose **Help > About** from the main menu. The **About** dialog box is displayed. Check the U2000 version.

NOTE

If the version information does not meet the actual requirement, uninstall the U2000 and obtain the correct software version to reinstall the U2000. For details, see the *iManager U2000 High Availability System (Veritas) Software Installation Guide (Windows)*.

4 Start the U2000 client.

1. On the desktop, double-click the **U2000 Client** shortcut icon.
2. In the dialog box that is displayed, enter a U2000 user name and password. If you have changed the password for the **admin** user when logging in to the System Monitor, enter the new password.

NOTE

There are two data transmission modes, namely, **Common** and **Security(SSL)**. You can query data transmission modes on the server. The default data transmission mode is **Common**. For details, see [A.9.53 How to Set the Communication Mode on the U2000 Server for the High Availability System \(Windows\)](#).

----End

2.4.2 Loading or Updating a License File

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.

[2.4.2.1 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.

[2.4.2.2 Loading a U2000 License](#)

This topic describes how to load a U2000 license. This topic describes how to install a U2000 license. Before using a U2000, you must load a U2000 license.

2.4.2.1 Updating a Veritas License

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

Prerequisite

The formal Veritas license must be obtained.

Context



NOTE

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

Procedure

- 1 Back up all the license files in the **C:\Program Files\Common Files\Veritas Shared\vrtslic\lic** directory.
- 2 In **Control Panel**, click **Add or Remove Programs**. In the **Add or Remove Programs** dialog box, select the Veritas Storage Foundation HA 5.1 for Windows (Server Components) program, and then click **Change**.
- 3 In the dialog box that is displayed, click the **License Management** option button, and then click **Next**.
- 4 Enter the license that is newly applied for, that is, VRTS STORAGE FOUNDATION STANDARD. Then, click **Update**. Click **Finish**.



NOTE

- The information about the demo or formal license that is newly applied for is contained in the license file.
 - The licenses that are newly applied for include VRTS STORAGE FOUNDATION STANDARD, VRTS VOLUME REPLICATOR OPTION, and VRTS CLUSTER SERVER HA/DR.
- 5 Repeat the preceding steps, enter the license keys of VRTS VOLUME REPLICATOR OPTION and VRTS CLUSTER SERVER HA/DR.
 - 6 Run the following command to check whether the updated license takes effect:

```
C:\> vxlicrep
```

Check whether the license key of the related component is updated and whether the authentication date of the component is correct.
 - 7 Restart the OS.

----End

2.4.2.2 Loading a U2000 License

This topic describes how to load a U2000 license. This topic describes how to install a U2000 license. Before using a U2000, you must load a U2000 license.

Prerequisite

- The OS and database must run properly on the primary site.
If the database has not been started, start it by referring to [A.5.4 How to Start the SQL Server Database](#).
- The processes of the U2000 must be properly started on the primary site.
If the processes of the U2000 has not been started, start it by referring to [A.9.26 How to Start the U2000 Processes of the High Availability System \(Windows\)](#).

Context

If you select the License installation method during the installation, the installation script automatically copies the License file of the U2000 to the **license** directory in the U2000 installation path. Manual copying is not required.

Procedure

- **Method one: Use commands to load the license.**
 1. Log in to the server on the primary site.
 2. Copy the authorized license file to the U2000 server. Directly copying and pasting the license file to the **D:\U2000\server\etc\conf\license** path is prohibited.

NOTE

- Do not modify the contents in the license file.
- Check whether a temporary license file exists in the **D:\U2000\server\etc\conf\license** folder. If the file exists, create a backup folder and then copy and paste the temporary license file to it.

3. Update the U2000 license.
 - (1) Log in to the OS of the server.
 - (2) Run the following command to update the U2000 license file:

```
> updateLicense -file License_file_name
```

NOTE

In the command, *License_file_name* indicates a file name or the combination of an absolute path and a 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)

- (3) Enter **Y**, and then press **Enter**.

NOTE

After the preceding operations are performed, the license file is automatically loaded to the **D:\U2000\server\etc\conf\license** path and renamed.

4. Log in to the server on the secondary site.
5. Check whether the temporary license file exists in the **D:\U2000\server\etc\conf\license** folder. If yes, create the backup folder and copy and paste the temporary license file to it.
6. Copy and paste the updated license file on the primary site to the **D:\U2000\server\etc\conf\license** path on the server on the secondary site.

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

1. Copy and paste the authorized license to the server where the U2000 client is installed. If the U2000 and server are on the same computer, directly copying and pasting the license file to the **D:\U2000\server\etc\conf\license** path is prohibited.

 NOTE

- Do not modify the contents in the license file.
- Check whether a temporary license file exists in the **D:\U2000\server\etc\conf\license** folder. If the file exists, create a backup folder and then copy and paste the temporary license file to it.

2. Update the U2000 license on the primary site.

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

 NOTE

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

3. Update the U2000 license on the secondary site.

- (1) On the primary site, log in to the VCS client. Right-click the AppService resource group and choose **Switch to > Remote switch** from the shortcut menu.
- (2) Select the clusters and systems to be switched.
- (3) Click **OK**.
- (4) In the **Confirm** dialog box, click **Yes** to switch U2000 services to the secondary site.
- (5) 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

2.4.3 Modifying System Parameters

This topic describes how to modify the host name, IP address, time, DST of the time zone, component, instance, and passwords of the OS and database users according to the collected planning information.

Modify the associated parameters according to the difference between the planning information and system parameters.

Parameter	Operation Method
Host name and IP address (Including route)	● To Modify the host name, see A.9.13 How to Change the Host Name of the High Availability System (Windows). ● To Modify the IP address, see A.9.12 How to Modify the Server IP Address of High Availability System (Windows).
Time and time zone	● Modifying the time 1. Access the Control Panel window. Then, double-click the Date and Time icon. 2. In the dialog box that is displayed, click the Date and Time tab to set the current system date and time. Then, click OK. ● Modifying the time zone and DST 1. Access the Control Panel window. Then, double-click the Date and Time icon. 2. In the dialog box that is displayed, click the Time Zone tab. Select a time zone where the server resides from the drop-down list. 3. If you require the server to automatically adjust the time according to the DST, click the Internet Time tab, and then select the Automatically synchronize with an Internet time server check box. 4. Click OK.
Component and instance	● To add a component, see D.4.1 Adding a Component. ● To delete a component, see D.4.2 Deleting a Component. ● To add a instance, see D.4.3 Adding an Instance. ● To delete a instance, see D.4.5 Deleting an Instance. ● To modify an instance name or a piece of remarks, see D.4.6 Changing the Name and Remarks of an Instance.
Password for the database supper user	D.4.8 Changing the Password of the Administrator of the Database
Password for the database user NMSuser	D.4.9 Changing the Password of the User of the Database
Password for the MSuite	D.3.4 Changing the Password of the MSuite

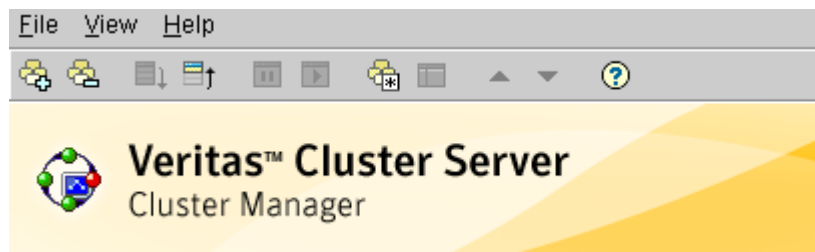
Parameter	Operation Method
Password of the super user administrator of the OS	A.1.2 How to Change the Password of the OS Administrator?

2.4.4 Starting the High Availability System (Windows)

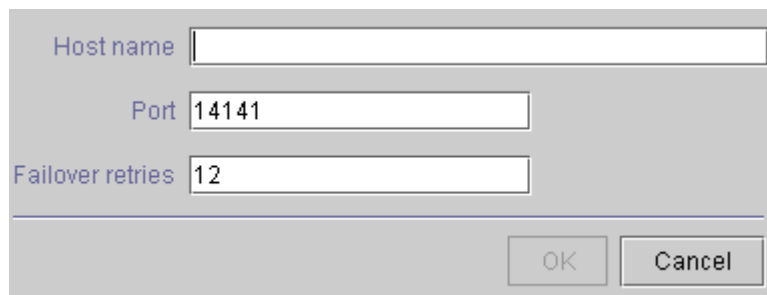
This topic describes how to start the high availability system. Starting the U2000 high availability system includes starting the U2000 server and logging in to the U2000 client.

Procedure

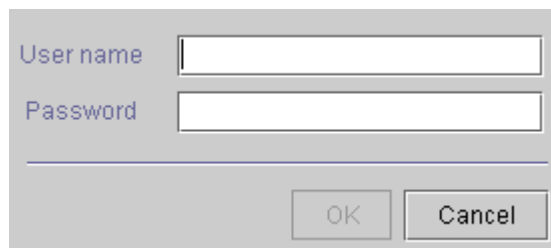
- 1 Log in to the OS of the server of the active site.
- 2 Choose **Start > Programs > Symantec > Veritas Cluster Server > Veritas Cluster Manager - Java Console** to start the VCS client.



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



- 4 Enter the IP address of the system of the primary site. Then, click **OK**.



- 5 Enter the default user name **admin** and the initial password **password** for the VCS client. Then, click **OK**.
- 6 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 database process and the NMS server process.

 TIP

Click the **Resources** tab to view the start status of each resource.

Normally, on the **Status** tab page, **State** of the server of the active site in the **Group Status on Member Systems** area is **Online**, and **Status** in the **Resource Status** area is **Online on primary**.

 NOTE

In actual configuration, use the actual host name.

7 View the running status of each process through the System Monitor. Details are as follows:

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 [4.4.3 Setting the Access Control List](#).

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**.

For details about how to set the communication mode on the U2000 server for the single-server system (Solaris), see [A.9.51 How to Set the Communication Mode on the U2000 server for the Single-Server System \(Solaris\)](#).

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.

8 Start the U2000 client.

1. On the desktop, double-click the **U2000 Client** shortcut icon.
2. In the dialog box that is displayed, enter a U2000 user name and password. If you have changed the password for the **admin** user when logging in to the System Monitor, enter the new password.

 NOTE

There are two data transmission modes, namely, **Common** and **Security(SSL)**. You can query data transmission modes on the server. The default data transmission mode is **Common**. For details, see [A.9.53 How to Set the Communication Mode on the U2000 Server for the High Availability System \(Windows\)](#).

----End

2.5 Modifying Parameters for a High Availability System (Solaris)

This topic describes how to modify parameters for a centralized system, including the host name and IP address, route, time and time zone, subsystem, instance, and user password.

2.5.1 Preparing for the Modification of System Parameters

This topic describes how to prepare for the modification of system parameters. Before modifying parameters for a high availability system (Solaris), you must get familiar with the networking structure and environment requirements, collect planning information, check hardware connections, power on a server, apply for a Veritas license and U2000 license, and check system installation.

2.5.2 Loading or Updating a License File

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.

2.5.3 Modifying System Parameters

This topic describes how to modify the host name and IP address, route, time and time zone, component, instance, and passwords of the OS and database users according to the collected planning information.

2.5.4 Starting a High Availability System (Solaris)

This topic describes how to start a U2000 high availability system. Starting a U2000 high availability system includes starting the U2000 server and logging in to a U2000 client.

2.5.1 Preparing for the Modification of System Parameters

This topic describes how to prepare for the modification of system parameters. Before modifying parameters for a high availability system (Solaris), you must get familiar with the networking structure and environment requirements, collect planning information, check hardware connections, power on a server, apply for a Veritas license and U2000 license, and check system installation.

2.5.1.1 Networking Structure

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

2.5.1.2 Environment Requirements

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

2.5.1.3 Collecting Planning Information

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

2.5.1.4 Checking Hardware Connections

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

2.5.1.5 Powering On a Server

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

2.5.1.6 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.

2.5.1.7 Applying for a U2000 License

This topic describes how to apply for a U2000 license.

2.5.1.8 Checking System Installation

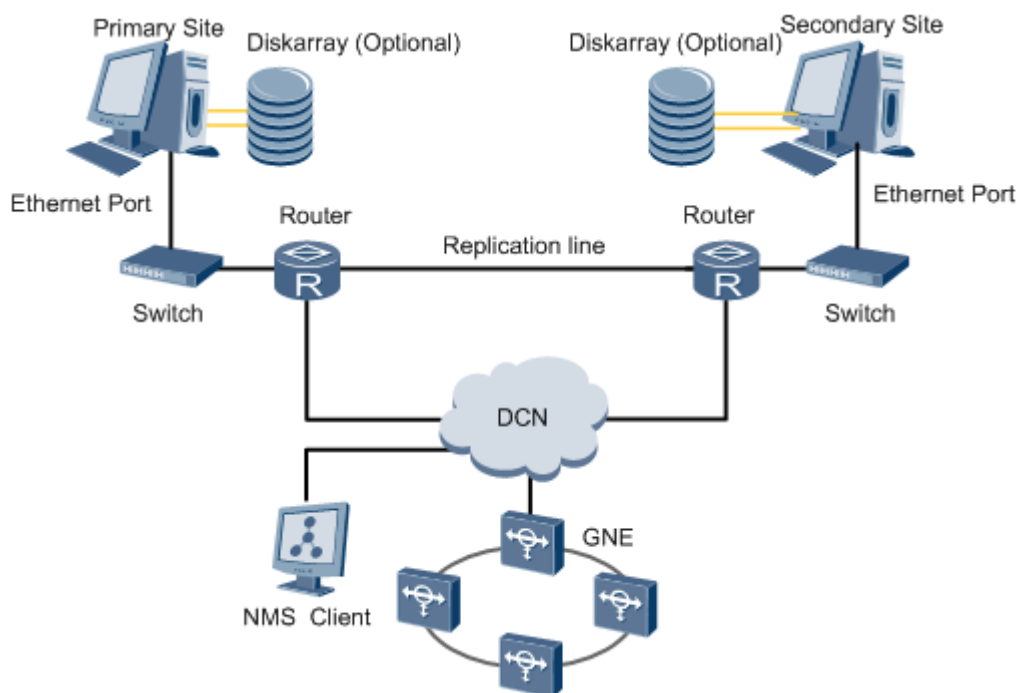
This topic describes how to check the installation of a high availability system (Solaris). Before modifying system parameters, you must ensure that the high availability system (Solaris) is installed and its version is correct.

2.5.1.1 Networking Structure

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

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

Figure 2-22 Networking structure of a high availability system (Solaris)



Networking Description About a high availability system (Solaris)

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

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

2.5.1.2 Environment Requirements

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

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

Table 2-36 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 $3 \times 10^4/\text{m}^3$.
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 uninterruptible 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. The bandwidth between primary and secondary sites must be 2 Mbit/s at least.

2.5.1.3 Collecting Planning Information

This topic describes how to collect planning information. Before commissioning the high availability system (Solaris), collect required information, including the host name, IP address,

route, time zone and time, user password, installation path, component quantity, and instance quantity.

Complete planning for the information listed in the following tables according to the *iManager U2000 Planning Guide*. Collect and record the planning 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 2-37 Host name list

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



CAUTION

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

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

```

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

```

You need to plan the following types of IP addresses:

- IP address of the workstation controller: This type of IP address is used to remotely log in to a workstation to manage and maintain workstation hardware. For example, you can use it to remotely install the OS or log in to a workstation to perform operation and maintenance if the OS fails to start properly.

- IP address of the disk array controller: This type of IP address is used to remotely manage and maintain equipment.
- System IP address: This type of IP address is used to log in to a server to manage and maintain the OS. It is the IP address of the OS.
- IP address of the heartbeat network service: This type of IP address is used to detect status of the network connection between the primary and secondary sites.
- IP address of the replication network service: This type of IP address is used to replicate data between Primary and secondary sites.
- NMS application IP address: This type of IP address is used to provide external NMS services, such as the communication between the NMS server and the clients or NEs.

 NOTE

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

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

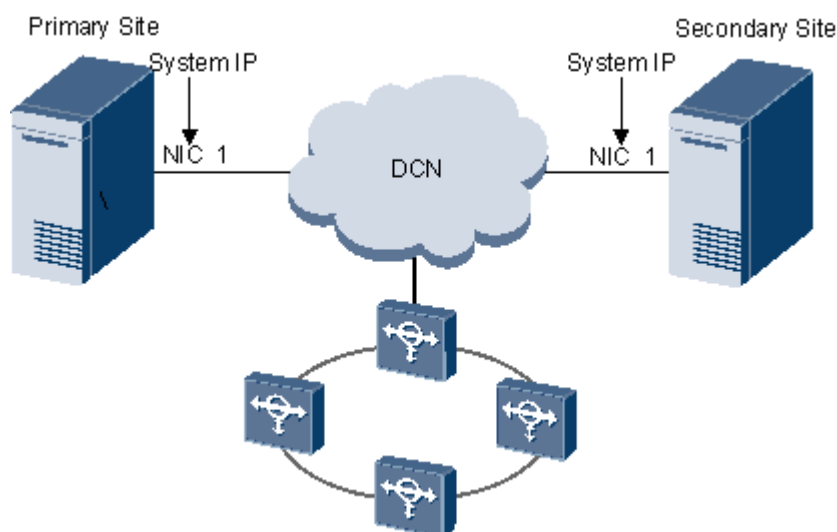
 NOTE

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

Single-NIC Scheme (Recommended)

Single-NIC scheme: Only one NIC is required. [Figure 2-23](#) shows the networking diagram. The single-NIC scheme is recommended.

Figure 2-23 Networking example (single-NIC scheme)



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

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

IP planning example: [Table 2-38](#) shows the planning example.

Table 2-38 Example of IP address planning of the single-NIC scheme

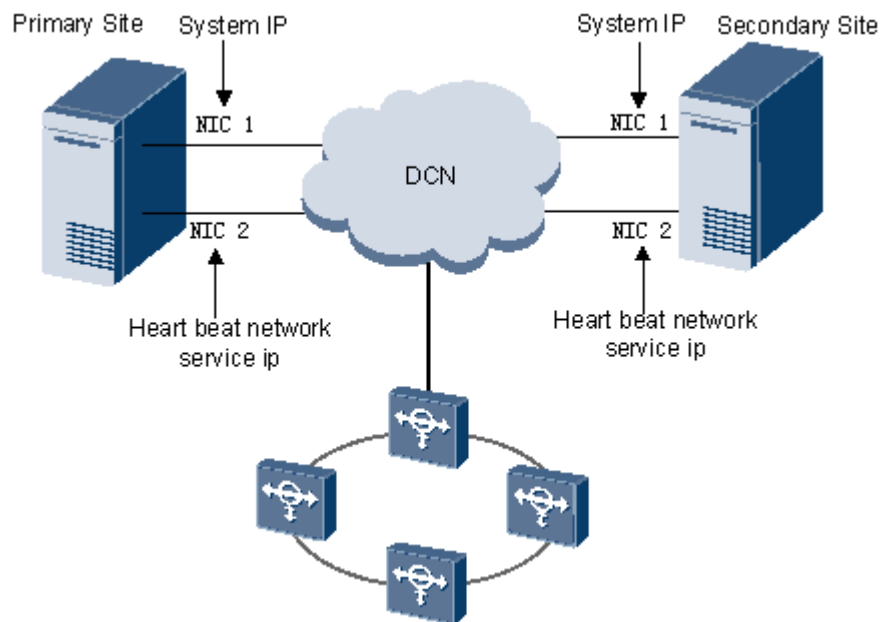
Site	Item	Example (IP Address/ Subnet Mask/Gateway)	Description
Primary site	IP address of the workstation controller	T5220 workstation: 129.9.1.20/255.255.255.0/129.9.1.254	● Plan the IP address according to the model of the selected workstation. ● The M4000 has the primary controller and secondary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

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

Double-NIC Scheme (Without IPMP)

Double-NIC scheme (without IPMP): Two NICs are required. [Figure 2-24](#) shows the networking diagram.

Figure 2-24 Networking example (double-NIC scheme (without IPMP))



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

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

**CAUTION**

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

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

IP planning example: Table 2-39 shows the planning example.

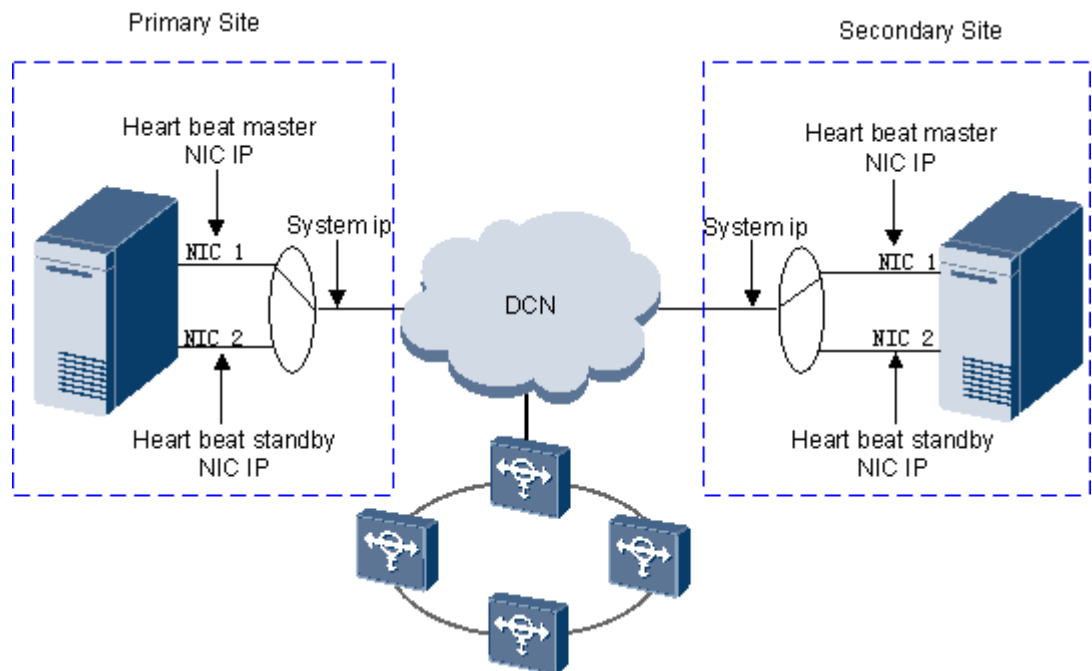
Table 2-39 Example of IP address planning of the double-NIC scheme (without IPMP)

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

Site	Item	Example (IP Address/ Subnet Mask/Gateway)	Description
		M4000 workstation: - Primary controller: 129.9.1.25/255.255.255.0/129.9.1.254 - Secondary controller: 129.9.2.25/255.255.255.0/129.9.2.254	primary controller and secondary controller cannot be on the same network segment.
	IP address of the disk array controller	OceanStor S2600: - Primary controller: 129.9.1.26/255.255.255.0/129.9.1.254 - Secondary controller: 129.9.1.27/255.255.255.0/129.9.2.254	-
	System IP address	129.9.1.2/255.255.255.0/129.9.1.254 - Used NIC: e1000g0	-
	IP address of the heartbeat network service	129.9.2.4/255.255.255.0/129.9.2.254 - Used NIC: e1000g1	-

Double-NIC Scheme (with IPMP)

Double-NIC scheme (with IPMP): Two NICs are required. [Figure 2-25](#) shows the networking diagram.

Figure 2-25 Networking example (double-NIC scheme (with IPMP))**IP planning description:**

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

**CAUTION**

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

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

IP planning example: [Table 2-40](#) shows the planning example.

Table 2-40 Example of IP address planning of the two-NIC scheme (with IPMP)

Site	Item	Example (IP Address/ Subnet Mask/Gateway)	Description
Primary site	IP address of the workstation controller	T5220 workstation: 129.9.1.20/255.255.255.0/129.9.1.254	- Plan the IP address according to the model of the selected workstation. - The M4000 has the primary controller and secondary controller. The IP addresses of the primary controller and secondary controller cannot be on the same network segment.
		M4000 workstation: - Primary controller: 129.9.1.21/255.255.255.0/129.9.1.254 - Secondary controller: 129.9.2.21/255.255.255.0/129.9.2.254	
	IP address of the disk array controller	OceanStor S2600: - Primary controller: 129.9.1.22/255.255.255.0/129.9.1.254 - Secondary controller: 129.9.1.23/255.255.255.0/129.9.2.254	-
	System IP address	129.9.1.1/255.255.255.0/129.9.1.254	-
	IP address of the active heartbeat NIC	129.9.1.2/255.255.255.0/129.9.2.254 - Used NIC: e1000g0	-
Secondary site	IP address of the workstation controller	T5220 workstation: 129.9.1.24/255.255.255.0/129.9.1.254	- Plan the IP address according to the model of the selected workstation. - The M4000 has the primary controller and secondary controller. The IP addresses of the primary controller and secondary controller cannot be on the same network segment.
		M4000 workstation: - Primary controller: 129.9.1.25/255.255.255.0/129.9.1.254 - Secondary controller: 129.9.2.25/255.255.255.0/129.9.2.254	

Site	Item	Example (IP Address/ Subnet Mask/Gateway)	Description
	IP address of the disk array controller	OceanStor S2600: ● Primary controller: 129.9.1.26/255.255.255.0/129.9.1.254 ● Secondary controller: 129.9.1.27/255.255.255.0/129.9.2.254	-
	System IP address	129.9.1.4/255.255.255.0/129.9.1.254	-
	IP address of the active heartbeat NIC	● 129.9.1.5/255.255.255.0/129.9.2.254 ● Used NIC: e1000g0	-
	IP address of the standby heartbeat NIC	● 129.9.1.6/255.255.255.0/129.9.3.254 ● Used NIC: e1000g1	-

Other Schemes

Contact Huawei engineers for scheme design.

Table 2-41 Route list

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

NOTE

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

Table 2-42 Time zone and time list

Item	Example	Plan
Time zone	PRC Asia > Shanghai	
Time	14:00	

Table 2-43 User and password list

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

Table 2-44 Quantity list of configured components and instances

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

2.5.1.4 Checking Hardware Connections

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

Prerequisite

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

Procedure

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

NOTE

- Configuring disk arrays is optional. If no disk array is configured, skip the connection to disk arrays.
- The following hardware connection diagrams are based on a single-NIC network configuration scheme. For details about a single-NIC network configuration scheme, see [2.5.1.3 Collecting Planning Information](#). The hardware connections based on other network configuration schemes are similar.
- The following figure shows the hardware connection of the T5220 server.

Figure 2-26 Hardware connection between the T5220 server and the OceanStor S2600

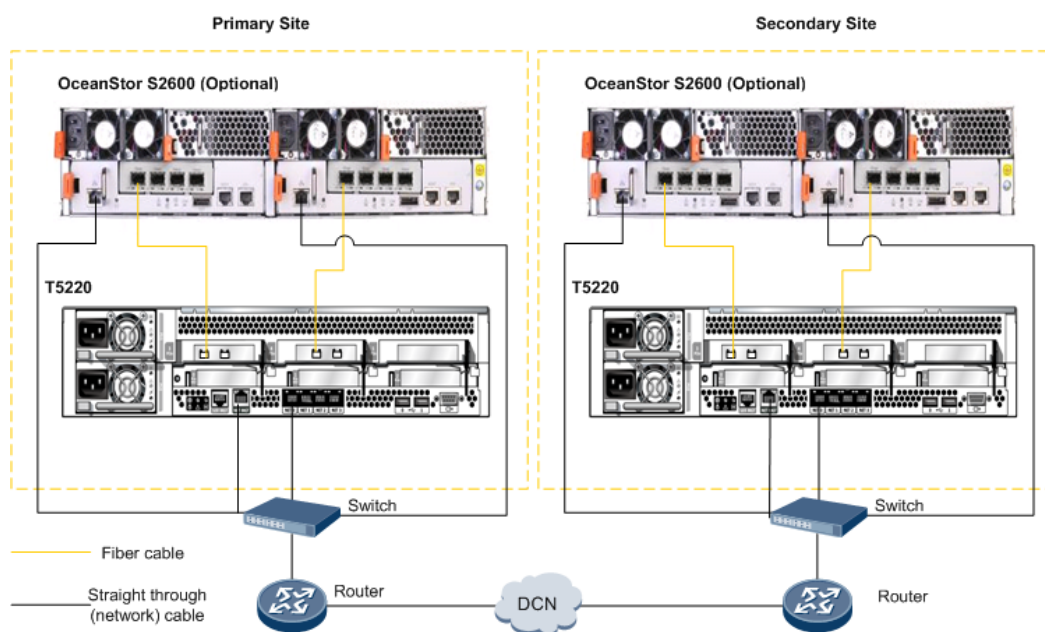


Figure 2-27 Hardware connection between the T5220 server and the OceanStor S3100

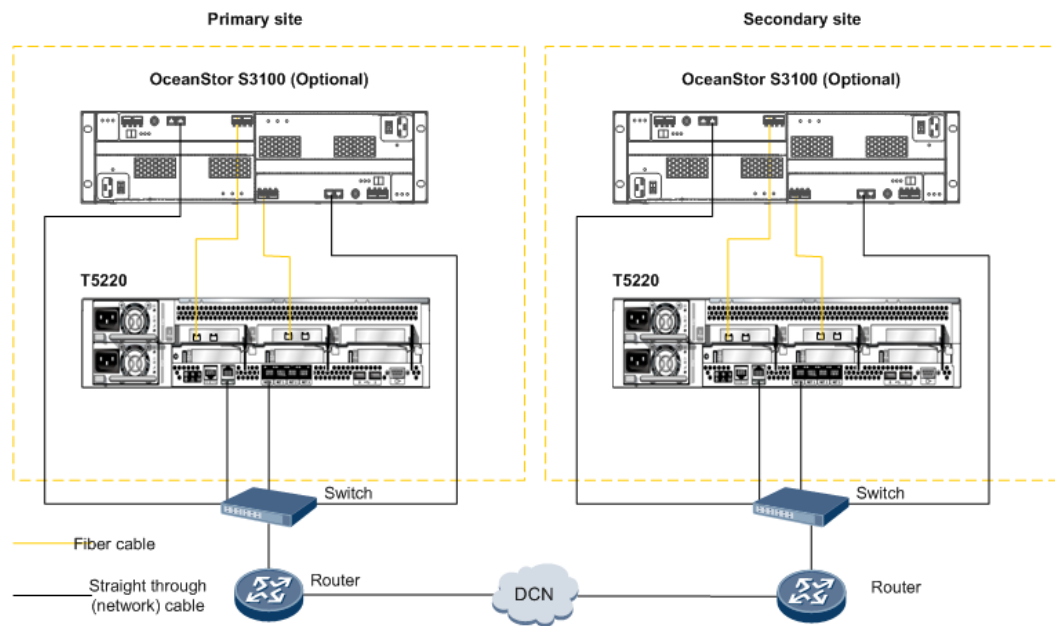
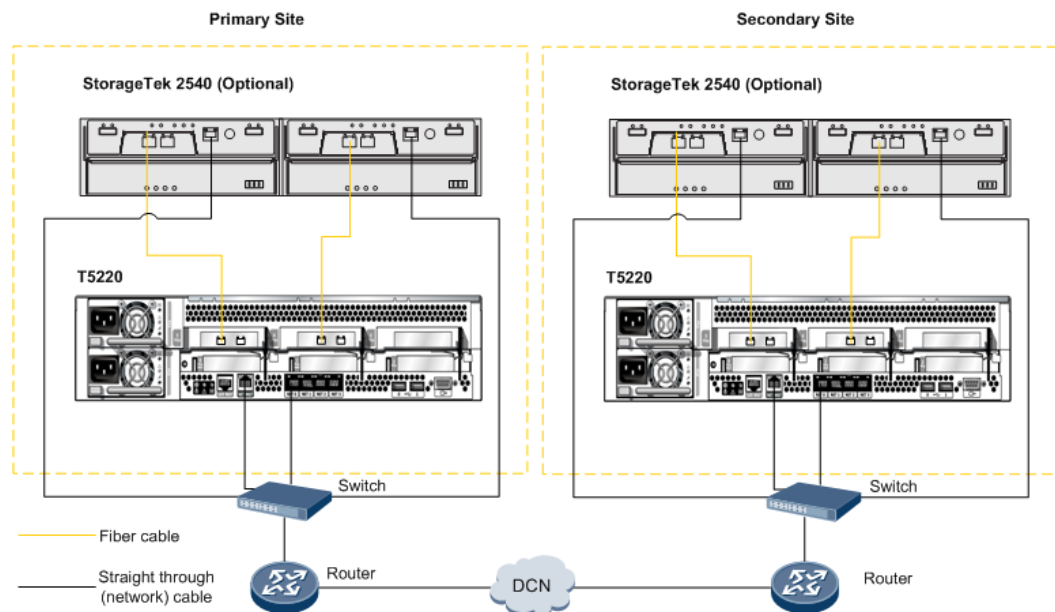


Figure 2-28 Hardware connection between the T5220 server and the StorageTek 2540



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

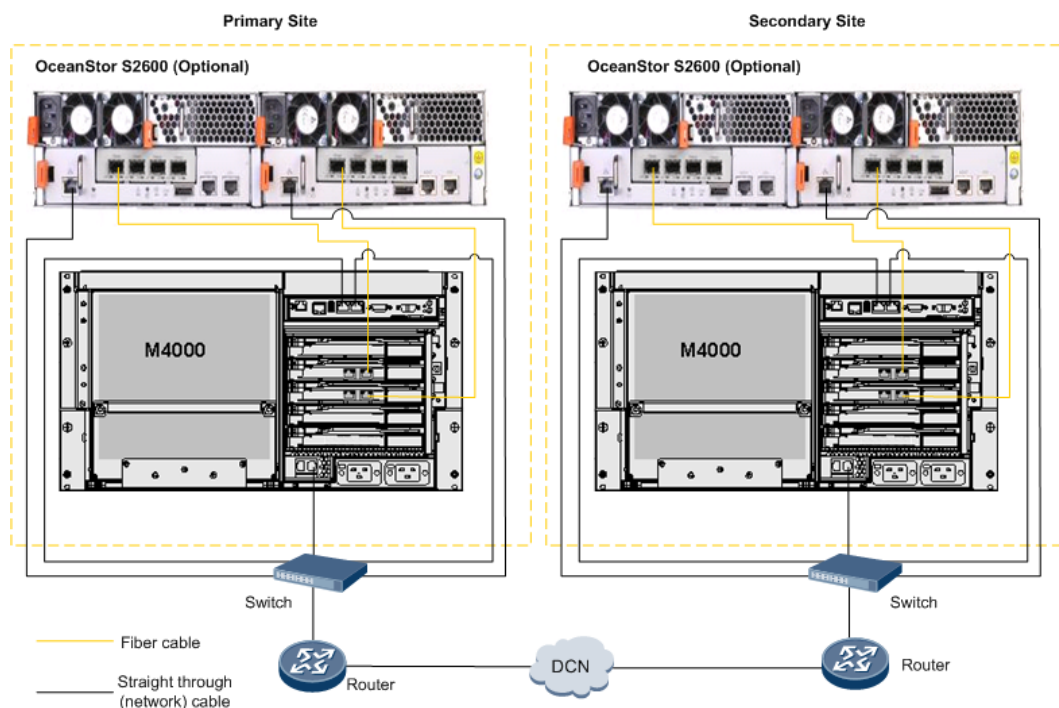
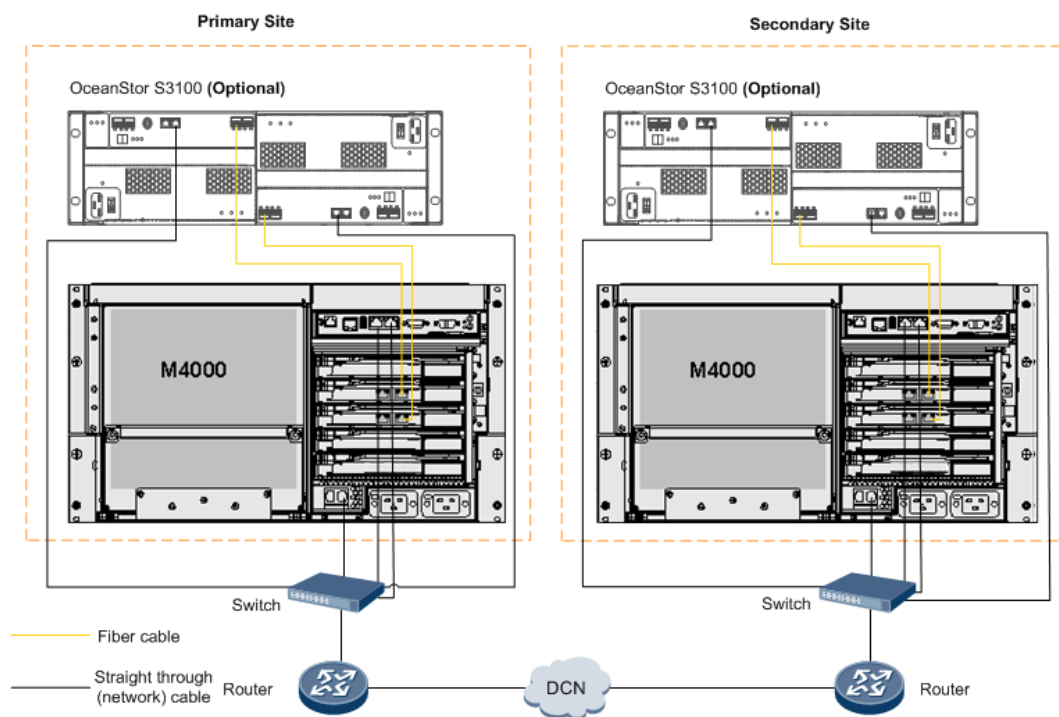
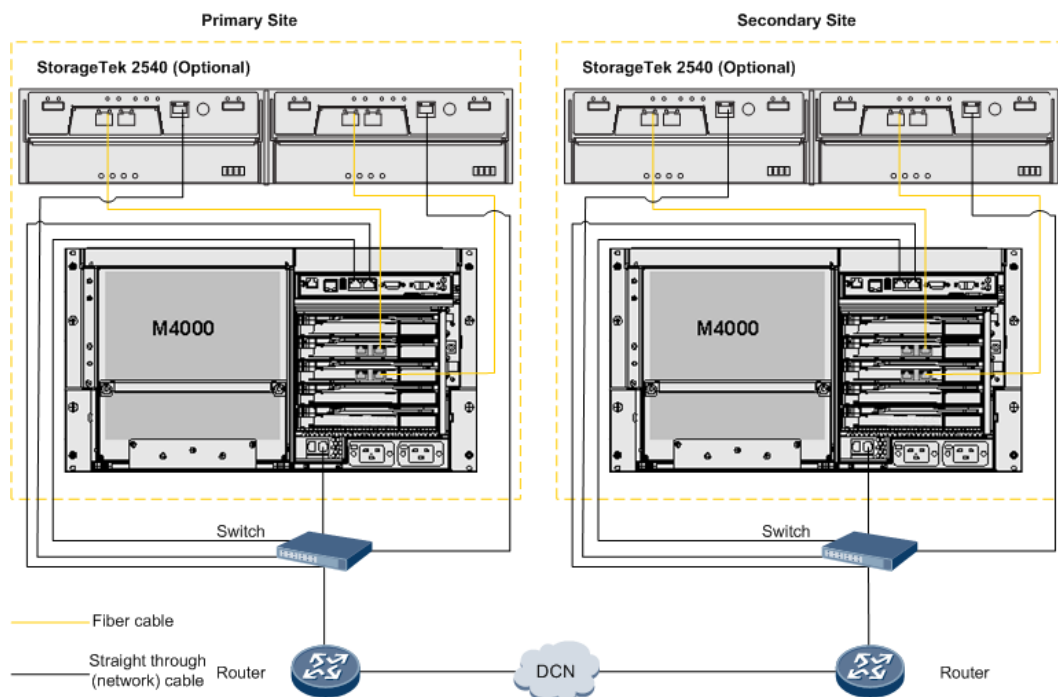
Figure 2-29 Hardware connection between the M4000 server and the OceanStor S2600**Figure 2-30** Hardware connection between the M4000 server and the OceanStor S3100

Figure 2-31 Hardware connection between the M4000 server and the StorageTek 2540



4 Check the plugs and sockets.

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

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

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

----End

2.5.1.5 Powering On a Server

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

T5220 Server

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

NOTE

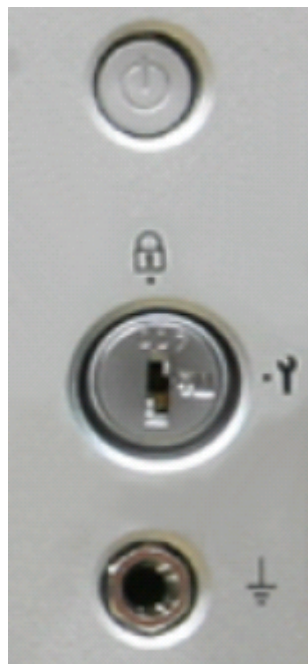
The power button is on the left of the server's front panel. It is labeled with , as shown in the following figure.

Figure 2-32 Power button of the T5220 server**NOTE**

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

M4000 Server

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

Figure 2-33 Power button of the M4000 server

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

 NOTE

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

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

Disk Arrays



CAUTION

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

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

2.5.1.6 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

2.5.1.7 Applying for a U2000 License

This topic describes how to apply for a U2000 license.

Context

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

The U2000 license is valid as long as it is bound to any of the server ESNs. To avoid applying for a new license due to replacing certain network interface cards (NICs), save all the ESNs to ensure proper use of the U2000 license.
- In a high availability system (Veritas hot standby) scheme, the primary and secondary sites share a U2000 license. The U2000 license file is bound to the ESNs of the primary

and secondary sites. When applying for a U2000 license, you must save the ESNs of the primary and secondary sites separately.

Procedure

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

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

NOTE

Make the following preparations:

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

```
# cd /opt
# tar xvf U2000version_ESN_solaris_SPARC.tar
```
 3. Run the following command to view the ESN:

```
# ./esn
```

Information similar to the following is displayed:

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

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

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

```
# . /export/home/nmsuser/.profile
```

```
# cd /opt/U2000/server/lbin
# ./esn
```

NOTE

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

Information similar to the following is displayed:

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

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

NOTE

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

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

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

----End

2.5.1.8 Checking System Installation

This topic describes how to check the installation of a high availability system (Solaris). Before modifying system parameters, you must ensure that the high availability system (Solaris) is installed and its version is correct.

Context

- During installation of the U2000 software, the OS user **nmsuser** is created automatically. The **nmsuser** user is used to regularly maintain a U2000.
- During installation of the U2000 software, only one default NMS user, that is, user **admin**, is provided. The **admin** user is the administrator of the U2000 and has the highest rights of the U2000. The default password of user **admin** is blank. You must change the default password during first-time login.

Procedure

- 1 Log in to the OSs of the servers of the primary and secondary sites as the **root** user.
- 2 To view the U2000 installation path `/opt/U2000` and the Sybase software installation path `/opt/sybase` for the primary and secondary sites, run the following commands:

```
# cd /opt
# ls
```

Information similar to the following is displayed:

```
HWENGR
HWICMR
sybase
U2000
...
```

- If the displayed information contains **U2000** and **Sybase**, the U2000 has been installed.
- If the displayed information does not contain **U2000**, install a U2000 according to the *iManager U2000 High Availability System (Veritas) Software Installation Guide (Solaris)*.

3 To check the U2000 version, run the following commands:

```
# cd /opt/U2000/server/etc/conf
# cat imap.cfg
```

Information similar to the following is displayed:

```
...
VER = U2000V100R002C01
```

The last line of the displayed information shows the U2000 version. If the version information does not meet the actual requirement, uninstall the U2000 and obtain the correct software version to install the U2000 again. For details, see the *iManager U2000 High Availability System (Veritas) Software Installation Guide (Solaris)*.

4 To check whether disk arrays are properly mounted, run the following command:

 NOTE

If no disk array has been configured, skip this step.

```
# df -h
```

Information similar to the following is displayed:

Filesystem	size	used	avail	capacity	Mounted on
/dev/vx/dsk/bootdg/rootvol	15G	4.6G	10G	32%	/
/devices	0K	0K	0K	0%	/devices
ctfs	0K	0K	0K	0%	/system/contract
proc	0K	0K	0K	0%	/proc
mnttab	0K	0K	0K	0%	/etc/mnttab
swap	42G	1.8M	42G	1%	/etc/svc/volatile
objfs	0K	0K	0K	0%	/system/object
sharefs	0K	0K	0K	0%	/etc/dfs/sharetab
fd	0K	0K	0K	0%	/dev/fd
/dev/vx/dsk/bootdg/var	15G	1.4G	13G	10%	/var
swap	42G	88K	42G	1%	/tmp
swap	42G	40K	42G	1%	/var/run
swap	42G	0K	42G	0%	/dev/vx/dmp
swap	42G	0K	42G	0%	/dev/vx/rdmp
/dev/vx/dsk/bootdg/opt	21G	2.9G	18G	15%	/opt
/dev/odm	0K	0K	0K	0%	/dev/odm
/dev/vx/dsk/datadg/lv_database	20G	20M	19G	1%	/opt/sybase
/dev/vx/dsk/datadg/lv_nms_data	89G	64M	88G	1%	/opt/sybase/data
/dev/vx/dsk/datadg/lv_nms	197G	64M	195G	1%	/opt/U2000
/dev/vx/dsk/datadg/lv_backup	197G	64M	195G	1%	/opt/backup
/dev/vx/dsk/datadg/lv_ftproot	295G	64M	292G	1%	/ftproot

Pay attention to the lines that contain **datadg**.

- If the values of **Mounted on** for the lines that contain **datadg** are the same as the preceding command output, disk arrays are properly mounted.
- If the values of **Mounted on** for the lines that contain **datadg** are different from the preceding command output, disk arrays are not properly mounted. Contact Huawei engineers to locate the fault.

5 Do as follows to check the Veritas version and patch information:

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

```
# pkginfo -l VRTSvxvm
```

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

```
PKGINST: VRTSvxvm
NAME: Binaries for VERITAS Volume Manager by Symantec
CATEGORY: system
ARCH: sparc
VERSION: 5.1,REV=10.06.2009.22.05
BASEDIR: /
VENDOR: Symantec Corporation
DESC: Virtual Disk Subsystem
PSTAMP: 5.1.002.000-5.1RP2-2010-08-27
INSTDATE: Nov 16 2010 02:09
HOTLINE: http://support.veritas.com/phonesup/phonesup_ddProduct_.htm
EMAIL: support@veritas.com
STATUS: completely installed
FILES:      898 installed pathnames
          37 shared pathnames
          110 directories
          384 executables
          364221 blocks used (approx)
```

Pay attention to information to the right of **PSTAMP**. If the information to the right of **PSTAMP** is not **5.1.002.000-5.1RP2-2010-08-27**, you must reinstall Veritas 5.1 or contact Huawei engineers.

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

```
# pkginfo -l VRTSvcs
```

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

```
PKGINST: VRTSvcs
NAME: Veritas Cluster Server by Symantec
CATEGORY: system
ARCH: sparc
VERSION: 5.1
BASEDIR: /
VENDOR: Symantec Corporation
DESC: Veritas Cluster Server by Symantec
PSTAMP: 5.1.002.000-5.1RP2-2010-08-26_19.00.00
INSTDATE: Nov 16 2010 02:17
STATUS: completely installed
FILES:      281 installed pathnames
          27 shared pathnames
           4 linked files
          60 directories
          102 executables
          234265 blocks used (approx)
```

Pay attention to information to the right of **PSTAMP**. If the information to the right of **PSTAMP** is not **5.1.002.000-5.1RP2-2010-08-26_19.00.00**, you must reinstall Veritas 5.1 or contact Huawei engineers.

6 To check disk group status, run the following command:

```
# vxdg list
```

Information similar to the following is displayed:

```
vxdg list
```

NAME	STATE	ID
rootdg	enabled	1281152223.12.primaster
datadg	enabled	1281151979.10.primaster

- If the value of **STATE** is **enabled**, the disk group status is correct.
- If the value of **STATE** is not **enabled**, the disk group does not function properly. Contact Huawei engineers to locate the fault.

7 To check disk status, run the following command:

```
# vxdisk list
```

Information similar to the following is displayed:

DEVICE	TYPE	DISK	GROUP	STATUS
c1t0d0s2	auto:sliced	disk01	rootdg	online
c1t1d0s2	auto:sliced	disk02	rootdg	online
c1t2d0s2	auto:sliced	disk03	datadg	online
c1t3d0s2	auto:sliced	disk04	rootdg	online
c1t4d0s2	auto:sliced	disk05	rootdg	online
c1t5d0s2	auto:sliced	disk06	datadg	online

NOTE

The equipment names in the **DEVICE** column may be different from those displayed on the terminal according to the actual situation of the workstation. Here, six hard disks are taken as an example.

- If the value of **STATUS** is **online**, the disk status is correct.
- If the value of **STATUS** is not **online**, the disk does not function properly. Contact Huawei engineers to locate the fault.

8 To check disk volume status, run the following command:

```
# vxprint -v
```

Information similar to the following is displayed:

Disk group: rootdg

TY	NAME	ASSOC	KSTATE	LENGTH	PLOFFS	STATE	TUTILO	PUTILO
v	backup	fsgen	ENABLED	161493120	-	ACTIVE	-	-
v	home	fsgen	ENABLED	4212864	-	ACTIVE	-	-
v	opt	fsgen	ENABLED	283116672	-	ACTIVE	-	-
v	rootvol	root	ENABLED	41945472	-	ACTIVE	-	-
v	swapvol	swap	ENABLED	33560448	-	ACTIVE	-	-
v	var	fsgen	ENABLED	41945472	-	ACTIVE	-	-

Disk group: datadg

TY	NAME	ASSOC	KSTATE	LENGTH	PLOFFS	STATE	TUTILO	PUTILO
v	lv_nms_data	datarvg	ENABLED	83886080	-	ACTIVE	-	-
v	srl_vol	datarvg	ENABLED	2097152	SRL	ACTIVE	-	-

NOTE

The displayed information varies with the data of the hard disks that are actually configured.

- If more than two hard disks are configured, the two disk groups (rootdg and datadg) are available.
- If only two disks are configured, only one disk group (datadg) is available.

Reference Standards

- All disk volumes used by the U2000 exist. Currently, the U2000 uses the following disk volumes: backup, home, opt, rootvol, swapvol, var, lv_nms_data, and srl_vol.
- The value of **KSTATE** must be **ENABLED** for all disk volumes.
- The value of **STATE** must be **ACTIVE** for all disk volumes.

If disk volume status does not meet the preceding requirements, run the following command to record details about all disk volumes, and contact Huawei local office or customer service center in time according to warranty information.

```
# vxprint -l disk volume name
```

9 To check whether the replication between the primary and secondary sites is normal, run the following command on the primary site:

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

Information similar to the following is displayed:

```

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

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

```

If the value of **Replication status** is **replicating (connected)**, the replication is normal.

----End

2.5.2 Loading or Updating a License File

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.

2.5.2.1 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.

2.5.2.2 Loading a U2000 License

This topic describes how to load a U2000 license. This topic describes how to install a U2000 license. Before using a U2000, you must load a U2000 license.

2.5.2.1 Updating a Veritas License

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

Prerequisite

The formal Veritas license must be obtained.

Context

NOTE

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

Procedure

- 1 Log in to the OS as the **root** user.
- 2 To back up all the license files in the **/etc/vx/licenses/lic** path, run the following commands:

```
# mkdir /export/home/licenses  
# mv /etc/vx/licenses/lic/*.vxlic /export/home/licenses
```
- 3 To access the path where the script for updating licenses is stored, run the following command:

```
# cd /opt/VRTS/bin
```
- 4 To update the VxVM license, run the following command:

```
# ./vxlicinst
```

The following information is displayed:

Symantec License Manager vxlicinst utility version 3.02.33.0

Copyright (C) 1996-2007 Symantec Corporation. All rights reserved.

Enter your license key :

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



NOTE

- X indicates the a letter or digit of a license key.
- The information about the demo or formal license that is newly obtained is contained in the license file.
- The new licenses include VRTS STORAGE FOUNDATION STANDARD, VRTS VOLUME REPLICATOR OPTION, and VRTS CLUSTER SERVER HA/DR.

- 6 Repeat step 4, and then enter the new license key of VRTS VOLUME REPLICATOR OPTION.
- 7 Repeat step 4, and then enter the new license key of VRTS CLUSTER SERVER HA/DR.

- 8 To check whether the updated license takes effect, run the following command:

```
# /opt/VRTSvlic/bin/vxlicrep
```

Check whether the license key of the associated component is updated and whether the authentication date of the component is correct.

- 9 To stop the VCS service, run the following commands:

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

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

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

A message similar to the following will be displayed:

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



NOTE

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

- 11 To restart the OS, run the following commands:

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

----End

2.5.2.2 Loading a U2000 License

This topic describes how to load a U2000 license. This topic describes how to install a U2000 license. Before using a U2000, you must load a U2000 license.

Prerequisite

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

Context

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

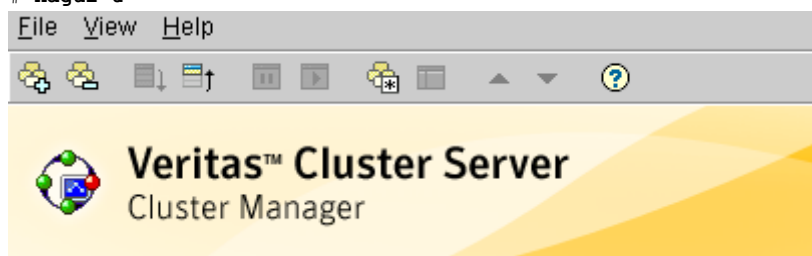
Two methods are available for loading a U2000 license.

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

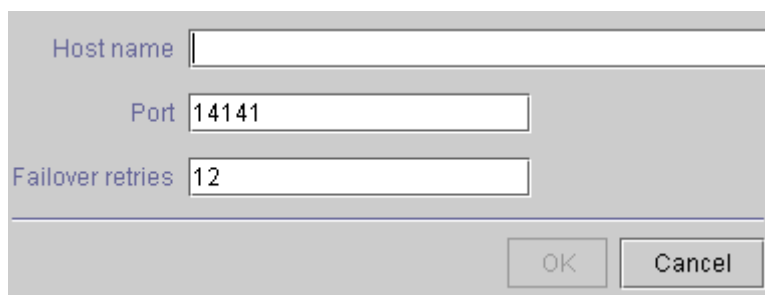
Procedure

- 1 On the primary site, do as follows to start U2000 processes:
 1. Run the following command as the **root** user to start the VCS client:

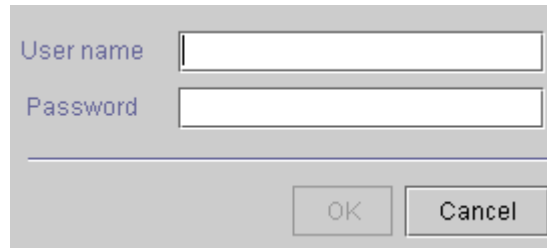
```
# hagui &
```



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



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



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

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

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

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

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

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

- 3 Load the U2000 license.

Method one: Use commands to load the license.

1. Send the license file to the U2000 installation path **/export/home/nmsuser** of the primary site in ASCII mode by FTP as the **root** user. Details are as follows:
 - a. Log in to the PC where the license file is stored.
 - b. Choose **Start** > **Run**. In the **Run** dialog box, enter **ftp system IP address of the server** and click **OK**. An FTP connection is established and a CLI is displayed.
 - c. In the CLI, enter **nmsuser** as the name of the OS user.
User (IP_address: (none)) :**nmsuser**
 - d. Enter the password for the **nmsuser** user.
Password:
 - e. Set the format of the file to be transferred using FTP to ASCII.
ftp> **ascii**
 - f. Navigate to the path on the computer where the license file is stored.
ftp> **lcd PC_directory**
 - g. Navigate to the **/export/home/nmsuser** directory.
ftp> **cd /export/home/nmsuser**
 - h. Run the **put** command to upload the license file to the server.
ftp> **put "License_file_name"**
 - i. To exit the FTP program, run the following command:
ftp> **quit**
2. Do as follow to make the license take effect:
 - a. log in to the OS of the U2000 server as the **nmsuser** user on the primary site.

- b. To update the U2000 license file, run the following commands:

```
$ cd /export/home/nmsuser
$ updateLicense -file License_file_name
```

Information similar to the following is displayed:

state	product	feature	item	name	old
value	new value				
no change:	U2000	COMMON	LSW1CAPA01	Client	
500	500				
no change:	U2000	COMMON	LSW1CAPA01	Client	
1	1				
no change:	U2000	COMMON	LSW1FMCLT01	Alarm Export	
1	1				
no change:	U2000	COMMON	LSW1RENOTI01	Client	
1	1				

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

- c. Enter **Y**, and then press **Enter**.
3. Send the license file to the `/opt/U2000/server/etc/conf/license` path on the secondary site in ASCII mode by FTP as the **nmsuser** user. For details, [3.1](#).

Method two: Load the license in the GUI.

Update the license on the primary site.

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

NOTE

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

Update the license on the secondary site.

- On the primary site, log in to the VCS client. For details, see [1.1](#).
- Right-click the AppService resource group and choose **Switch to > Remote switch** from the shortcut menu.
- Select the clusters and systems to be switched.
- Click **OK**.
- In the **Confirm** dialog box, click **Yes** to switch U2000 services to the secondary site.
- 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

2.5.3 Modifying System Parameters

This topic describes how to modify the host name and IP address, route, time and time zone, component, instance, and passwords of the OS and database users according to the collected planning information.



CAUTION

- In the scenario where the servers delivered by Huawei have been preinstalled, change the host names and IP addresses for the servers of the primary and secondary sites. Connect the primary and secondary sites to ensure that they communicate with each other normally.
- After connecting the primary and secondary sites, modify the associated parameters according to the planning information.

Parameter	Operation Method
Host name and IP address (Including route)	A.9.14 How to Change the IP Address and Host name for the High Availability System (Solaris)
Time and time zone	D.4.7 Setting the System Time and Time Zone
Connecting the primary and secondary sites	D.6.1 Establishing the HA Relationship Between the Primary and Secondary Sites
Component and instance	● To add a component, see D.4.1 Adding a Component. ● To delete a component, see D.4.2 Deleting a Component. ● To add a instance, see D.4.3 Adding an Instance. ● To delete a instance, see D.4.5 Deleting an Instance. ● To modify an instance name or a piece of remarks, see D.4.6 Changing the Name and Remarks of an Instance.
Password for the database supper user	D.4.8 Changing the Password of the Administrator of the Database
Password for the database user NMSuser	D.4.9 Changing the Password of the User of the Database
Password for the MSuite	D.3.4 Changing the Password of the MSuite

Parameter	Operation Method
Password for the OS user root	In a CLI, run the following command to change the password for the root user: # passwd root New Password: enter the new password of root Re-enter new Password: Re-enter new password of root
Password for the OS user nmsuser	In a CLI, run the following command to change the password for the nmsuser user: # passwd nmsuser New Password: enter the new password of nmsuser Re-enter new Password: Re-enter new password of nmsuser

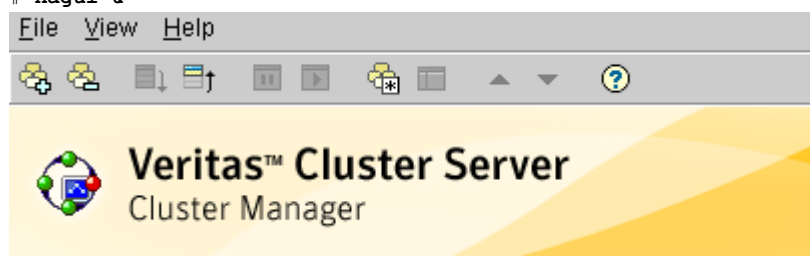
2.5.4 Starting a High Availability System (Solaris)

This topic describes how to start a U2000 high availability system. Starting a U2000 high availability system includes starting the U2000 server and logging in to a U2000 client.

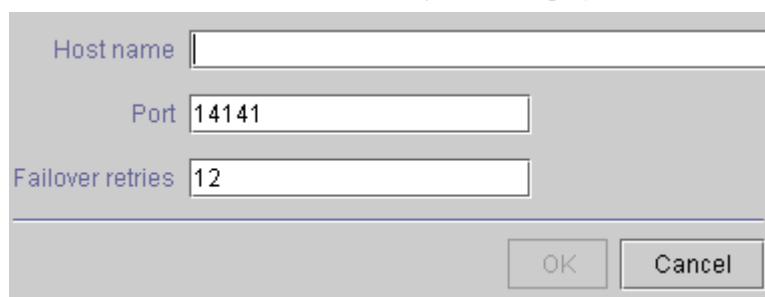
Procedure

- 1 Log in to the OS of the server on the active site as the **root** user.
- 2 To start a VCS client, run the following command:

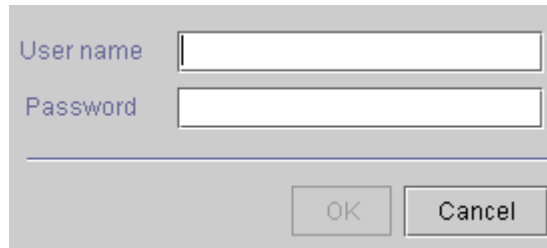
```
# hagui &
```



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



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



- 5 Enter the default user name **admin** and the initial password **password** for the VCS client. Then, click **OK**.
- 6 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.
- 7 In the dialog box that is displayed, click **Yes**.
 - 8 View the running status of each process through the System Monitor as user **nmsuser** to log in to the server GUI, as follows:



CAUTION

If you cannot log in to the GUI of the server OS, do as follows to view the process status:

1. Run the **su - nmsuser** command to switch to the **nmsuser** user.
2. Run the **svc_adm -cmd status** command to view the process status.

-
1. Log in the OS as the **nmsuser** user.
 2. On the desktop of the OS, double-click the **U2000 System Monitor** shortcut icon.
 3. In the dialog box that is displayed, enter a 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**.

- If the client and server applications are on the same host and the server uses the **SSL** mode, then the client can use the **Common** or **SSL** mode. The client can only use the **Common** mode if the server uses the **Common** mode.
- If the client and server applications are not on the same host, the client can log in to the server only when it uses the same mode as the server.

For details about how to set the communication mode on the U2000 server for a high availability system (Solaris), see [A.9.54 How to Set the Communication Mode of the Server in a High Availability System \(Solaris\)?](#).

If the U2000 processes with the startup mode of automatic have started properly, the U2000 functions properly.

If a process is not started, right-click the process and choose **Start the Process** from the shortcut menu.

If the U2000 does not function properly, contact Huawei engineers.

9 Log in to a U2000 client.

If the U2000 server is equipped with a monitor, directly log in to a U2000 client from the server. If the U2000 server is not equipped with any monitor, log in to the server using the remote desktop control software.

 NOTE

You are unable to log in to a U2000 client from the U2000 server if you cannot login to the server in GUI mode. In this case, log in to the server using an independent client. For details, see [5 Commissioning the Communication Between the Server and an Independent Client](#).

1. Access the **Java Desktop System, Release 3** session process of the OS as the **nmsuser** user.

 NOTE

If the **Solaris Registration Wizard** dialog box is displayed, click the **Run the Solaris software without registering** option button and then click **Next**. In the dialog box that is displayed, click **Never Register**.

2. Log in to the U2000 client.
 - a. On the desktop of the **Java Desktop System, Release 3**, double-click the **U2000 Client** shortcut icon.
 - b. In the dialog box that is displayed, enter a U2000 user name and password to access the main window of the client.
 - c. If you are required to log in to the U2000 server using another client, set the ACL login control right for the exact server where the client resides in the main window of the client. For details, see the Help.

----End

2.6 Modifying the Parameters of the High Availability System (SUSE Linux-Distributed)

This topic describes how to modify the parameters of the high availability system (SUSE Linux-distributed), including the host name and IP address, route, time and time zone, subsystem, instance, and user password.

[2.6.1 Preparing for the Modification of System Parameters](#)

This topic describes how to prepare for the modification of high availability system (SUSE Linux-distributed) parameters. Before modifying system parameters, you must get familiar with the networking structure and environment requirements, collect planning information, check hardware connections, power on a server, apply for a Veritas license and U2000 license, and check system installation.

[2.6.2 Loading or Updating a License File](#)

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.

[2.6.3 Modifying System Parameters](#)

This topic describes how to modify the host name and IP address, route, time and time zone, component, instance, and passwords of the OS and database users according to the collected planning information.

[2.6.4 Starting the High Availability System \(SUSE Linux-Distributed\)](#)

This topic describes how to start the high availability system. Starting the U2000 high availability system includes starting the U2000 server and logging in to the U2000 client.

2.6.1 Preparing for the Modification of System Parameters

This topic describes how to prepare for the modification of high availability system (SUSE Linux-distributed) parameters. Before modifying system parameters, you must get familiar with the networking structure and environment requirements, collect planning information, check hardware connections, power on a server, apply for a Veritas license and U2000 license, and check system installation.

[2.6.1.1 Networking Structure](#)

This topic describes the networking structure of a high availability system (SUSE Linux-distributed). Before commissioning a high availability system (SUSE Linux-distributed), you must get familiar with the networking structure of the high availability system (SUSE Linux-distributed).

[2.6.1.2 Environment Requirements](#)

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

[2.6.1.3 Collecting Planning Information](#)

This topic describes how to collect planning information. Before commissioning 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.

[2.6.1.4 Checking Hardware Connections](#)

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

2.6.1.5 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.

2.6.1.6 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.

2.6.1.7 Applying for a U2000 License

This topic describes how to apply for a U2000 license.

2.6.1.8 Checking System Installation

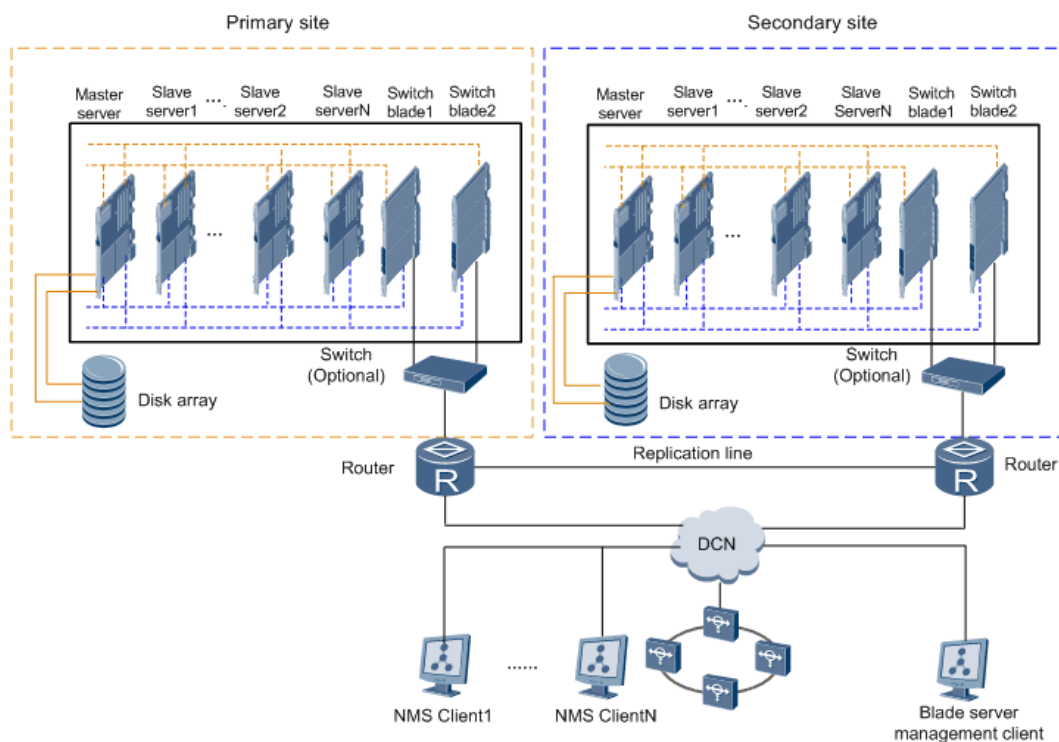
This topic describes how to check the installation of a high availability system (SUSE Linux-distributed). Before modifying system parameters, you must ensure that the high availability system (SUSE Linux-distributed) has been installed and its version is correct.

2.6.1.1 Networking Structure

This topic describes the networking structure of a high availability system (SUSE Linux-distributed). Before commissioning 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 2-34 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 a 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.

2.6.1.2 Environment Requirements

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

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

Table 2-45 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 $3 \times 10^4/\text{m}^3$.
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. The bandwidth between primary and secondary sites must be 2 Mbit/s at least.

2.6.1.3 Collecting Planning Information

This topic describes how to collect planning information. Before commissioning 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 planning 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 2-46 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 2-47 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 2-47 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 - IBM blade server: 192.168.70.125/255.255 . 255.0/192.168.70.1	
		Primary controller IP address	129.9.1.103/255 . 255.255.0/129.9 .1.254	
	Disk array	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 - IBM blade server: 192.168.70.126/255.255 . 255.0/192.168.70.1	
		Primary controller IP address	129.9.1.106/255 . 255.255.0/129.9 .1.254	
	Disk array	Secondary controller IP address	129.9.1.107/255 . 255.255.0/129.9 .1.254	

Table 2-48 shows the planning of system IP addresses of the master and slave servers on the primary and secondary sites.

Table 2-48 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: 129.9.1.30/255.255.0/129.9.1.254 ● slave server: 129.9.1.31/255.255.0/129.9.1.254	
	Private network segment	192.168.100.0	
Secondary Site	System network interface	eth0	
	System IP address	● master server: 129.9.1.40/255.255.0/129.9.1.254 ● slave server: 129.9.1.41/255.255.0/129.9.1.254	
	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 2-49 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 2-50 Time zone and time list

Item	Example	Plan
Time zone	PRC Asia > Shanghai	
Time	14:00	

Table 2-51 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 2-52 Quantity list of configured components and instances

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

Table 2-53 Installation path list

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

2.6.1.4 Checking Hardware Connections

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

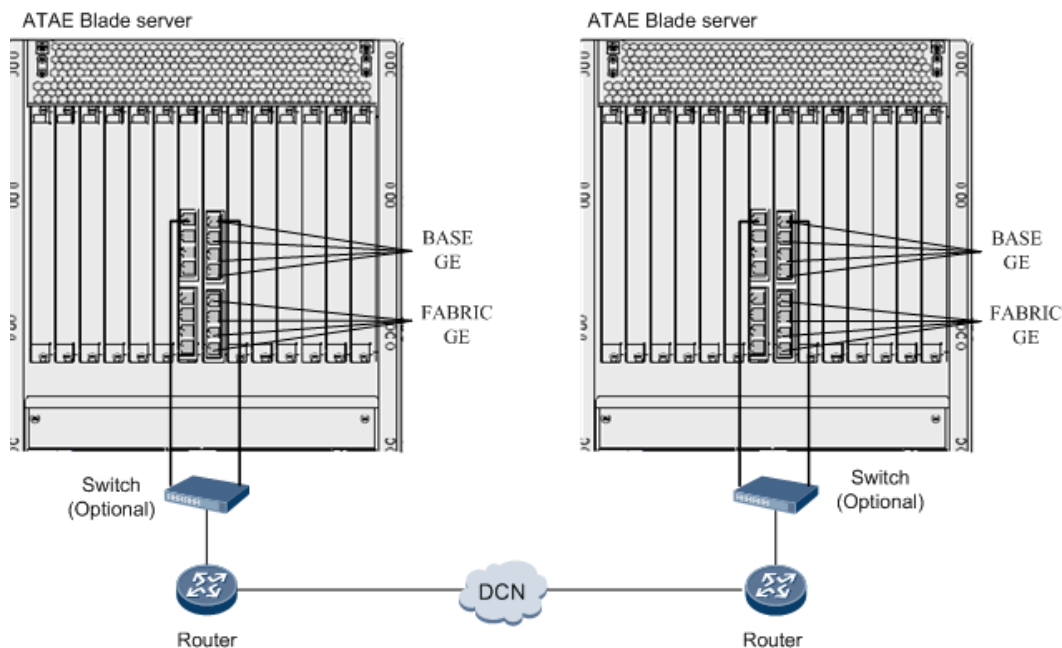
Prerequisite

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

Procedure

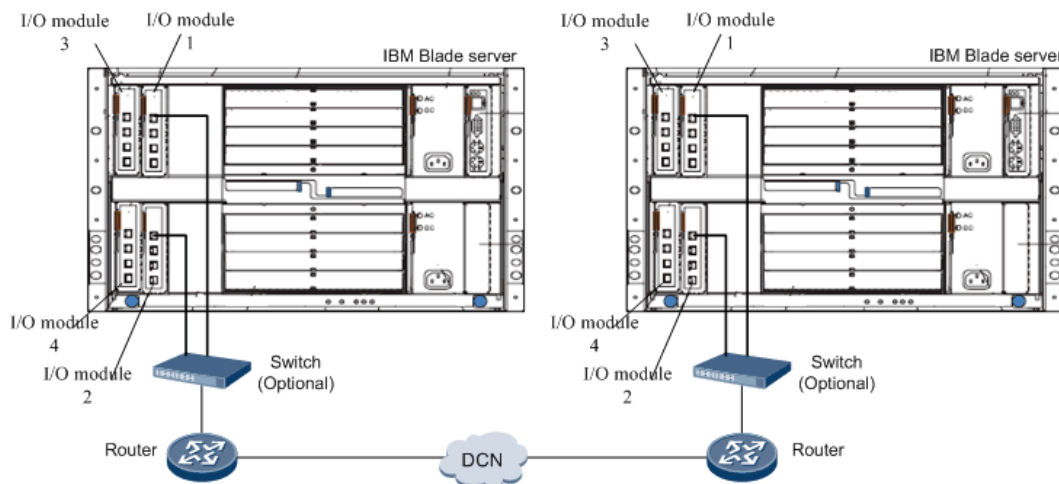
- 1 Ensure that the power cables and ground wires for all components are tightly connected and in good contact and that the polarities are properly placed.
- 2 Ensure that all cables are bundled and free of visible damage.
- 3 Check whether the card is in a correct slot of a subrack.
During U2000 installation, a label is attached to each card to identify the associated slot.
You must insert a card into a proper slot.
- 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 2-35 Connecting the ATAE blade server to the public network through the switching board



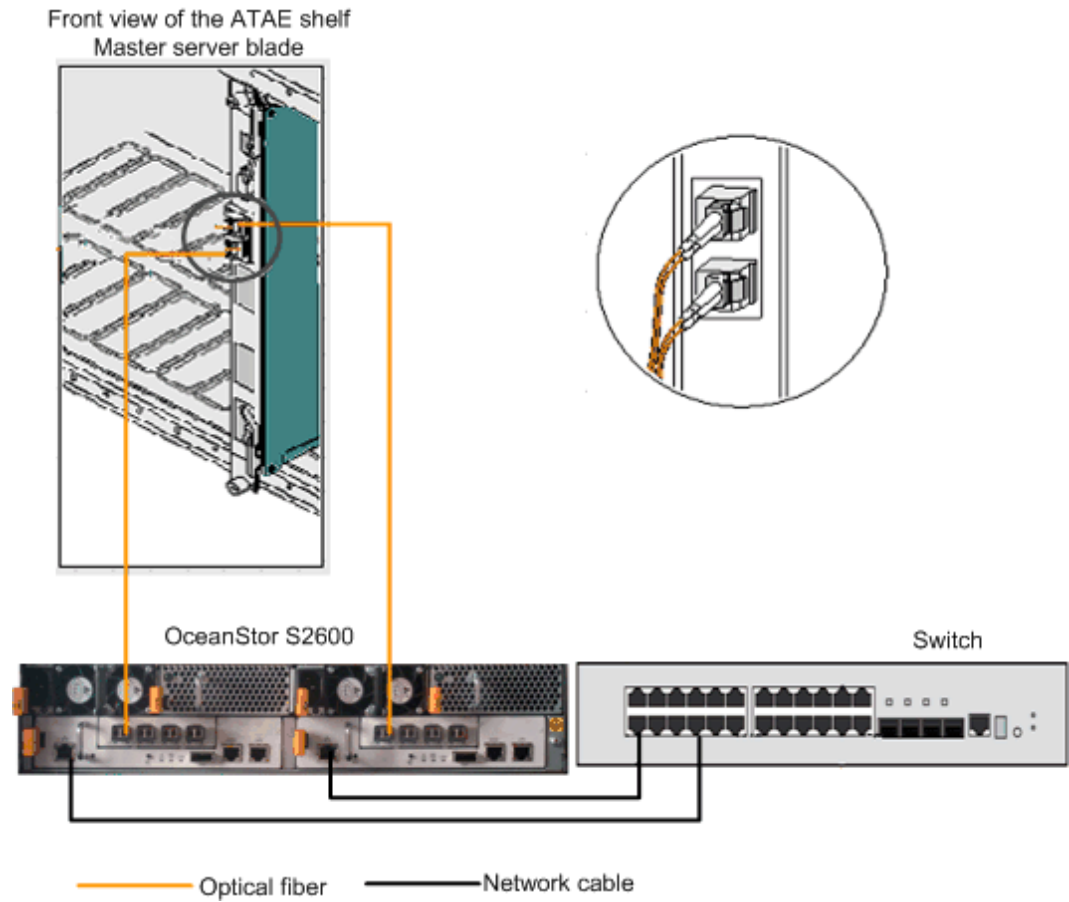
- The IBM blade server is connected to the external network through I/O module 1 or I/O module 2. The following figure shows how to connect the cables.

Figure 2-36 Connecting the IBM blade server to the public network through the switching board

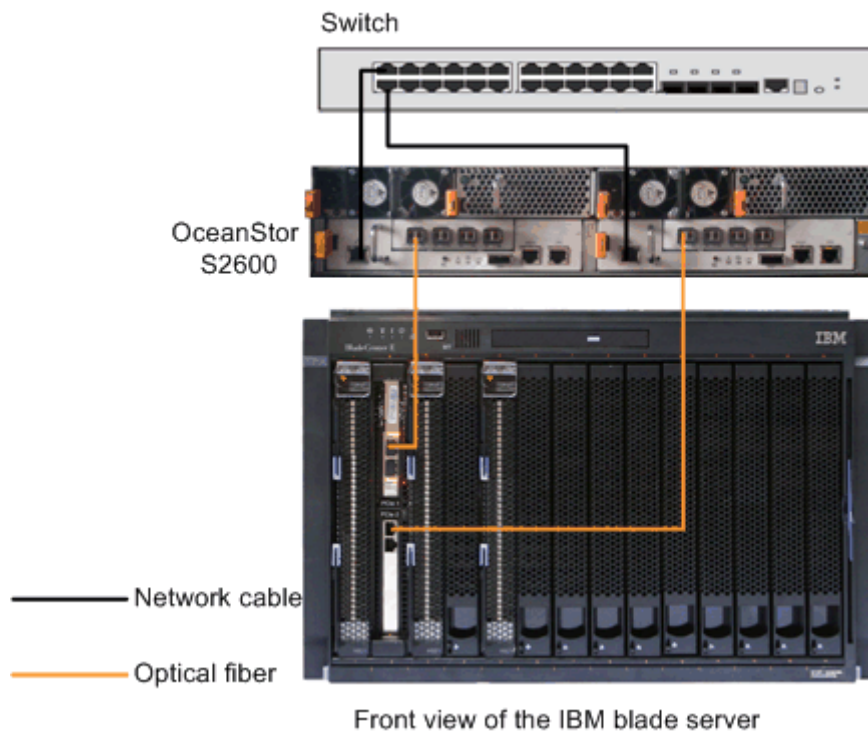


- 5 Check the connection cables of blade server and the disk array against the hardware connection diagram.
 - The ATAE blade server is connected to a disk array using fibers, as shown in the following figure.

Figure 2-37 Diagram of the connection between the ATAE blade server and a disk array

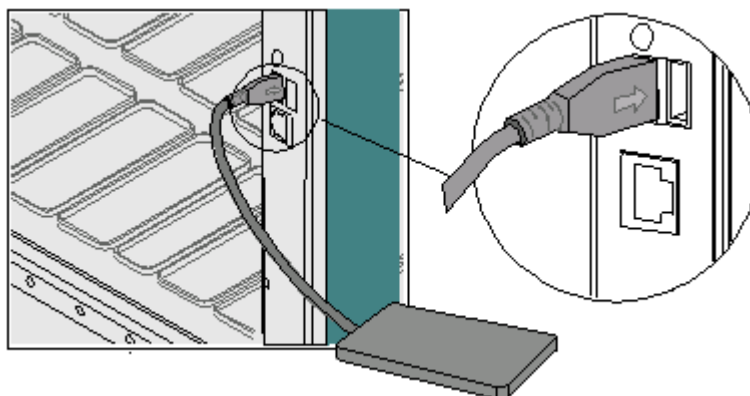


- The IBM blade server is connected to a disk array using fibers, as shown in the following figure.

Figure 2-38 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 2-39 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

2.6.1.5 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.

2.6.1.6 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

2.6.1.7 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

2.6.1.8 Checking System Installation

This topic describes how to check the installation of a high availability system (SUSE Linux-distributed). Before modifying system parameters, you must ensure that the high availability system (SUSE Linux-distributed) has been installed and its version is correct.

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 view the installation directory **/opt/U2000** of the U2000 and the installation directory **/opt/oracle** of the Oracle software of the primary and secondary sites:

```
# cd /opt
# ls
```

Information similar to the following is displayed:

```
HWENGR
HWICMR
oracle
U2000
...
```

- If the displayed information contains **U2000** and **oracle**, it indicates that the U2000 is installed.
 - If the U2000 is not installed, install it according to the *iManager U2000 High Availability System (Veritas) Software Installation Guide (SUSE Linux)*.
- 3 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. For details, see the *iManager U2000 High Availability System (Veritas) Software Installation Guide (SUSE Linux)*.

4 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/ftpoot
/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.

5 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.

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
```

```
VRTSvcssea-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.

6 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.

7 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.

8 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	TUTILO	PUTILO
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
```

9 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
```

----End

2.6.2 Loading or Updating a License File

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.

2.6.2.1 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.

2.6.2.2 Loading a U2000 License

This topic describes how to load a U2000 license. This topic describes how to install a U2000 license. Before using a U2000, you must load a U2000 license.

2.6.2.1 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  
# hstop -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

2.6.2.2 Loading a U2000 License

This topic describes how to load a U2000 license. This topic describes how to install a U2000 license. Before using a U2000, you must load 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 (_).

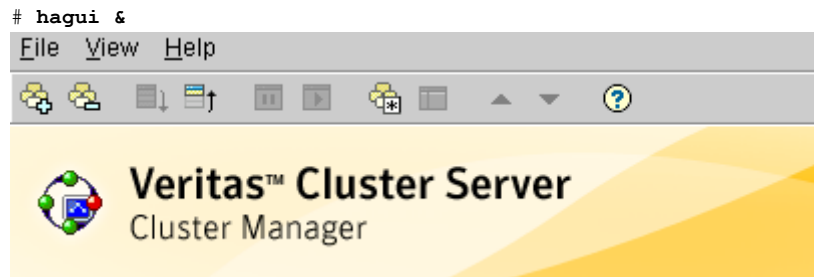
Context

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

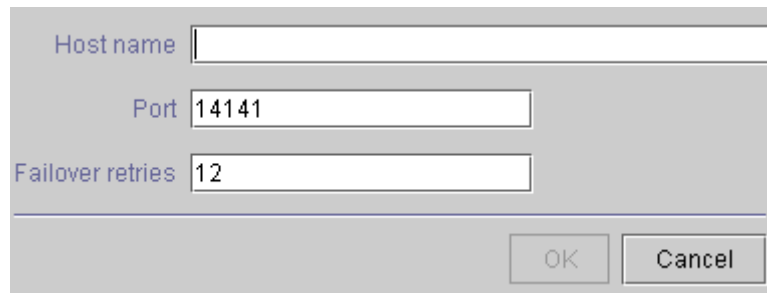
Procedure

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

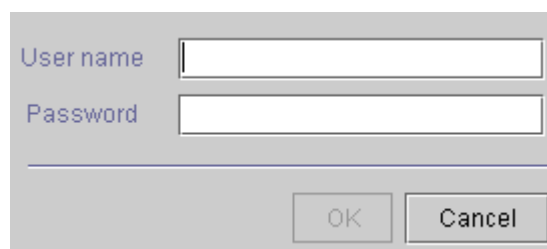
1. Run the following command as the **root** user to start the VCS client:



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

2.6.3 Modifying System Parameters

This topic describes how to modify the host name and IP address, route, time and time zone, component, instance, and passwords of the OS and database users according to the collected planning information.

**CAUTION**

- In the scenario where the servers delivered by Huawei have been preinstalled, change the host names and IP addresses for the servers of the primary and secondary sites. Connect the primary and secondary sites to ensure that they communicate with each other normally.
- After connecting the primary and secondary sites, modify the associated parameters according to the planning information.

Parameter	Operation Method
Host name and IP address (Including route)	A.9.15 How to Change the IP Address and Host Name of the High Availability System (SUSE Linux-Distributed)
Time and time zone	D.4.7 Setting the System Time and Time Zone
Connecting the primary and secondary sites	D.6.1 Establishing the HA Relationship Between the Primary and Secondary Sites
Component and instance	● To add a component, see D.4.1 Adding a Component. ● To delete a component, see D.4.2 Deleting a Component. ● To add a instance, see D.4.3 Adding an Instance. ● To delete a instance, see D.4.5 Deleting an Instance. ● To modify an instance name or a piece of remarks, see D.4.6 Changing the Name and Remarks of an Instance.
Password for the database supper user	D.4.8 Changing the Password of the Administrator of the Database
Password for the database user NMSuser	D.4.9 Changing the Password of the User of the Database
Password for the MSuite	D.3.4 Changing the Password of the MSuite
Password for the OS user root	In a CLI, run the following command to change the password for the root user: <pre># passwd root</pre> New Password: enter the new password of root Re-enter new Password: Re-enter new password of root
Password for the OS user nmsuser	In a CLI, run the following command to change the password for the nmsuser user: <pre># passwd nmsuser</pre> New Password: enter the new password of nmsuser Re-enter new Password: Re-enter new password of nmsuser

2.6.4 Starting the High Availability System (SUSE Linux-Distributed)

This topic describes how to start the high availability system. Starting the U2000 high availability system includes starting the U2000 server and logging in to the U2000 client.

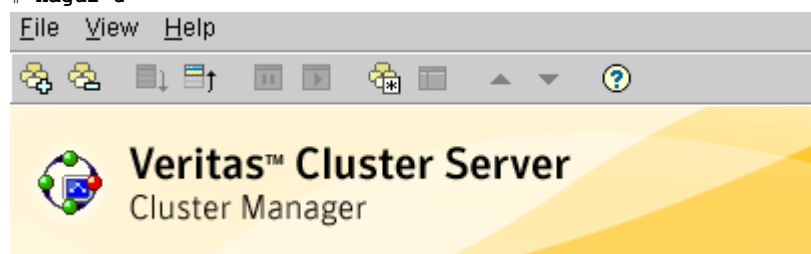
Prerequisite

The OSs of all the servers, including the master server and slave server, of the primary and secondary sites must be started.

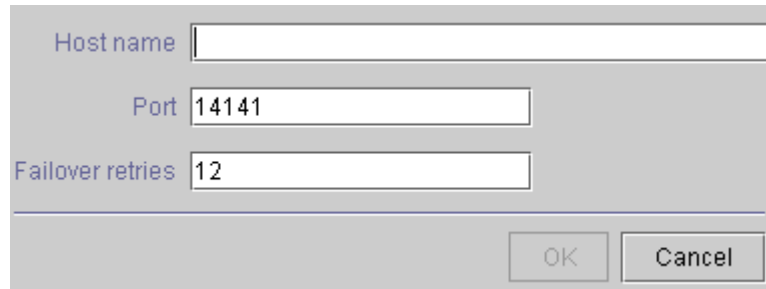
Procedure

- 1 Log in to the OS of the master server of the active site as the **root** user.
- 2 To start a VCS client, run the following command:

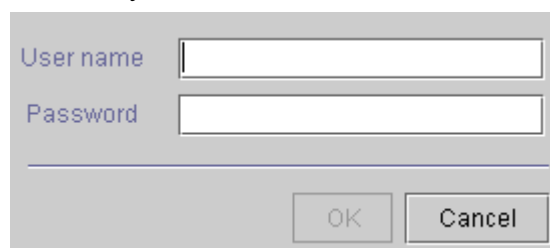
```
# haguì &
```



- 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 initial password **password** for the VCS client. Then, click **OK**.
- 6 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 Oracle process and the NMS server process.

 TIP

Click the **Resources** tab to view the start status of each resource.

Normally, on the **Status** tab page, **State** of the server of the active site in the **Group Status on Member Systems** area is **Online**, and **Status** in the **Resource Status** area is **Online on primary**.



NOTE

In actual configuration, use the actual host name.

7 Start the U2000 client.



NOTE

Because no U2000 client and System Monitor client are available in the SUSE Linux OS, log in to the independent U2000 client. For details, see [5 Commissioning the Communication Between the Server and an Independent Client](#).

----**End**

3 Configuring System NTP Solutions

About This Chapter

This topic describes the concepts and time synchronization principles related to NTP, NTP solution associated to each installation scheme, and detailed operation instructions.

[3.1 NTP Overview](#)

This topic describes the concepts related to NTP and provides brief description about time synchronization, including the purpose, overview, and principles of time synchronization.

[3.2 NTP Configuration Schemes](#)

This topic describes how to NTP configuration schemes. The NTP solutions vary according to the schemes adopted in the actual installation and deployment of the U2000. NTP configuration schemes for each installation scheme are described.

[3.3 NTP Configuration Task Set](#)

This topic describes how to configure the NTP server and client in the Windows OS, Solaris OS, and SUSE Linux OS respectively.

3.1 NTP Overview

This topic describes the concepts related to NTP and provides brief description about time synchronization, including the purpose, overview, and principles of time synchronization.

3.1.1 Purpose of Time Synchronization

Time synchronization aims to ensure the consistency in the time of the U2000 and NE.

3.1.2 Overview of Time Synchronization

This part describes the definition of time synchronization, the elements of time synchronization scheme, and the impact on system performance and other O&M features.

3.1.3 Time Synchronization Principle

This topic describes the time synchronization principle and hierarchical networking principle of the Network Time Protocol (NTP) and the Simple Network Time Protocol (SNTP).

3.1.1 Purpose of Time Synchronization

Time synchronization aims to ensure the consistency in the time of the U2000 and NE.

The networking is complex with a large number of NEs. Because the NEs on a network are operated and maintained in a uniform manner, the time of the NEs must be the same so that the U2000 manages the alarm and performance data reported by the NEs in good order.

Inaccurate time has the following disadvantages:

- If alarm time is inaccurate, you may misjudge the sequence of raised alarms, the interval between alarm raising and alarm reporting, and the associations between alarms.
- When the U2000 collects the statistics of performance data, inaccurate time decreases the precision of statistics.

Therefore, a set of non-human intervention measures (NTP Time Synchronization Plans) must be provided to change the time of the U2000 and NEs so that they remain synchronous.

3.1.2 Overview of Time Synchronization

This part describes the definition of time synchronization, the elements of time synchronization scheme, and the impact on system performance and other O&M features.

Definition of Time Synchronization

Time synchronization refers to the synchronization of the absolute time. The start time of a signal should be consistent with the Universal Time Coordinated (UTC).

Time synchronization aims to adjust the clock and time of the internal devices according to the received time.

Elements of Time Synchronization Scheme

More than two elements are involved in the time synchronization scheme: the method of time synchronization and the selection of time reference sources.

- Currently, the common method is to realize time synchronization according to the Network Time Protocol (NTP) and the Simple Network Time Protocol (SNTP).

- To ensure the correctness of the time reference in the entire network, you must select a standard time reference source. A common time reference source is the GPS satellite.

Impact on System Performance

If time synchronization is implemented in client/server mode described in the NTP protocol, the message frame between the NTP client and the NTP server is 128 bytes. Therefore, time synchronization does not affect the performance of network transmission. If a large amount of NTP clients request to connect to the NTP server at the same time, these connections consume more resources of the NTP server, such as the CPU and the memory of the NTP server. In this case, time synchronization may affect the server performance.

Therefore, if you use the NTP protocol to construct a time synchronization network, the number of NTP nodes under a NTP server cannot exceed 300. Otherwise, the performance of the NTP server may be affected. The interval for the time synchronization request of an NTP client should be 30 minutes or longer. In addition, you need reduce the probability of concurrent requests.

Impact on O&M

The time synchronization feature is vital in the O&M of network. It can benefit the other features in the following ways:

- Ensure the correctness and consistency of the time on the network management system (NMS) and NEs in the network. Time synchronization can affect the timeliness of fault reporting, correctness of fault information, and fault correlation analysis in fault management. If the NE time is inaccurate or the NE time is inconsistent with the NMS time, a mistake may be made when you identify or handle faults.
- Have a significant impact on the correctness of log recording, querying, displaying, auditing, and analyzing. If the time is inaccurate or the NE time is inconsistent with the NMS time, log records may be incorrect and log auditing is affected.
- Have a significant impact on recording, collecting, and analyzing performance data in performance management. If the time is inaccurate or the NE time is inconsistent with the NMS time, this leads to inaccuracy of the time to record the NE performance data and invalidation of the performance data.
- Have a significant impact on the services such as call tracing and problem identifying. If the time is inaccurate or the NE time is inconsistent with the NMS time, the call tracing service may fail.

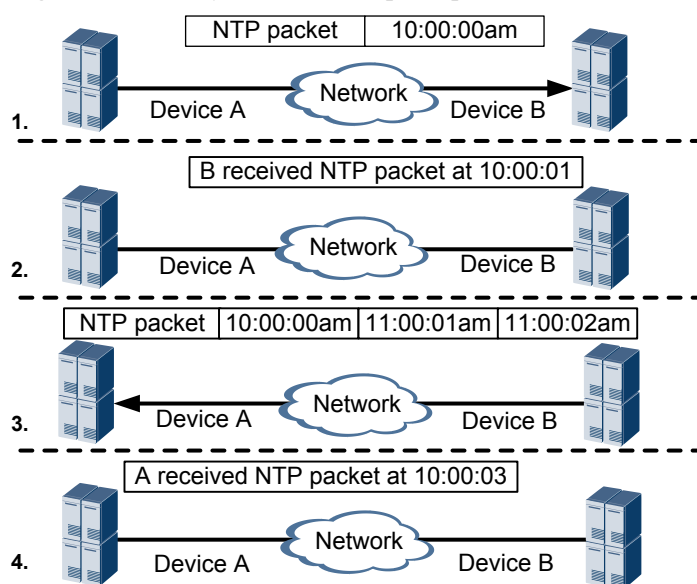
3.1.3 Time Synchronization Principle

This topic describes the time synchronization principle and hierarchical networking principle of the Network Time Protocol (NTP) and the Simple Network Time Protocol (SNTP).

NTP Synchronization Principle

NTP is used for time synchronization between the distributed time server and client. NTP defines the structure, algorithm, entity, and protocol that are used in the time synchronization. NTP is based on the IP and UDP protocol of TCP/IP, and it can also be used by other protocol suites. Theoretically, the accuracy of NTP can reach one nanosecond.

Figure 3-1 shows the basic principle of the NTP time synchronization.

Figure 3-1 NTP synchronization principle

Device A and Device B are connected through the network. Each of them has independent system time. Now the system time of the two devices needs to be synchronized automatically. Suppose the following conditions are met:

- The clock of Device A is set to 10:00:00 and that of Device B is set to 11:00:00 before the system time of Device A and that of Device B are synchronized.
- Device B serves as the NTP time server, that is, Device A synchronizes its time with that of Device B.
- A data packet takes one second for unidirectional transfer between Device A and Device B.

If Device A needs to synchronize its time with that of Device B, the following information is required:

- Offset: time deviation between Device A and Device B.
- Delay: time loss during the time synchronization between Device A and Device B.

When **Offset** and **Delay** are known, Device A can calculate the amount of time that needs to be modified if Device A synchronizes its time with that of Device B. NTP specifies how to calculate the values of **Offset** and **Delay**.

The process of time synchronization is as follows:

1. Device A sends an NTP message packet to Device B. The message packet contains the time stamp when it is sent from Device A. The time stamp is **10:00:00am (T1)**.
2. When the NTP message packet reaches Device B, Device B adds its own time stamp **11:00:01am (T2)** to the packet.
3. When the NTP message packet leaves Device B, Device B adds its own time stamp **11:00:02am (T3)** to the packet.
4. When Device A receives the response message packet, it adds a new time stamp **10:00:03am (T4)** to the packet.

Now Device A has enough information to calculate the two important parameters **Offset** and **Delay**.

- Delay of the period that Device A sends the NTP message and receives the response message: $\text{Delay} = (T4 - T1) - (T3 - T2)$.
- Time offset between Device A and Device B: $\text{Offset} = ((T2 - T1) + (T3 - T4))/2$.

Based on this information, Device A can set its own clock to synchronize with that of Device B.

NTP Hierarchical Networking Principle

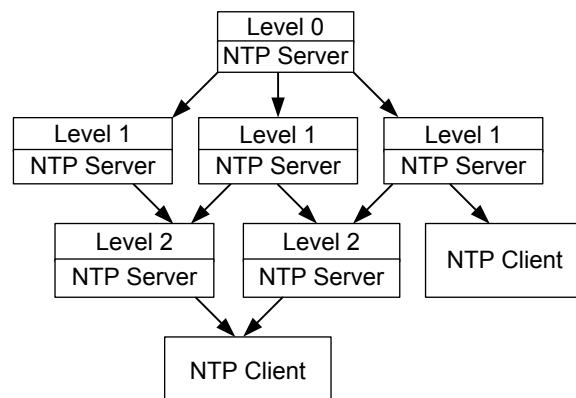
According to the principle and purpose of the time synchronization mechanism, time consistency is better when the clock sources are fewer. Due to the huge and complex network, however, it is not practical to connect all the devices that need to be synchronized to the same time server. Therefore, the hierarchical structure is used in the NTP model.

Theoretically, the time synchronization network is divided into 16 (from 0 to 15) or more levels according to accuracy and importance. In practice, the levels are less than six.

The devices of the 0 level are in special position. They are the reference time sources of the synchronization network. They are located on the top of the network and use the Global Positioning System (GPS), that is, the UTC time codes broadcast by the GPS.

The devices in a subnetwork plays multiple roles. For example, a device of the second level serves as the client for the devices of the first level and server for the devices of the third level.

Figure 3-2 NTP hierarchical networking



As shown in [Figure 3-2](#), the servers in the NTP hierarchical networking can be configured as follows:

- NTP servers of the top level: NTP servers of the 0 level that provide time synchronization service for the next level.
- NTP servers of the medium level: NTP servers of the levels such as the first and second levels that obtain time from the NTP servers of the upper level and provide the time synchronization service for the servers of the lower level.
- NTP clients: Obtain time from the NTP servers of the upper level but do not provide the time synchronization service.

A host can obtain time information from multiple NTP servers and an NTP server can provide time information for multiple hosts. The hosts of the same level can provide time information for each other. NTP can provide up to 15 levels of clients.

NOTE

NTP uses the port number 123 and uses UDP for communication. Therefore, ensure that the IP links are normal between nodes.

Comparison Between SNTP and NTP

SNTP is a simplified policy of the NTP server and client. The implementation methods for time synchronization are the same between SNTP and NTP, but the following control functions of NTP are more powerful than those of SNTP:

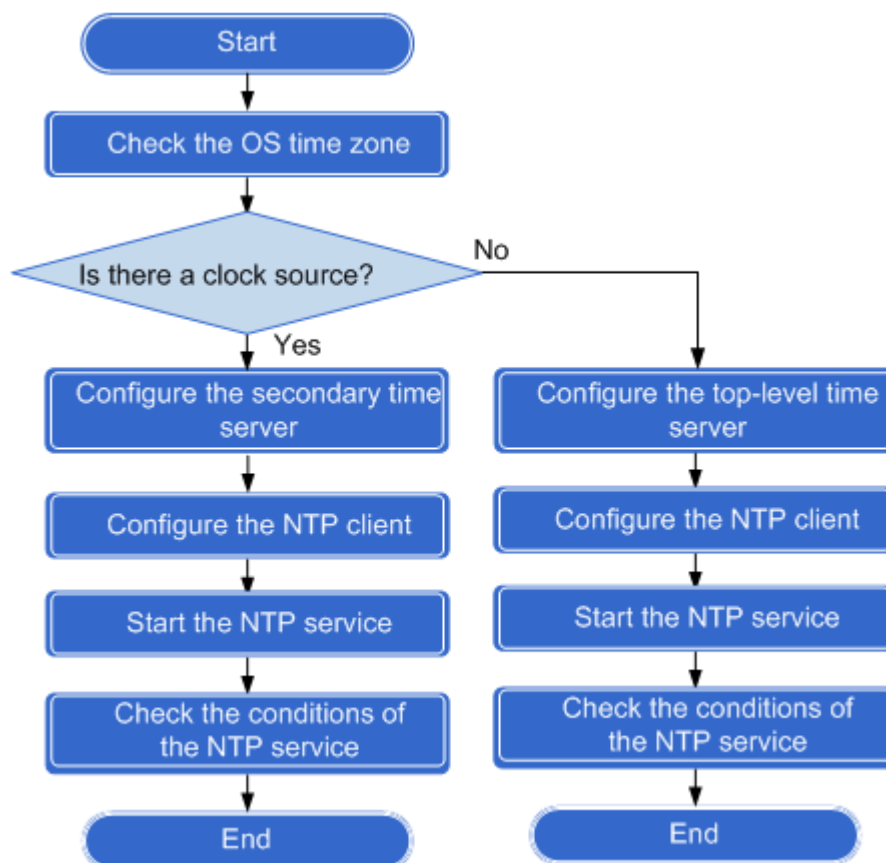
- Error processing function of time synchronization
- Multi-server filtering function
- Selection of multiple time sources (obtaining the most accurate time source among the connected NTP servers by algorithm-based comparison and analysis)

3.2 NTP Configuration Schemes

This topic describes how to NTP configuration schemes. The NTP solutions vary according to the schemes adopted in the actual installation and deployment of the U2000. NTP configuration schemes for each installation scheme are described.

Though the process of configuring NTP varies in different installation schemes, the basic process is the same. [Figure 3-3](#) shows the basic process.

Figure 3-3 Basic process of configuring NTP





CAUTION

- Correct NTP service configuration helps to achieve clock synchronization between the NTP server and NTP client. The time of the NTP server and the time of the NTP client can be in different time zones and different time. Make sure that the time is consistent with the standard date and time zone of the local area, and that the difference between the NTP server time and the local standard time is less than two minutes.
- The Windows OS does not support the configuration of NTP server; therefore, the operation of configuring the NTP server in the Windows OS is not described.
- Either the NMS maintenance suite or the command line can be used to configure NTP.
 - If the U2000 server is deployed as the NTP server at the highest level or an NTP client, either the NMS maintenance suite or the command line can be used to configure NTP.
In the Windows OS, the NMS maintenance suite cannot be used to configure NTP.
 - If the U2000 server is deployed as the NTP server at the medium layer, only the command line can be used to configure NTP.

[3.2.1 Configuring the NTP Solution to the Installation Scheme of the Single-Server System \(Windows\)](#)

This topic describes how to configure the NTP solution to the installation scheme of the Single-Server System(Windows).

[3.2.2 Configuring the NTP Solution to the Installation Scheme of the Single-Server System \(Solaris\)](#)

This topic describes how to configure the NTP solution to the installation scheme of the Single-Server System (Solaris).

[3.2.3 Configuring the NTP Solution to the Installation Scheme of the Single-Server System \(SUSE Linux-Distributed\)](#)

This topic describes how to configure the NTP solution to the installation scheme of the Single-Server System (SUSE Linux-Distributed).

[3.2.4 Configuring the NTP Solution to the Installation Scheme of the High Availability System \(Solaris\)](#)

This topic describes how to configure the NTP solution to the installation scheme of the High Availability System (Solaris).

[3.2.5 Configuring the NTP Solution to the Installation Scheme of the High Availability System \(Windows\)](#)

This topic describes how to configure the NTP solution to the installation scheme of the High Availability System (Windows).

[3.2.6 Configuring the NTP Solution to the Installation Scheme of the High Availability System \(SUSE Linux - Distributed\)](#)

This topic describes how to configure the NTP solution to the installation scheme of the High Availability System (SUSE Linux - Distributed).

3.2.1 Configuring the NTP Solution to the Installation Scheme of the Single-Server System (Windows)

This topic describes how to configure the NTP solution to the installation scheme of the Single-Server System(Windows).

Prerequisite

- A server that is installed with the Solaris OS or SUSE Linux OS must be configured as the NTP server.
- If the time difference between the NTP client and NTP server is large, for example, tens of minutes, the time on the NTP client cannot be synchronized with that on the NTP server once. In this case, you need to adjust the time difference for several times. Thus, the difference between the time on the NTP client and that on the NTP server should be shorter than five minutes. In this manner, the influence imposed by major time adjustment can be avoided on the application.

Context

- If you adopt the preceding scheme in the installation and deployment of the U2000, it is recommended that you configure the U2000 server in the Windows OS as the NTP client and configure the U2000 client in the Windows OS as the NTP client.
- Correct NTP service configuration helps to achieve clock synchronization between the NTP server and NTP client. The time of the NTP server and the time of the NTP client can be in different time zones and different time. Make sure that the time is consistent with the standard date and time zone of the local area, and that the difference between the NTP server time and the local standard time is less than two minutes.
- The Windows OS does not support the configuration of the NTP server.

Procedure

- 1 Check the time configuration of the U2000 server.

Open **Date and Time** on the Control Panel. In the **Date and Time** Properties dialog box, check the time zone, date and time.

The following errors may occur on the server:

- The time zone is incorrect.
- The date is incorrect.
- The server time is two minutes earlier or later than the local time.

If any of the preceding errors occur, perform the following steps to avoid system exceptions.

1. Stop all the time-based services, for example, the database service and U2000 service.
2. Correct the time zone, date, and time. For details, see [2.1.2 Modifying System Parameters](#).

NOTE

You can configure the NTP service only after you complete the preceding steps. All the stopped time-based applications need to be restarted after the configuration.

- 2 Configure the NTP client.

For details, see [3.3.2.1 Configuring the Windows OS as the NTP Client](#).

- 3 Start the NTP service in the Windows OS.

For details, see [3.3.2.2 Starting the NTP Service in the Windows OS](#).

----End

3.2.2 Configuring the NTP Solution to the Installation Scheme of the Single-Server System (Solaris)

This topic describes how to configure the NTP solution to the installation scheme of the Single-Server System (Solaris).

Prerequisite

If the time difference between the NTP client and NTP server is large, for example, tens of minutes, the time on the NTP client cannot be synchronized with that on the NTP server once. In this case, you need to adjust the time difference for several times. Thus, the difference between the time on the NTP client and that on the NTP server should be shorter than five minutes. In this manner, the influence imposed by major time adjustment can be avoided on the application.

Context

- If you adopt the preceding scheme during the installation and deployment of the U2000, it is recommended that you configure the U2000 server in the Solaris OS to function as the intermediate time server. If there is no clock source, it is recommended that you configure the server to function as the time server of the highest stratum. Configure the U2000 client as the NTP client.
- Correct NTP service configuration helps to achieve clock synchronization between the NTP server and NTP client. The time of the NTP server and the time of the NTP client can be in different time zones and different time. Make sure that the time is consistent with the standard date and time zone of the local area, and that the difference between the NTP server time and the local standard time is less than two minutes.
- In addition to the following method, you can also configure NTP by using the NMS maintenance tool. For details, see [D.4.10 Configuring the NTP Service](#).

Procedure

1 Check the time configuration of the U2000 server.

1. Run the following command to check the OS time zone:

```
# echo $TZ
```

2. Run the following command to check the OS date and time:

```
# date
```

The following errors may occur on the server:

- The time zone is incorrect.
- The date is incorrect.
- The server time is two minutes earlier or later than the local time.

If any of the preceding errors occur, perform the following steps to avoid system exceptions.

- a. Stop all the time-based service (For example, database service and U2000 service).
- b. Correct the time zone, date, and time. For details, see [2.2.2 Modifying System Parameters](#).

 NOTE

You can configure the NTP service only after you complete the preceding steps. All the stopped time-based applications need to be restarted after the configuration.

2 Configure the NTP server.

Configure the intermediate time server. For details, see [3.3.3.2 Setting the Solaris system to the Secondary Time Server](#).

If there is no clock source, you can configure the server to function as the time server of the highest stratum. For details, see [3.3.3.1 Setting the Solaris system as the Top-Level Time Server](#).

3 Configure the NTP client.

- If you deploy the U2000 client in the Solaris OS, configure the Solaris OS to function as the NTP client. For details, see [3.3.3.3 Setting the Solaris system to the NTP Client](#).
- If you deploy the U2000 client in the Windows OS, configure the Windows OS to function as the NTP client. For details, see [3.3.2.1 Configuring the Windows OS as the NTP Client](#).

4 Start the NTP service in the Solaris OS.

For details, see [3.3.3.4 Starting the NTP Service on the Solaris system](#).

5 Check the conditions of the NTP service in the Solaris OS.

For details, see [3.3.3.5 Checking the Conditions of the NTP Service in the Solaris OS](#).

----End

3.2.3 Configuring the NTP Solution to the Installation Scheme of the Single-Server System (SUSE Linux-Distributed)

This topic describes how to configure the NTP solution to the installation scheme of the Single-Server System (SUSE Linux-Distributed).

Prerequisite

If the time difference between the NTP client and NTP server is large, for example, tens of minutes, the time on the NTP client cannot be synchronized with that on the NTP server once. In this case, you need to adjust the time difference for several times. Thus, it is recommended that you check the time on the client first and minimize the time difference. In this manner, the influence imposed by major time adjustment can be avoided on the application.

Context

- If you adopt the preceding scheme during the installation and deployment of the U2000, it is recommended that you configure the master server and slave server of the U2000 to function as the NTP server and NTP client respectively. When you configure the master server of the U2000, configure it to function as the intermediate time server first. If there is no clock source, configure the master server to function as the time server of the highest stratum. Configure the U2000 client as the NTP client.
- Correct NTP service configuration helps to achieve clock synchronization between the NTP server and NTP client. The time of the NTP server and the time of the NTP client can be in different time zones and different time. Make sure that the time is consistent with the

standard date and time zone of the local area, and that the difference between the NTP server time and the local standard time is less than two minutes.

- In addition to the following method, you can also configure NTP by using the NMS maintenance tool. For details, see [D.4.10 Configuring the NTP Service](#).

Procedure

- 1 Check the time configuration of the U2000 server.

Run the following command to check the OS time zone, date, and time:

```
# yast2 timezone
```

The following errors may occur on the server:

- The time zone is incorrect.
- The date is incorrect.
- The server time is two minutes earlier or later than the local time.

If any of the preceding errors occur, perform the following steps to avoid system exceptions.

1. Stop all the time-based service (Database service and U2000 service).
2. Correct the time zone, date, and time. For details, see [2.3.2 Modifying System Parameters](#).

NOTE

You can configure the NTP service only after you complete the preceding steps. All the stopped time-based applications need to be restarted after the configuration.

- 2 Configure the NTP server.

Configure the intermediate time server. For details, see [3.3.4.2 Setting the SUSE Linux system to the Secondary Time Server](#).

If there is no clock source, configure the server to function as the time server of the highest stratum. For details, see [3.3.4.1 Setting the SUSE Linux system as the Top-Level Time Server](#).

- 3 Configure the NTP client.

- If you deploy the U2000 client in the SUSE Linux OS, configure the SUSE Linux OS to function as the NTP client. For details, see [3.3.4.3 Setting the SUSE Linux to the NTP Client](#).
- If you deploy the U2000 client in the Windows OS, configure the Windows OS to function as the NTP client. For details, see [3.3.2.1 Configuring the Windows OS as the NTP Client](#).
- If you deploy the U2000 client in the Solaris OS, configure the Solaris OS to function as the NTP client. For details, see [3.3.3.3 Setting the Solaris system to the NTP Client](#).

- 4 Start the NTP service of the SUSE Linux OS.

For details, see [3.3.4.4 Starting the NTP Service on the SUSE Linux](#).

- 5 Check the conditions of the NTP service of the SUSE Linux OS.

For details, see [3.3.4.5 Checking the Conditions of the NTP Service in the SUSE Linux OS](#).

----End

3.2.4 Configuring the NTP Solution to the Installation Scheme of the High Availability System (Solaris)

This topic describes how to configure the NTP solution to the installation scheme of the High Availability System (Solaris).

Prerequisite

If the time difference between the NTP client and NTP server is large, for example, tens of minutes, the time on the NTP client cannot be synchronized with that on the NTP server once. In this case, you need to adjust the time difference for several times. Thus, it is recommended that you check the time on the client first and minimize the time difference. In this manner, the influence imposed by major time adjustment can be avoided on the application.

Context

- If you adopt the preceding scheme during the installation and deployment of the U2000, it is recommended that you configure the active site server and standby site server to function as the NTP server and NTP client respectively. When you configure the active site server, configure it to function as the intermediate time server first. If there is no clock source, configure the active site server to function as the time server of the highest stratum. Configure the U2000 client as the NTP client.
- Correct NTP service configuration helps to achieve clock synchronization between the NTP server and NTP client. The time of the NTP server and the time of the NTP client can be in different time zones and different time. Make sure that the time is consistent with the standard date and time zone of the local area, and that the difference between the NTP server time and the local standard time is less than two minutes.
- In addition to the following method, you can also configure NTP by using the NMS maintenance tool. For details, see [D.4.10 Configuring the NTP Service](#).

Procedure

1 Check the time configuration of the U2000 server.

1. Run the following command to check the OS time zone:

```
# echo $TZ
```

2. Run the following command to check the OS date and time:

```
# date
```

The following errors may occur on the server:

- The time zone is incorrect.
- The date is incorrect.
- The server time is two minutes earlier or later than the local time.

If any of the preceding errors occur, perform the following steps to avoid system exceptions.

- a. Stop all the time-based service (For example, database service and U2000 service).

- b. Correct the time zone, date, and time. For details, see [2.5.3 Modifying System Parameters](#).

 NOTE

You can configure the NTP service only after you complete the preceding steps. All the stopped time-based applications need to be restarted after the configuration.

2 Configure the NTP server.

Configure the intermediate time server. For details, see [3.3.3.2 Setting the Solaris system to the Secondary Time Server](#).

If there is no clock source, you can configure the server to function as the time server of the highest stratum. For details, see [3.3.3.1 Setting the Solaris system as the Top-Level Time Server](#).

3 Configure the NTP client.

- If you deploy the U2000 client in the Solaris OS, configure the Solaris OS to function as the NTP client. For details, see [3.3.3.3 Setting the Solaris system to the NTP Client](#).
- If you deploy the U2000 client in the Windows OS, configure the Windows OS to function as the NTP client. For details, see [3.3.2.1 Configuring the Windows OS as the NTP Client](#).

4 Start the NTP service in the Solaris OS.

For details, see [3.3.3.4 Starting the NTP Service on the Solaris system](#).

5 Check the conditions of the NTP service in the Solaris OS.

For details, see [3.3.3.5 Checking the Conditions of the NTP Service in the Solaris OS](#).

----End

3.2.5 Configuring the NTP Solution to the Installation Scheme of the High Availability System (Windows)

This topic describes how to configure the NTP solution to the installation scheme of the High Availability System (Windows).

Prerequisite

- A server that is installed with the Solaris OS or SUSE Linux OS must be configured as the NTP server.
- If the time difference between the NTP client and NTP server is large, for example, tens of minutes, the time on the NTP client cannot be synchronized with that on the NTP server once. In this case, you need to adjust the time difference for several times. Thus, the difference between the time on the NTP client and that on the NTP server should be shorter than five minutes. In this manner, the influence imposed by major time adjustment can be avoided on the application.

Context

- If you adopt the preceding scheme in the installation and deployment of the U2000, it is recommended that you configure the active site server in the Windows OS as the NTP client, configure the standby site server in the Windows OS as the NTP client, and configure the U2000 client in the Windows OS as the NTP client.

- Correct NTP service configuration helps to achieve clock synchronization between the NTP server and NTP client. The time of the NTP server and the time of the NTP client can be in different time zones and different time. Make sure that the time is consistent with the standard date and time zone of the local area, and that the difference between the NTP server time and the local standard time is less than two minutes.
- The Windows OS does not support the configuration of the NTP server.
- In addition to the following method, you can also configure NTP by using the NMS maintenance tool. For details, see [D.4.10 Configuring the NTP Service](#).

Procedure

- 1 Check the time configuration of the U2000 server.

Open **Date and Time** on the Control Panel. In the **Date and Time** Properties dialog box, check the time zone, date and time.

The following errors may occur on the server:

- The time zone is incorrect.
- The date is incorrect.
- The server time is two minutes earlier or later than the local time.

If any of the preceding errors occur, perform the following steps to avoid system exceptions.

1. Stop all the time-based services, for example, the database service and U2000 service.
2. Correct the time zone, date, and time. For details, see [2.1.2 Modifying System Parameters](#).

NOTE

You can configure the NTP service only after you complete the preceding steps. All the stopped time-based applications need to be restarted after the configuration.

- 2 Configure the active site server in the Windows OS as the NTP client, configure the standby site server in the Windows OS as the NTP client, and configure the U2000 client in the Windows OS as the NTP client.

Configure the NTP client. For details, see [3.3.2.1 Configuring the Windows OS as the NTP Client](#).

For details, see [3.3.2.1 Configuring the Windows OS as the NTP Client](#).

- 3 Start the NTP service in the Windows OS.

For details, see [3.3.2.2 Starting the NTP Service in the Windows OS](#).

----End

3.2.6 Configuring the NTP Solution to the Installation Scheme of the High Availability System (SUSE Linux - Distributed)

This topic describes how to configure the NTP solution to the installation scheme of the High Availability System (SUSE Linux - Distributed).

Prerequisite

If the time difference between the NTP client and NTP server is large, for example, tens of minutes, the time on the NTP client cannot be synchronized with that on the NTP server once.

In this case, you need to adjust the time difference for several times. Thus, it is recommended that you check the time on the client first and minimize the time difference. In this manner, the influence imposed by major time adjustment can be avoided on the application.

Context

- If you adopt the preceding scheme during the installation and deployment of the U2000, it is recommended that you configure the master server of the active site to function as the NTP server and configure the slave server of the active site and the master and slave servers of the standby site to function as the NTP clients. Configure the U2000 client as the NTP client.
- Correct NTP service configuration helps to achieve clock synchronization between the NTP server and NTP client. The time of the NTP server and the time of the NTP client can be in different time zones and different time. Make sure that the time is consistent with the standard date and time zone of the local area, and that the difference between the NTP server time and the local standard time is less than two minutes.
- In addition to the following method, you can also configure NTP by using the NMS maintenance tool. For details, see [D.4.10 Configuring the NTP Service](#).

Procedure

- 1 Check the time configuration of the U2000 server.

Run the following command to check the OS time zone, date, and time:

```
# yast2 timezone
```

The following errors may occur on the server:

- The time zone is incorrect.
- The date is incorrect.
- The server time is two minutes earlier or later than the local time.

If any of the preceding errors occur, perform the following steps to avoid system exceptions.

1. Stop all the time-based service (Database service and U2000 service).
2. Correct the time zone, date, and time. For details, see [2.6.3 Modifying System Parameters](#).

NOTE

You can configure the NTP service only after you complete the preceding steps. All the stopped time-based applications need to be restarted after the configuration.

- 2 Configure the NTP server.

Configure the intermediate time server. For details, see [3.3.4.2 Setting the SUSE Linux system to the Secondary Time Server](#).

If there is no clock source, configure the server to function as the time server of the highest stratum. For details, see [3.3.4.1 Setting the SUSE Linux system as the Top-Level Time Server](#).

- 3 Configure the NTP client.

- If you deploy the U2000 client in the SUSE Linux OS, configure the SUSE Linux OS to function as the NTP client. For details, see [3.3.4.3 Setting the SUSE Linux to the NTP Client](#).
 - If you deploy the U2000 client in the Windows OS, configure the Windows OS to function as the NTP client. For details, see [3.3.2.1 Configuring the Windows OS as the NTP Client](#).
 - If you deploy the U2000 client in the Solaris OS, configure the Solaris OS to function as the NTP client. For details, see [3.3.3.3 Setting the Solaris system to the NTP Client](#).
- 4 Start the NTP service of the SUSE Linux OS.
- For details, see [3.3.4.4 Starting the NTP Service on the SUSE Linux](#).
- 5 Check the conditions of the NTP service of the SUSE Linux OS.
- For details, see [3.3.4.5 Checking the Conditions of the NTP Service in the SUSE Linux OS](#).
- End

3.3 NTP Configuration Task Set

This topic describes how to configure the NTP server and client in the Windows OS, Solaris OS, and SUSE Linux OS respectively.

[3.3.1 Configuring the NTP Service by Using the NMS Maintenance Suite](#)

This topic describes how to configure the NTP service. After installing the U2000, you can configure the NTP service by using the MSuite.

[3.3.2 Manually Configuring the NTP Service by Using Commands \(Windows\)](#)

This topic describes how to manually configure the NTP service by using commands in the Windows OS.

[3.3.3 Manually Configuring the NTP Service by Using Commands \(Solaris\)](#)

This topic describes how to manually configure the NTP service by using commands in the Solaris OS.

[3.3.4 Manually Configuring the NTP Service by Using Commands \(SUSE Linux\)](#)

This topic describes how to manually configure the NTP service by using commands in the SUSE Linux OS.

3.3.1 Configuring the NTP Service by Using the NMS Maintenance Suite

This topic describes how to configure the NTP service. After installing the U2000, you can configure the NTP service by using the MSuite.

Prerequisite

- The U2000 and database must be shut down. For details, see [E Shutting Down the U2000](#).
- The time zone of the workstation must be the same as that of the tracked clock source.

Context

- The MSuite does not support the operation of configuring the U2000 server as the NTP server at the medium layer.
- In the Windows OS, using the MSuite to configure NTP is unavailable.

Procedure

- 1 Log in to the MSuite client. For details, see [D.2.2 Logging In to the MSuite Client](#).
- 2 On the MSuite client, choose **Deploy > Configure NTP**. The **Configure NTP** dialog box is displayed.
- 3 Enter the IP address of the NTP server, and then click **OK**.

TIP

- If you need to configure the NMS server as the NTP server at the top layer, that is, external clock sources are not traced, set **NTP server IP** to *127.0.0.1*.
- If you need to configure the NMS server as the NTP client, that is, external clock sources are traced, set **NTP server IP** to the IP address of the server that is traced.

- 4 Click **OK**.
- 5 Restart the OS.

----End

Example

How to Configure the Primary Site as the NTP Server of the Highest Stratum and the Secondary Site as the NTP Client in the high availability system (Veritas hot standby), as Defined in the NTP Configuration Scheme, When No External Clock Source Is Available?

1. Configure the primary site as the NTP server of the highest stratum. Log in to the MSuite server of the primary site and configure the primary site by referring to the preceding steps. In the **NTP server IP** field, enter *127.0.0.1*.
2. Configure the secondary site as the NTP client. Log in to the MSuite server of the secondary site and configure the secondary site by referring to the preceding steps. In the **NTP server IP** field, enter the system IP address of the primary site.

3.3.2 Manually Configuring the NTP Service by Using Commands (Windows)

This topic describes how to manually configure the NTP service by using commands in the Windows OS.

[3.3.2.1 Configuring the Windows OS as the NTP Client](#)

This topic describes how to configure the Windows OS as the NTP client through the Windows NTP service and how to synchronize the time of the NTP client with the time of the NTP server.

[3.3.2.2 Starting the NTP Service in the Windows OS](#)

This topic describes how to start the NTP service in the Windows OS to implement time synchronization.

[3.3.2.3 Stopping the NTP Service in the Windows OS](#)

This topic describes how to stop the NTP service in the Windows OS.

3.3.2.1 Configuring the Windows OS as the NTP Client

This topic describes how to configure the Windows OS as the NTP client through the Windows NTP service and how to synchronize the time of the NTP client with the time of the NTP server.

Prerequisite

- The Windows OS works properly.
- The clock source of the NTP server works properly.

Context

The configuration procedure is applicable to the Windows 2000 Professional or Windows XP Professional OS. You can refer to this topic to perform settings in other Windows versions since they are similar to the NTP service settings. For details about the NTP service, see the related documents of Microsoft Windows.

Procedure

- 1 To set the Windows system to the NTP client, do as follows:



CAUTION

It is suggested to back up the registry before you manually modify it.

1. Open the Windows **Registry Editor**: Choose **Start > Run**, in the **Run** dialog box enter **regedit**, and then press **Enter**.
2. Under the key **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters**, modify the value of **LocalNTP** to **0**.



NOTE

- The default value of **LocalNTP** is **0**.
- In Windows, if the registry does not contain **LocalNTP**, it indicates that the value of **LocalNTP** can be ignored and you need not modify the value.

- 2 Specify the NTP clock source:

1. Open the CLI window: Choose **Start > Run**, in the **Run** dialog box enter **cmd**, and then press **Enter**.
2. Running the following command:

```
c:\> net time /setsntp:<NTP Server IP address>
```



NOTE

The execution result of **net time** is saved in Windows registry. Therefore, the parameters configured using **net time** still works after you restart Windows.

- 3 To cancel your settings, run the following command:

```
c:\> net time /setsntp
```

- 4 View the specified NTP server of the current machine by running the following command:

```
C:\> net time /queryntp
```

- 5 Check the status of NTP by running the following command:

```
C:\> tasklist /svc
```

Check whether the **svchost.exe** process contains the **W32Time** service. If the process contains the **W32Time** service, it indicates that the NTP service is running.

 NOTE

To start the **W32Time** service in Windows, run the **net start w32time** command. To stop the **W32Time** service in Windows, run the **net stop w32time** command.

----End

3.3.2.2 Starting the NTP Service in the Windows OS

This topic describes how to start the NTP service in the Windows OS to implement time synchronization.

Context

- Check whether the current time zone, date, and time of the Windows are correct before you start the NTP service. If they are incorrect, correct them.
- After you start the NTP service, the NTP client starts to synchronize the time with that of the NTP server and slowly adjusts the time deviation. As the adjustment is in the millisecond level, it does not affect the running of the Windows.

Procedure

- 1 Check if the time zone, date, and time of the server are correct. If not, adjust them manually. For details, see section [2.1.2 Modifying System Parameters](#)
- 2 In the command prompt window, run the following command to check whether the NTP service is started.

```
C:\> tasklist /svc
```

Check whether the **svchost.exe** process contains the **W32Time** service. If the process contains the **W32Time** service, it indicates that the NTP service is running.

- 3 If the NTP service process is running, stop it first by running the following command:

```
C:\> net stop w32time
```

- 4 In the command prompt window, run the following command to start the NTP service.

```
C:\> net start w32time
```

----End

3.3.2.3 Stopping the NTP Service in the Windows OS

This topic describes how to stop the NTP service in the Windows OS.

Context

After the NTP service is stopped, the U2000 server fails to synchronize the time with that of the NTP server. This may result in a time deviation.

Procedure

- 1 In the command prompt window, run the following command to check whether the NTP service is stopped.

```
C : \> tasklist /svc
```

Check whether the **svchost.exe** process contains the **W32Time** service. If the process not contains the **W32Time** service, it indicates that the NTP service is stopped.

- 2 In the command prompt window, run the following command to stop the NTP service.

```
C : \> net stop w32time
```

----End

3.3.3 Manually Configuring the NTP Service by Using Commands (Solaris)

This topic describes how to manually configure the NTP service by using commands in the Solaris OS.

[3.3.3.1 Setting the Solaris system as the Top-Level Time Server](#)

This topic describes how to configure the Solaris system as the top-level time server.

[3.3.3.2 Setting the Solaris system to the Secondary Time Server](#)

This task is performed to set the Solaris system to the secondary NTP server. The secondary NTP server synchronizes the time with that of the upper-level server and provides a standard time source for a lower-level server.

[3.3.3.3 Setting the Solaris system to the NTP Client](#)

This topic describes how to set the Solaris system to the NTP client.

[3.3.3.4 Starting the NTP Service on the Solaris system](#)

This task is performed to start the NTP service on the Solaris system to synchronize the time.

[3.3.3.5 Checking the Conditions of the NTP Service in the Solaris OS](#)

This topic describes how to check the conditions of the NTP service in the Solaris OS. Solaris allows you to run the **ntpq -p** and **ntptime** commands to check whether the NTP synchronization status is normal.

[3.3.3.6 Stopping the NTP Service in the Solaris OS](#)

This topic describes how to stop the NTP service in the Solaris OS.

3.3.3.1 Setting the Solaris system as the Top-Level Time Server

This topic describes how to configure the Solaris system as the top-level time server.

Procedure

- 1 Log in to the Solaris as **root**.

- 2 Run the following commands:

cp /etc/inet/ntp.server /etc/inet/ntp.conf

vi /etc/inet/ntp.conf
- 3 Modify **server 127.127.XType.0** to **server 127.127.1.0 prefer**.
- 4 Modify **fudge 127.127.XType.0 stratum 0** to **fudge 127.127.1.0 stratum 0**.
- 5 Save **/etc/inet/ntp.conf**, and then exit the vi editor.

----End

3.3.3.2 Setting the Solaris system to the Secondary Time Server

This task is performed to set the Solaris system to the secondary NTP server. The secondary NTP server synchronizes the time with that of the upper-level server and provides a standard time source for a lower-level server.

Prerequisite

The time zone, date, and time of the Solaris are set correctly.

Procedure

- 1 Log in to the Solaris system as the **root** user.
 - 2 Run the following commands:

cp /etc/inet/ntp.server /etc/inet/ntp.conf

vi /etc/inet/ntp.conf
 - 3 Modify all "XType" to "1".
 - 4 Add "server XXX.XXX.XXX.XXX" before "server 127.127.1.0 prefer" to specify the IP address of the upper-level NTP server. Each line maps to an NTP server.
-  **NOTE**
- "XXX.XXX.XXX.XXX" represents the IP address of the upper-level NTP server. If there are multiple upper-level NTP servers, write as many rows as necessary. For example:
server XXX.XXX.XXX.XXX prefer server XXX.XXX.XXX.XXX prefer
- 5 Delete "stratum 0" from "fudge 127.127.1.0 stratum 0".
 - 6 Add "#" before "broadcast 224.0.1.1 ttl 4".
 - 7 Save the **/etc/inet/ntp.conf** file and exit from the vi editor.

----End

3.3.3.3 Setting the Solaris system to the NTP Client

This topic describes how to set the Solaris system to the NTP client.

Procedure

1 Log in to the Solaris system as the **root** user.

2 Run the following commands:

```
# cp /etc/inet/ntp.client /etc/inet/ntp.conf
```

```
# vi /etc/inet/ntp.conf
```

3 Add a line to file: **server XXX.XXX.XXX.XXX**.



NOTE

XXX.XXX.XXX.XXX represents the IP address of the upper-level NTP server, such as server 10.10.10.100.

4 Disable the multicast client mode. Put a comment (# character without quotes) in front of `multicastclient 224.0.1.1`. For example, `# multicastclient 224.0.1.1`.

5 Save the `/etc/inet/ntp.conf` file and exit from the vi editor.

----End

3.3.3.4 Starting the NTP Service on the Solaris system

This task is performed to start the NTP service on the Solaris system to synchronize the time.

Context

- The NTP boot script is in `/etc/rc2.d/`. After you start Solaris, the NTP service is started automatically. Therefore, you need not add the NTP boot script manually.
- Check whether the current time zone, date, and time of the Solaris are correct before you start the NTP service. If they are incorrect, correct them.
- After you start the NTP service, the NTP client starts to synchronize the time with that of the NTP server and slowly adjusts the time deviation. As the adjustment is in the millisecond level, it does not affect the running of the Solaris.

Procedure

1 Log in to the Solaris system as the **root** user.

2 Check if the time zone, date, and time of the server are correct. If not, adjust them manually. For details, see section [2.2.2 Modifying System Parameters](#).

3 Run the following command to check whether the NTP service is started:

The following information is displayed:

```
root 25972 25945 0 15:45:06 pts/5 0:00 grep ntp
```



NOTE

- If the screen output does not contain `/usr/lib/inet/xntpd`, it indicates that the NTP service is not started.
- You can also run the following command to check whether the NTP service is started. `online` indicates that the NTP service is already started.

```
# svcs -a | grep ntp
```

```
online          9:57:29 svc:/network/ntp:default
```


4 If the NTP service process is running, stop it first by running the following command:

- In solaris 10
svcadm disable *svc:/network/ntp:default*
- In solaris 8
/etc/rc2.d/S74xntpd stop

5 Run the following command to start the NTP service:

- In solaris 10
svcadm enable *svc:/network/ntp:default*
- In solaris 8
/etc/rc2.d/S74xntpd start

----End

3.3.3.5 Checking the Conditions of the NTP Service in the Solaris OS

This topic describes how to check the conditions of the NTP service in the Solaris OS. Solaris allows you to run the **ntpq -p** and **ntptrace** commands to check whether the NTP synchronization status is normal.

Context

- The **remote** field in the return message of the **ntpq -p** command is the IP address of the reference time source. It indicates the status of the reference time source.
- The **ntptrace** command traces the entire NTP synchronization link from the local machine to the NTP server at the highest level. For details, run the **ntptrace -v** command.
- When the NTP server and NTP client are started, it takes fifteen minutes for detection. During the detection, when the **ntpq -p** command is run, the remote time source is not displayed with *. When the **ntptrace** command is run, **Timeout** or **Not Synchronized** is displayed. Wait for fifteen minutes, and then run the **ntpq -p** command or **ntptrace** command.

Procedure

- 1 In command line mode, run the **ntpq -p** command to view the NTP clock source.
- 2 In command line mode, run the **ntptrace** command to view the NTP synchronization link.

----End

Result

- If the Solaris is the NTP server at the intermediate level, the return result is as follows:

```
# ntpq -p
```

remote offset	disp	refid	st	t	when	poll	reach	delay
=====								
==								
*10.161.94.212		.LCL.	1	u	165	512	377	
0.406	61.294	0.111						
+local(0)		Local(0)	3	1	29	64	377	
0.000	0.000	0.000						

ntptrace

```
localhost: stratum 2, offset 0.000049, synch distance 0.02863
10.161.94.212: stratum 1, offset -0.001166, synch distance 0.01024
```

- In the return result obtained after the **ntpq -p** command is run, *10.161.94.212 indicates that the IP address of the NTP server is 10.161.94.212. The asterisk (*) indicates that the status is normal. From the value in the st column, you can know that 10.161.94.212 is at level 1.
- The return result (localhost: stratum 2) obtained after the **ntptrace** command is run indicates that the server is at level 2, and the IP address of the server at the upper level is 10.161.94.212 at level 1.

- If the Solaris is the NTP client at the intermediate level, the return result is as follows:

ntpq -p

```

      remote          refid          st          t          when          poll
reach  delay        offset  disp
=====
=
*10.161.94.214      10.161.94.212      2          u          58          64
377      0.37      0.217      0.05
```

ntptrace

```
localhost:stratum 3, offset 0.000035, synch distance 0.08855
10.161.94.214: stratum 2, offset 0.000224, synch distance 0.07860
10.161.94.212: stratum 1, offset 0.060569, synch distance 0.01036,
refid 'LCL'
```

- In the return result obtained after the **ntpq -p** command is run, *10.161.94.214 indicates that the IP address of the NTP server is 10.161.94.214. The asterisk (*) indicates that the status is normal. From the value in the st column, you can know that 10.161.94.214 is at level 2.
- The return result (localhost:stratum 3) obtained after the **ntptrace** command is run indicates that the server is at level 3, and the IP address of the server at the upper level is 10.161.94.212 at level 1.

3.3.3.6 Stopping the NTP Service in the Solaris OS

This topic describes how to stop the NTP service in the Solaris OS.

Context

After the NTP service is stopped, the U2000 server fails to synchronize the time with that of the NTP server. This may result in a time deviation.

Procedure

- 1 Log in to the Solaris as the **root** user.
- 2 Stop the NTP service.
 - In Solaris 10, run the following command:

```
# svcadm disable svc:/network/ntp:default
```

 NOTE

The command can be run only once. This means that the NTP service is not enabled each time the system is restarted.

- In Solaris 8, run the following command:
`# /etc/rc2.d/S74xntpd stop`

3 Check whether the NTP service is stopped and run the following command:

```
# ps -ef | grep ntp
```

If `/usr/lib/inet/xntpd` is not displayed, it indicates that the NTP service is stopped.

----End

3.3.4 Manually Configuring the NTP Service by Using Commands (SUSE Linux)

This topic describes how to manually configure the NTP service by using commands in the SUSE Linux OS.

3.3.4.1 Setting the SUSE Linux system as the Top-Level Time Server

This topic describes how to configure the SUSE Linux system as the top-level time server.

3.3.4.2 Setting the SUSE Linux system to the Secondary Time Server

This task is performed to set the SUSE Linux system to the secondary NTP server. The secondary NTP server synchronizes the time with that of the upper-level server and provides a standard time source for a lower-level server.

3.3.4.3 Setting the SUSE Linux to the NTP Client

This topic describes how to set the SUSE Linux to the NTP client.

3.3.4.4 Starting the NTP Service on the SUSE Linux

This task is performed to start the NTP service on the SUSE Linux to synchronize the time.

3.3.4.5 Checking the Conditions of the NTP Service in the SUSE Linux OS

This topic describes how to check the conditions of the NTP service in the SUSE Linux OS. The SUSE Linux OS provides two commands for querying the NTP status: `ntpq -p` and `ntptrace`. According to the NTP status, you can understand whether the NTP synchronization is normal.

3.3.4.6 Stopping the NTP Service in the SUSE Linux OS

This topic describes how to stop the NTP service in the SUSE Linux OS.

3.3.4.1 Setting the SUSE Linux system as the Top-Level Time Server

This topic describes how to configure the SUSE Linux system as the top-level time server.

Procedure

- 1 Log in to the SUSE Linux as **root**.
- 2 Run the following commands:

```
# cp /etc/inet/ntp.server /etc/inet/ntp.conf
```

```
# vi /etc/inet/ntp.conf
```
- 3 Modify **server 127.127.XType.0** to **server 127.127.1.0 prefer**.
- 4 Modify **fudge 127.127.XType.0 stratum 0** to **fudge 127.127.1.0 stratum 0**.

- 5 Save `/etc/inet/ntp.conf`, and then exit the vi editor.

----End

3.3.4.2 Setting the SUSE Linux system to the Secondary Time Server

This task is performed to set the SUSE Linux system to the secondary NTP server. The secondary NTP server synchronizes the time with that of the upper-level server and provides a standard time source for a lower-level server.

Prerequisite

The time zone, date, and time of the SUSE Linux are set correctly.

Procedure

- 1 Log in to the SUSE Linux system as the **root** user.
- 2 Run the following commands:

```
# cp /etc/inet/ntp.server /etc/inet/ntp.conf
```

```
# vi /etc/inet/ntp.conf
```
- 3 Modify all "XType" to "1".
- 4 Add "server XXX.XXX.XXX.XXX" before "server 127.127.1.0 prefer" to specify the IP address of the upper-level NTP server. Each line maps to an NTP server.



NOTE

"XXX.XXX.XXX.XXX" represents the IP address of the upper-level NTP server. If there are multiple upper-level NTP servers, write as many rows as necessary. For example:
server XXX.XXX.XXX.XXX prefer server XXX.XXX.XXX.XXX prefer

- 5 Delete "stratum 0" from "fudge 127.127.1.0 stratum 0".
- 6 Add "#" before "broadcast 224.0.1.1 ttl 4".
- 7 Save the `/etc/inet/ntp.conf` file and exit from the vi editor.

----End

3.3.4.3 Setting the SUSE Linux to the NTP Client

This topic describes how to set the SUSE Linux to the NTP client.

Procedure

- 1 Log in to the SUSE Linux as the **root** user.
- 2 Run the following command to configure SUSE Linux to the NTP client.
 1. # **yast2 ntp-client**
 2. Under **Automatically Start NTP Daemon**, select **During Boot**.
 3. In the **Warning** dialog box, select **Continue**.
 4. In the **Address** text box, enter the IP address of the NTP server.

5. Select **Test** to check whether the NTP server is available.

 NOTE

If the NTP server is unavailable, remove faults as prompted.

6. Click **Finish**.

----End

3.3.4.4 Starting the NTP Service on the SUSE Linux

This task is performed to start the NTP service on the SUSE Linux to synchronize the time.

Context

- Check whether the current time zone, date, and time of the SUSE Linux are correct before you start the NTP service. If they are incorrect, correct them.
- After you start the NTP service, the NTP client starts to synchronize the time with that of the NTP server and slowly adjusts the time deviation. As the adjustment is in the millisecond level, it does not affect the running of the SUSE Linux.

Procedure

- 1 Log in to SUSE Linux as the **root** user.
- 2 Check that the time zone, date, and time of the server are correct. If they are incorrect, change them manually. For details, see [2.3.2 Modifying System Parameters](#).
- 3 Run the following command to start the NTP service:

```
# service ntp start
```

----End

3.3.4.5 Checking the Conditions of the NTP Service in the SUSE Linux OS

This topic describes how to check the conditions of the NTP service in the SUSE Linux OS. The SUSE Linux OS provides two commands for querying the NTP status: **ntpq -p** and **ntptrace**. According to the NTP status, you can understand whether the NTP synchronization is normal.

Context

- **ntpq -p** returns the `remote` field that provides the address and status of the reference clock source.
- **ntptrace** traces the entire NTP synchronization chain from the local computer to the NTP top stratum. For details, run **ntptrace -v**.
- After the NTP Server and NTP Client are started, the check takes about five minutes. When you run **ntpq -p** during the check, the returned clock source addresses in `remote` does not contain *. When you run **ntptrace**, however, `Timeout` or `Not Synchronized` is returned. In this case, wait for five minutes, and then run **ntpq -p** or **ntptrace** again.

Procedure

- 1 On the CLI, run **ntpq -p**.

2 Run **ntptrace**.

----End

Result

- When the SUSE Linux OS is the NPT server at the middle stratum, the returned information is as follows:

ntpq -p

```

remote      refid      st    t    when    poll    reach    delay
offset      jitter
=====
==
*10.161.94.212 .LCL.      1      u    165      512    377
0.406      61.294    0.111
+local(0)      Local(0) 3      1      29      64      377
0.000      0.000    0.000

```

ntptrace

```

localhost:stratum 1, offset      0.060665, syncn distance 0.01015, refid
'LCL'
#

```

- The information returned by **ntpq -p** indicates that the IP address of the NTP server that the host synchronizes is 10.161.94.212 at stratum 1. The asterisk (*) indicates that the synchronization is normal.
- The information returned by **ntptrace** indicates that the host is at stratum 2 and that the IP address of the host at the previous stratum is 10.161.94.212 at stratum 1.

- When the SUSE Linux OS is the NPT client at the middle stratum, the returned information is as follows:

ntpq -p

```

remote      refid      st    t    when    poll
reach      delay    offset    disp
=====
=
*10.161.94.214      10.161.94.212      2      u    58      64
377      0.37      0.217      0.05

```

ntptrace

```

localhost:stratum 3, offset      0.000035, syncn distance 0.08855
10.161.94.214: stratum 2, offset 0.000224, synch distance 0.07860
10.161.94.212: stratum 1, offset 0.060569, synch distance 0.01036,
refid 'LCL'

```

- *10.161.94.214 returned by **ntpq -p** indicates that the IP address of the NTP server that the host synchronizes is 10.161.94.214 at stratum 2. The asterisk (*) indicates that the synchronization is normal.
- The information returned by **ntptrace** indicates that the host is at stratum 3, the IP address 10.161.94.214 is at stratum 2, and that the IP address 10.161.94.212 at stratum 1.

3.3.4.6 Stopping the NTP Service in the SUSE Linux OS

This topic describes how to stop the NTP service in the SUSE Linux OS.

Context

After the NTP service is stopped, the U2000 server fails to synchronize the time with that of the NTP server. This may result in a time deviation.

Procedure

- 1 Log in to SUSE Linux as the **root** user.
- 2 Run the following command to stop the NTP service:

```
# service ntp stop
```

----End

4 Configuring NMS System Security

About This Chapter

This topic describes the security policies and security management function of the U2000. With the security policies and security management function, you can perform authority- and domain-based management, and monitor and manage the login NMS users in real time. In this manner, you can ensure the network and data security and protect the network against illegitimate logins or incorrect operations.

[4.1 Configuring System Security Policies](#)

This topic describes how to configure system security policies. The OS security is the basic of the secure running of the U2000. It involves many aspects such as the security of the OS, and antivirus.

[4.2 U2000 Application Security](#)

This topic describes the application security policies of the U2000.

[4.3 Configuring Communications Security](#)

This topic describes the policies for communications security of the U2000, including southbound communications security, northbound communications security, inter-server communications security, and client communications security, and how to configure the client to communicate with equipment through the SSH protocol and configure the server to communicate with the client through the SSL protocol.

[4.4 Setting Security Policies of U2000 Users](#)

A user of the SMMangers group can set the password policy and account policy of the U2000 user, to enhance the security.

4.1 Configuring System Security Policies

This topic describes how to configure system security policies. The OS security is the basic of the secure running of the U2000. It involves many aspects such as the security of the OS, and antivirus.

You can take measures in the following aspects to ensure the security of the OS:

- Os security management.
- Antivirus. You need to install the antivirus software.

SetSolaris Solution

SEK SetSolaris is developed to enhance the security of Sun Solaris systems. The system security is enhanced through parameter settings. Also, security risks are checked and reported. SetSolaris V100R004 is compliant with CIS Benchmark 4.0.

SEK SetSolaris comes with the GUI and CLI. The GUI allows you to configure, perform, and save system policies. It allows single-click operations. The CLI allows you to perform system policies to enhance the system security. You can set the parameters using SEK SetSolaris as and when required. This tool is mainly used after the installation of a new OS to set the security parameters of the system.

The software package of SEK SetSolaris contains user manuals and customized U2000 security policy configuration, that is, **SEKConf.tar**. The path where the **SEKConf.tar** are stored is **/opt/HWICMR/conf/Install/SetSolaris/**. For the installation and usage of SEK SetSolaris, see the user manuals in the software package.

Antivirus Solution

The U2000 adopts the Trend Micro OfficeScan Viruswall 8.0 as the antivirus solution.

The OfficeScan Viruswall protects the Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows 95, Windows 98, and Windows Me against viruses (including file-type viruses and Macro viruses), malicious codes (including malicious Java programs and ActiveX controls), spyware (including files and programs), and greyware (including files and programs).

The OfficeScan Viruswall provides a unified console so that the administrator can configure, monitor, and maintain the antivirus measures for PCs. This improves and simplifies the management of enterprise antivirus policies.

For the details about how to install, deploy, and commission the antivirus software, see the operation guide delivered along with the antivirus software.

4.2 U2000 Application Security

This topic describes the application security policies of the U2000.

4.2.1 OS User Security

This section describes the OS user types and their rights related to U2000.

4.2.2 Database User Security

This topic describes the database user security. The data related to the NMS is stored in the database. Therefore, the security of database users must be ensured.

4.2.3 Security of the Database System Files

This topic describes the security planning of the database system files.

4.2.4 User Security Policy

The U2000 security management mainly involves the objects management, password management, access control management, and role-based and domain-based management.

4.2.5 Log Management Policy

Log security management includes the U2000 operation log, U2000 security log, NE security log, log dump, and log forwarding management.

4.2.6 Security of the System Data

Periodically and efficiently backing up the applications and data of the NMS is a powerful way to ensure the system security. Malicious and undesigned security threats cannot be avoided. If a security incident occurs and degrades the system security, the backup scheme can be used to restore the system in time. This is an indispensable security measure for the NMS.

4.2.7 NE Security Management

The NE security management includes NE access control, NE user management, NE operation right management and NE data security management.

4.2.1 OS User Security

This section describes the OS user types and their rights related to U2000.

- **Table 4-1** lists the Solaris OS users related to the U2000 and their rights.

Table 4-1 Solaris OS users related to the U2000 and their rights

User	Description
root	The root user is the default system administrator of the Solaris or SUSE Linux OS. With the highest right of the OS, the root user controls all resources, creates other users, assigns rights to other users, and performs all operations of the OS. The root user is responsible for installing or uninstalling the application software of the U2000 server. In general situations, perform operations in the OS as common users.
sybase	The sybase user is responsible for setting Sybase environment variables, installing, maintaining and managing the Sybase database. With all the rights of the directory /opt/sybase, the sybase user can manage the Sybase database, for example, configuring Sybase environment variables and starting/stopping the Sybase service.

User	Description
nmsuser	When you install the U2000 in the Solaris OS, the U2000 creates a nmsuser user of the Solaris OS automatically. The nmsuser user is responsible for setting environment variables of the U2000 server and starting the U2000 client at the server. The nmsuser user has all the rights of the directory / nmsuser. The file ./profile in this directory records environment variables for U2000 running.

- **Table 4-2** lists the Linux OS users related to the U2000 and their rights.

Table 4-2 Linux OS users related to the U2000 and their rights

User	Description
root	The root user is the default system administrator of the Solaris or SUSE Linux OS. With the highest right of the OS, the root user controls all resources, creates other users, assigns rights to other users, and performs all operations of the OS. The root user is responsible for installing or uninstalling the application software of the U2000 server. In general situations, perform operations in the OS as common users.
oracle	OS user who performs operations about the Oracle database. The oracle user is responsible for installing, deploying, and maintaining the Oracle database to ensure the OS and data security. It is recommended that the oracle user have the following attributes: ● Home directory: /opt/oracle ● Owner group: dba ● shell: /bin/bash
nmsuser	When you install the U2000 in the SUSE Linux OS, the U2000 creates a nmsuser user of the SUSE Linux OS automatically. The nmsuser user is responsible for setting environment variables of the U2000 server and starting the U2000 client at the server. The nmsuser user has all the rights of the directory / nmsuser. The file ./profile in this directory records environment variables for U2000 running.

- **Table 4-3** lists the Windows OS users related to the U2000 and their rights.

Table 4-3 Windows OS users related to the U2000 and their rights

User	Description
administrator	The administrator user is the default system administrator of the Windows OS. With the highest right of the OS, the administrator user controls all resources, creates other users, assigns rights to other users, and performs all operations of the OS. The administrator user is responsible for installing or uninstalling the application software of the U2000 server. In general situations, perform operations in the OS as common users.

4.2.2 Database User Security

This topic describes the database user security. The data related to the NMS is stored in the database. Therefore, the security of database users must be ensured.

- Solaris OS:

Table 4-4 shows the Sybase database users of the U2000 and their rights.

Table 4-4 Database users and their rights

Database User	Description
sa	The default system administrator of the database is the sa user. The sa user has the highest management rights on the database. Therefore, the password security for the sa user must be ensured.
NMSuser	After the U2000 is installed, the database user, that is, NMSuser is automatically created. It is recommended that you immediately change the password of the created user with the database user password management tool after the installation of the U2000.

- Linux OS:

Table 4-5 shows the oracle database users of the U2000 and their rights.

Table 4-5 Database users and their rights

Database User	Description
sys	Superuser of the Oracle database, who has all operation rights of the database. In view of security, this user does not perform routine maintenance.

Database User	Description
system	Administrator of the Oracle database. It is recommended that this user should not perform routine maintenance.
dba	Database user created by the system user. You need to create the dba user manually. Generally this user is responsible for performing routine operations and maintenance of the Oracle database. It is recommended that the name of the user should be easy to remember.
NMSuser	After the U2000 is installed, the database user, that is, NMSuser is automatically created. It is recommended that you immediately change the password of the created user with the database user password management tool after the installation of the U2000.

- Windows OS:

Table 4-6 shows the SQL Server database users of the U2000 and their rights.

Table 4-6 Database users and their rights

Database User	Description
sa	The default system administrator of the SQL Server database is the sa user. The sa user has the highest management rights on the database. Therefore, the password security for the sa user must be ensured.
NMSuser	After the U2000 is installed, the database user, that is, NMSuser is automatically created. It is recommended that you immediately change the password of the created user with the database user password management tool after the installation of the U2000.

4.2.3 Security of the Database System Files

This topic describes the security planning of the database system files.

The efficient method of improving the database security is to periodically back up, restore, and verify data on a timely basis. For the security planning suggestions, see [4.2.6 Security of the System Data](#).

4.2.4 User Security Policy

The U2000 security management mainly involves the objects management, password management, access control management, and role-based and domain-based management.

Security Management Objects

User: The user name and the password of a U2000 client user uniquely identifies the U2000 management rights entitled to the user. When a user is added to a user group, the user has all the operation rights of this user group.

- The U2000 provides a default user: admin. It is the super user of the system and has a higher authority than the system administrator group. You can neither modify the rights of the user admin, nor add user admin to other user groups.
- The user name assigned to **NE Software Management**, also called **Data Center (DC)**, cannot be the same as a user name that is already used to log in to the U2000.

User Group: This is a collection of the U2000 users that have the same management rights. The attributes of the user groups include general (name, description, user group type, maximum sessions), members, domain, operation rights and current session.

- The U2000 provides the following default user groups: administrator group, maintenance group, monitor group, operator group, and SMManager group.
- The administrator group and security administrator group have operation and maintenance rights for security management, while the other groups do not have security management rights.
- By default, the maintainer group has the rights of any operation set for maintenance, the operator group has the rights of any operation set for operation, and the monitor group has the rights of any operation set for monitoring. The default rights are in the descending sequence of maintainer group rights, operator group rights, and monitor group rights.

NOTE

You can perform **Export operation Sets** operation to view detail operation rights.

Object Set: This is a collection of multiple pieces of managed object. Object sets are established to facilitate the user right management. If a user (or user group) is authorized with the operation rights of an object set, the user (or user group) can perform all the authorized operations on all the objects within the object set. This saves you the trouble of setting the management rights for each NE one by one. Object sets can be created by geographical area, network layer, equipment type and so on.

Operation Set: This is a collection of client-side operations. Operation sets are established to facilitate the user right management. Different client-side operations have different impacts on the system security. Those operations that impose similar impacts on the system security are allocated to the same operation set. In this way, if a user (or user group) is authorized with the rights of an operation set, the user (or user group) can perform all the operations in the operation set. The U2000 has default operation sets. If the default operation sets do not meet the requirements for the right allocation, you can create new operation sets as required.

Account Policy and Password Policy

Account Policy: The password policy specifies the minimum length of the user name, login policy, and unlock policy. You can set the account policy to ensure account security.

Password Policy: The password policy specifies the password complexity, update period, and character restrictions. Using the password policy prevents users from setting a very simple password or using the same password for a long time.

Client Access Control

Remote Maintenance User Management: The U2000 supports the remote maintenance. It allows a remote maintenance terminal to log in to the U2000 server to perform operations on the NEs managed by the U2000. This is a way of maintenance that is commonly used during the remote equipment fault location and the scheduled check. The remote maintenance user is the U2000 user that logs in to the U2000 server through the remote maintenance client. By default, the remote maintenance user is disabled. Before you start the remote maintenance, you need to enable the remote maintenance user, and set related parameters of the user as required.

SSL Protocol: If the server and the client communicate by the SSL protocol, the data interchanged between the server and the client is encrypted. In this way, the security of the network data is guaranteed.

Single-User Mode: If the U2000 switches from the multiuser mode to the single-user mode, all other users are forced to log out and cannot log in again unless the multiuser mode is enabled. If no user is logged in under the single-user mode, only the user that has the right of switching user mode can log in to the U2000.

Client Lockout: To ensure the network security, the U2000 locks out a U2000 client if the user does not perform any operations on the client for a long time. This operation only locks out the client, but not affect the normal running of the U2000.

Role-Based and Domain-Based Management

The role-based and domain-based management is based on the allocation of the object set and operation set. The role-based management function (operation set) enables you to divide the U2000 rights to different function domains. The domain-based management function (object set) enables you to construct different network domains in unit of NE. You can easily control the user rights by entitling the rights of any function domain and network domain portfolio to a U2000 user.

Usually you can use the following two ways to allocate rights to a user or a user group:

- Add a user to a user group. The user added to the user group enjoys all the rights of the user group. This way is always used to allocate basic user rights.
- Adjust user rights. Some operation rights can be added or deleted. This way is always used when the current user or user group does not meet the requirements for the user right. Operation rights of the default user and user groups be adjusted except admin user, administrators user group, and SMMManager user group.

ACL

The ACL is a secure access control mechanism. It restricts a user to log in to the server through only the clients with the specified IP addresses.

ACL can effectively control the client IP address from which the user can log in to the U2000. In this case, even if the user account and the password are obtained by illegal users, these users cannot log in to the U2000, thus the U2000 security is improved. The U2000 provides two ACLs:

- System ACL
The ACL of the entire U2000. All the users can log in to the U2000 only through specific IP addresses or network segments.
- User ACL
The ACL of a user. The current user can log in to the U2000 only through specific IP addresses or network segments.



The IP addresses or the network segments for the user ACL need to be within the range of the IP addresses or the network segments for the system ACL.

Network Management System Maintenance Suite

To ensure the security of the network management system, the password for the network management system maintenance suite should be modified periodically.

4.2.5 Log Management Policy

Log security management includes the U2000 operation log, U2000 security log, NE security log, log dump, and log forwarding management.

Operation Log and Security Log

Operations and operation results of all the U2000 users are recorded in the U2000 operation log or security log.

- U2000 operation log: Records user operations irrelevant to the security on the client. For example, scheduled alarm acknowledgement and NE time synchronization.
- U2000 security log: Records user operations relevant to the security on the client. For example, creating a user and setting the user operation rights.

The U2000 provides a log browse function. You can also filter logs according to operation user, operation terminal, log type, severity level, and start and end time.

By querying logs, the administrator can track and check user operations. Pay close attention to operation logs. This helps you to learn the running information of the system. The logs keep a record of events relevant to the equipment operations. For example, querying, creating, and deleting an NE or other objects. The logs also help you to learn the user activities. For example, you can view operations performed by a user in the system.

NE Security Log

Operations and operation results of all the NE users are recorded in the NE security log. The U2000 provides an NE log browse function. You can also filter the logs according to the NE user name, event name, and start and end time. You can view but not delete the NE security log.

Log Dump

By setting the scheduled task dump, you can enable the U2000 to periodically save the log to a specified directory. This function facilitates log viewing, reduces records in the database, and speeds up the running of the system. By default, the dump path of the security log is **NMS installation path/server/dump/ThresholdExport/Log**. The dumped log can be saved in CSV or XML format.

Log Forwarding

U2000 log forwarding: The U2000 can forward the U2000 operation log to the Syslog server, and save all operations. This function provides references for maintenance and relieves the storage burden of the U2000 server.

NE log forwarding: The U2000 forwards various types of NE information to the Syslog server in a format that complies with the system log protocol. Network management and maintenance personnel can learn the NE status according to emergency of the information.

4.2.6 Security of the System Data

Periodically and efficiently backing up the applications and data of the NMS is a powerful way to ensure the system security. Malicious and undesigned security threats cannot be avoided. If a security incident occurs and degrades the system security, the backup scheme can be used to restore the system in time. This is an indispensable security measure for the NMS.

- **Manually backing up the database:** You can manually back up the database as required. For example, you must back up the database to avoid data loss before performing risky operations.
- **Regularly backing up the database:** You can set the policy of regularly backing up the database. Then, you can restore the data through the backup data as required.
- **Dumping data:** You can export the data in the database through manual dumping or automatic dumping and save the data to other locations.



NOTE

The dumped data is deleted from the database.

4.2.7 NE Security Management

The NE security management includes NE access control, NE user management, NE operation right management and NE data security management.

NE Access Control

LCT Access Control: If you need to use the U2000 LCT or Web LCT for the NE management and commissioning, you can enable the LCT access control so that the LCT can access the NE.

ACL: The access control list (ACL) provides the basic filtering function for the data flow. All NEs that have the ACL configured can determine whether to filter out an IP packet when the IP packet passes the NE. The ACL controls the direction of a specific data flow as to whether the data flow is transmitted in or out of a network.

Communication Port Access Control: An NE can access the U2000 by using the OAM, COM, Ethernet port or serial port. You can set the port for the NE access by enabling the access control of the port. By default, an NE is allowed to access the U2000 by Ethernet ports.

NE User Management

NE User: To ensure the security of the NE data, you must use the previously created NE user to log in to the NE. Also, you can only perform the operations that are authorized to the NE user.

NE User Level: According to the operation types authorized to a user, the NE users are regarded as having different operation levels. This level is known as the NE user level. The NE users of different levels are allocated to different NE user groups.

NE Security Parameters: According to the security settings of the NE, an NE automatically determines whether the password of the NE user remains valid, and whether the NE user is allowed to log in. The network manager should know the security settings of the NE, and modify the password of the NE user before it expires. The NE security parameters include the following: **Allowable Used Times for Outdated Password, Password Max. Valid Period, Password**

Min. Valid Period , Password Uniqueness, Lock Testing Time, Allowable illegal Access Times and Lock Time.

NE Operation Rights

NE Operation Rights: The operation right of NE users has different levels. The user with a higher right level can perform all operations that are authorized to a user with a lower right level. For example, the user of the operation level has all the operation rights authorized to the user of the monitor level. The following describes what operations are authorized to each level.

For Non-NA NEs, the NE user has the following five levels in ascending order: monitor level, operation level, maintenance level, system level, and debug level. The authorities of the five user levels are as follows:

- Monitor level: all the query commands, login, logout, password modification
- Operation level: all the fault and performance settings, part of security settings, part of configurations
- Maintenance level: part of security settings, part of configurations, communication settings, log management
- System level: all the security settings, all the configurations
- Debug level: all the security settings, all the configurations, debug commands

For the NA NEs, the NE user has the following four levels in ascending order: RTRV, MAINT, PROV, and SUPER. The authorities of the four user levels are as follows:

- RTRV: This user level has the right to use all query commands, to log in, to log out, and to change its own password.
- MAINT: This user level has all fault performance authorities, some security authorities, and some configuration authorities.
- PROV: This user level has some security authorities, some configuration authorities, the communication setting authority, and the log management authority.
- SUPER: This user level has all security and configuration authorities.

Authority Management: To ensure the security of the NE data, any one who wants to perform operations for an NE must log in to the NE as an NE user, and can only perform the operations authorized to this user. It is recommended that you create an NE user before configuring services. Make sure that when you create a common user account that can be used on all NEs, keep the right levels consistent to avoid the disorder of user right.

NE Data Backup/Restoration

NE Data Backup: Backing up the NE database is necessary for the daily maintenance. With the backup of the database, the NE can automatically restore the NE data and run normally in case the data in SCC is lost or the equipment powers off.

NE Data Restoration: During the daily maintenance, if an NE becomes faulty, the NE data is restored based on the data backup on the SCC or CF card.

4.3 Configuring Communications Security

This topic describes the policies for communications security of the U2000, including southbound communications security, northbound communications security, inter-server communications security, and client communications security, and how to configure the client

to communicate with equipment through the SSH protocol and configure the server to communicate with the client through the SSL protocol.

[4.3.1 Communication Security](#)

This topic describes the security protocols related to the U2000.

[4.3.2 Enabling a Device to Communicate with the Server through the SSH Protocol](#)

The SSH is a tool that is similar to Telnet. The difference is that the SSH encrypts the data during the transmission. The U2000 server communicates with the devices in SSH encryption authentication mode to ensure the security of data transmission.

[4.3.3 Setting the Communications Between the Server and the Client Through the SSL Protocol](#)

When you set the communication mode between the server and the client, you can use the Security Socket Layer (SSL) mode to ensure that the communication is secure.

4.3.1 Communication Security

This topic describes the security protocols related to the U2000.

[4.3.1.1 Southbound Communication Security](#)

This topic describes the interfaces related to the southbound communication security of the U2000.

[4.3.1.2 Northbound Communication Security](#)

This topic describes the interfaces related to the northbound communication security of the U2000.

[4.3.1.3 Communication Security Among Distributed Nodes](#)

This topic describes the protocols that are used to ensure the communication security among distributed nodes.

[4.3.1.4 Client Communication Security](#)

This topic describes the policies that ensure the communication security between the client and the server.

4.3.1.1 Southbound Communication Security

This topic describes the interfaces related to the southbound communication security of the U2000.

Qx Interface

The Qx interface adopts the private OptiX management protocol developed by Huawei. Through the Qx interface, the U2000 is connected to the OptiX series equipment.

SNMP SBI

The SNMP interface is compliant with the SNMP V1, V2, and V3 standards. Through the SNMP interface, the U2000 is connected to the Access Network equipments, routers, and switches.

cli SBI

Through the cli interface, the U2000 is connected to routers, switches, and security products.

4.3.1.2 Northbound Communication Security

This topic describes the interfaces related to the northbound communication security of the U2000.

The U2000 provides SNMP, CORBA, and XML NBIs. The U2000 can be interconnected with different third-party NMSs flexibly through NBIs, to provide the information about physical inventory and alarms to the upper-layer NMSs.

Table lists the equipment and their features that the NBIs of the U2000 support.

Interface Type	Equipment	Features and Functions
XML	MSTP, WDM, NA WDM, RTN, SONET, PTN, router, switch, security equipment, Access Network equipment	Physical inventory, alarm
CORBA	MSTP, WDM, NA WDM, RTN, SONET, PTN, router, switch, security equipment, Access Network equipment	Alarm
SNMP	MSTP, WDM, NA WDM, RTN, SONET, PTN, router, switch, security equipment, Access Network equipment	Alarm

XML NBI

The U2000 provides comprehensive graphical management for Huawei equipment and further enhances the XML NBI. Through the XML NBI, the U2000 is connected to the integrated NMSs or OSSs of telecom carriers. Based on the Hypertext Transfer Protocol (HTTP) and the SOAP/WebServices of the JMS Server, the XML NBI supports HTTP and SSL (HTTPS). The two protocols are mutually exclusive in application.

The inventory query function is performed by the `getInventory` service. The OSS calls the `getInventory` service of the XML NBI to know the status and usage of the resources in the management scope of the U2000.

The service provisioning function is performed by the `ProvisionRequest` service. The OSS calls the `ProvisionRequest` service of the XML NBI to configure data for the equipment and implement service availability.

The XML NBI of the U2000 performs the following functions:

- Manage physical inventory. The XML NBI supports the ability to query physical fibers or cables, and to query the inventory that includes ports on the physical equipment. The physical inventory includes NE, chassis or shelf, slot, sub slot, board, daughter board, physical port, physical fiber or cable. In addition, the XML NBI supports notifications of creating, modifying, and deleting the physical inventory.
- Manage alarms. The XML NBI supports the ability to obtain the active alarms, receive the alarm notifications sent by the NMS, and acknowledge and anti-acknowledge alarms.

CORBA NBI

The CORBA interface is one of the universal standard interfaces in the telecommunication field. Through the CORBA interface, the EMS and NMS from different vendors can be interconnected to perform management functions.

TMF multi-technology network management (MTNM) defines the CORBA based interface between NMS and EMS, and has been recognized by more and more equipment vendors.

The CORBA NBIT provided by the U2000 is compliant with the TMF513, TMF608, and TMF814 Recommendations.



NOTE

The U2000 provides two standard CORBA interfaces, that is, the T2000 CORBA interface and iMAP CORBA interface.

SNMP NBI

The SNMP NBI is one of the universal standard interfaces in the telecommunication field. Through the SNMP interface, the U2000 can connect to the upper-layer NMS of the telecom carrier or another vendor. The SNMP NBI provides the alarm reporting function.

The SNMP interface provided by the U2000 is compliant with the SNMP V1, V2 and V3 standards.

TL1 NBI

With rapid growth and large-scale application of networks, NMS needs to manage key services across equipment from different vendors in a centralized manner. The NMS of an equipment manufacturer mainly manage its own equipment, and provides NBIs to interconnect to the integrated NMS of the telecom carrier and the OSS. In this way, the key services across equipment from different vendors are managed in a centralized manner.

The U2000 provides a provisioning interface to connect to the OSS. The OSS enhances its functions based on this interface, and provides service handling automation. This interface is based on the TCP protocol.

The U2000 inventory resource interface connects to the OSS resource management system so that the users manage network resources in a centralized manner. This interface is based on the TCP protocol.

The TL1 interface of the U2000 mainly implements the preceding two functions. The details are as follows:

- Manage VLAN services.
- Manage Ethernet services.
- Manage permanent virtual channels (PVCs).
- Manage service ports.
- Manage the services related to an xDSL port.
- Manage gigabit passive optical network (GPON) services.
- Manage multicast services.
- Manage V5 services.
- Provision voice over IP (VoIP) services.

- Manage BRAS services.
- Manage ACL and QoS.
- Manage equipment physical resources.
- Manage PVCs, service ports, and other logical resources.
- Manage resource change notifications.

4.3.1.3 Communication Security Among Distributed Nodes

This topic describes the protocols that are used to ensure the communication security among distributed nodes.

The Secure Socket Layer (SSL) protocol is supported on the communication among the distributed nodes of the NMS. Encrypting transmitted data ensures that the data is not intercepted, captured, or tampered. Thus, the anti-attack capability of the NMS can be improved.

4.3.1.4 Client Communication Security

This topic describes the policies that ensure the communication security between the client and the server.

The SSLv3 protocol is supported on the communication between the NMS client and the server. The SSLv3 protocol provides the following services:

- Authenticating the validity of the client and server
- Encrypting data to hide the transmitted data and ensuring that the data transmitted between the client and server is not intercepted
- Protecting the data integrity and ensuring that the data is not tampered by the third party

4.3.2 Enabling a Device to Communicate with the Server through the SSH Protocol

The SSH is a tool that is similar to Telnet. The difference is that the SSH encrypts the data during the transmission. The U2000 server communicates with the devices in SSH encryption authentication mode to ensure the security of data transmission.

- This feature is used to enabling a device to communicate with the server through the SSH protocol related to routers, switches, and service gateways.
- The device must support the SSH settings if you log in to the device in SSH mode. For the detailed settings, see the configuration guide of the device. This topic take NE40E router for example.

Configuration on the NEs



NOTE

The SSH user can be authenticated in four modes: password, RSA, password-rsa, and all.

- When the SSH adopts the password or password-rsa authentication mode, configure a local user with the same name.
- When the SSH user adopts the RSA, password-rsa, or all authentication modes, the server should save the RSA public key for the SSH client.

1. In the system view, run the following command:

system-view

2. Generate a local key pair on the server, run the following command:

rsa local-key-pair create

3. Configure the VTY user interface.

user-interface vty 0 14**authentication-mode aaa****protocol inbound all****quit**

4. Create SSH user Client001.

- (1) Configure the password authentication for the SSH user Client001.

ssh user client001**ssh user client001 authentication-type password**

- (2) Configure the password of the SSH user Client001 to huawei.

aaa**local-user client001 password simple huawei****local-user client001 service-type ssh****local-user client001 level 3****quit**

5. Create SSH user Client002 and configure the rsa authentication for the SSH user Client002.

ssh user client002**ssh user client002 authentication-type rsa**

6. Configure the RSA public key on the server.

- (1) Generate a local key pair on the client.

system-view**sysname client002****rsa local-key-pair create**

- (2) View the RSA public key generated on the client.

display rsa local-key-pair public

- (3) Send the RSA public key generated on the client software to the server.

rsa peer-public-key RsaKey001

Enter "RSA public key" view, return system view with "peer-public-key end".

public-key-code beginEnter "RSA key code" view, return last view with "public-key-code end".
30818702 8181009D 11136259 D9380276 0F0F8561 33CE9EA1 4E0B124F B9DED240
B3AD26F2 E57EAF50 559BF99F 38EFE30A 13512BB3 DD95CF81 C5A7A965 2A89C41B
9DF4AAD0 77AD8B7C 2EAC30EA AEAE8B90 B2DAA408 6FA1964F 286FA7C9 1D5FDEFA
4800895C FBB0CF11 A1B9DF94 3FE751D6 F37E33EF BCA92881 E8268E92 3972697D
5E3901DB 2E6EFD02 0125**public-key-code end****peer-public-key end****quit**

7. Bind the SSH user Client002 to the RSA public key of the SSH client.

ssh user client002 assign rsa-key RsaKey001

8. Enable the STelnet service on the SSH server.

stelnet server enable

9. Configure the STelnet service for the SSH users Client001 and Client002.

ssh user client001 service-type stelnet

ssh user client002 service-type stelnet

Configuration on the U2000

1. On the device navigation tree or in the topological view, select a device, right-click, and choose **Tool > SSH**.
2. In the dialog box that appears, set the parameters.

For example, set **Authentication** to **By private key** and **User Name** to **usera**.



3. Click **OK**.

4.3.3 Setting the Communications Between the Server and the Client Through the SSL Protocol

When you set the communication mode between the server and the client, you can use the Security Socket Layer (SSL) mode to ensure that the communication is secure.

Context

- 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 procedure for enabling the SSL mode varies according to the OS.

NOTE

- If the client and server applications are on the same host and the server uses the **SSL** mode, then the client can use the **Common** or **SSL** mode. The client can only use the **Common** mode if the server uses the **Common** mode.
- If the client and server applications are not on the same host, the client can log in to the server only when it uses the same mode as the server.

Procedure

- Single-Server System (Windows):
For details about how to set the communication mode on the U2000 server for the single-server system (Windows), see [A.9.50 How to Set the Communication Mode on the U2000 server for the Single-Server System \(Windows\)](#).
- Single-Server System (Solaris)
For details about how to set the communication mode on the U2000 server for the single-server system (Solaris), see [A.9.51 How to Set the Communication Mode on the U2000 server for the Single-Server System \(Solaris\)](#).
- Single-Server System (SUSE Linux-Distributed)
For details about how to set the communication mode on the U2000 server for the single-server system (Linux), see [A.9.52 How to Configure the Communication Mode for a Linux-based U2000 Server?](#).
- High Availability System (Windows)
For details about how to set the communication mode on the U2000 server for the High Availability System (Windows), see [A.9.53 How to Set the Communication Mode on the U2000 Server for the High Availability System \(Windows\)](#).
- High Availability System (Solaris)
For details about how to set the communication mode on the U2000 server for the High Availability System (Solaris), see [A.9.54 How to Set the Communication Mode of the Server in a High Availability System \(Solaris\)?](#).
- High Availability System (SUSE Linux-Distributed)
For details about how to set the communication mode on the U2000 server for the High Availability System (Linux), see [A.9.55 How to Set the Communication Mode of the Server in a High Availability System \(SUSE Linux-Distributed\)](#).

----End

4.4 Setting Security Policies of U2000 Users

A user of the SMManagers group can set the password policy and account policy of the U2000 user, to enhance the security.

4.4.1 Changing the admin User Password

You need to periodically change the password of U2000 admin user to avoid password disclosure.

4.4.2 Setting the U2000 Login Mode

The U2000 provides two login modes: multiuser mode and single-user mode. In normal state, the U2000 runs in multiuser mode. When you need to maintain the U2000 server (for example, changing the user group, managed domain, or operation rights of a user), you can set the U2000 to run in single-user mode to avoid the interference from other users.

4.4.3 Setting the Access Control List

By setting the system or current user access control list (ACL), a user of the SMManagers can allow the client or user to log in to the U2000 from the computer with specified IP address or network segment.

[4.4.4 Setting the Password Policy](#)

To improve U2000 security, a user of the SMMangers group can set the password policy to prevent the user from using insecure passwords.

[4.4.5 Setting the Account Policy](#)

A user of the SMMangers group can set the account policy to ensure account security.

4.4.1 Changing the admin User Password

You need to periodically change the password of U2000 admin user to avoid password disclosure.

Procedure

- 1 Log in to the U2000 client.
- 2 Choose **File > Change Password** from the main menu.
- 3 In the **Change Password** dialog box, set the new password for the admin user.
- 4 Click **OK**.
- 5 Click **OK**.

----End

4.4.2 Setting the U2000 Login Mode

The U2000 provides two login modes: multiuser mode and single-user mode. In normal state, the U2000 runs in multiuser mode. When you need to maintain the U2000 server (for example, changing the user group, managed domain, or operation rights of a user), you can set the U2000 to run in single-user mode to avoid the interference from other users.

Context

Only the **admin** user can set the U2000 login mode.



CAUTION

Only the admin user can log in to the U2000 through a client and all the other users are forced to log out after the U2000 is switched from the multiuser mode to single-user mode. Switch to the multiuser mode after you complete the operations in the single-user mode to ensure that others can use the U2000 normally.

Procedure

- 1 Choose **File > Preferences** from the main menu.
- 2 In the **Preferences** dialog box, choose **System Login Mode** in the navigation tree on the left.

System Login Mode (Server Setting)

Please select a login mode. The selected login mode is applied to the current server logged in. The IP address of the server is 10.71.227.242.

☐ Single-user mode: Only one superuser can log in to the server at the same time. If another user is already logged, the user is forcibly logged out.

☒ Multiuser mode: Multiple users can log in to the server at the same time.

- 3 Set the U2000 login mode in the area on the right.

Setting Login Mode	Operations
Switch to a single-user mode	Choose Single-user mode and click OK. In the Set Switch Delay dialog box, set the delay of login mode switch, and then click OK. ● If the delay time is not 0, a dialog box is displayed. After the switch delay, the U2000 is switched to the single-user mode. ● If the delay time is 0, the warning dialog box is not displayed. The U2000 is switched to the single-user mode immediately. On the status bar, the single-user mode information is displayed. It indicates that the U2000 works in single-user mode.
Switch to a multiuser mode	Choose Multiuser mode, and then click OK. The U2000 is switched to the multiuser mode immediately. On the status bar, the multiuser mode information is displayed. It indicates that the U2000 works in multiuser mode.

----End

4.4.3 Setting the Access Control List

By setting the system or current user access control list (ACL), a user of the SMManagers can allow the client or user to log in to the U2000 from the computer with specified IP address or network segment.

Context

- The admin user has the permission to set the ACL of any user in the U2000. The user in the security administrator group has the permission to set the ACLs of the other users except the admin.
- The system ACL allows all the U2000 users to log in to the U2000 only through the clients of the specific IP addresses or network segment. The user ACL is a subset of the system ACL. The user ACL is effective only for the current user.



CAUTION

If there are multiple network adapters on the host where the client exists, you need to add the IP addresses of all network adapters to the ACL. This ensures that the U2000 client logs in normally.

Procedure

- Set the system ACL.
 1. Choose **Administration > NMS Security > ACL** from the main menu.
 2. In the **ACL** dialog box, set the system ACL.

Set the system ACL	Operation
Add a system ACL item	Click Add. In the New System Access Control Item dialog box, select the display mode of the IP address, set the related parameters, and then click OK. NOTE ● If the display mode of the IP address is Address or network segment, set the parameters IP address or network segment and Description. ● If the display mode of the IP address is Start IP address - end IP address, set the parameters Start IP Address, End IP Address, and Description.
Modify a system ACL item	1. In the ACL dialog box, select the system ACL item to be modified, and then click Modify. 2. In the Modify System Access Control Item dialog box, modify the related parameters, and then click OK. NOTE You cannot modify a display mode of an IP address directly. To modify a display mode of an IP address, you can delete a system ACL item and then add a new system ACL item.
Delete a system ACL item	In the ACL dialog box, select the system ACL item to be deleted, and then click Delete. In the Confirm dialog box, click Yes.

- Use the user ACL.
 1. Choose **Administration > NMS Security > NMS User Management** from the main menu.
 2. In the **NMS User Management** navigation tree, expand the **User** node, and then select a user.
 3. On the right of the interface, click the **ACL** tab and set the user ACL.
 - Use all the ACLs in the system: The ACL is not separately set for the user. Instead, the system ACL is used to control the IP addresses and network segments that the user can use for login.

- Use the specified ACLs: The ACL is separately set for the user. The items in the user ACL must be selected from the system ACL. That is, the user ACL is a subset of the system ACL, and it functions for the current user only.

 NOTE

- Use all ACLs in the system: An ACL is not separately set for a user. Instead, the system ACL is used to control the IP addresses and network segments that the user can use for login.
- Use a specified ACL: An ACL is set for a specified user. The items in a specified ACL must be selected from the system ACL. That is, the ACL is a subset of the system ACL, and it functions for a specified user only.
- After you click **Set ACL** at the lower right corner of the **ACL** tab page, the system ACL dialog box is displayed. You can modify the system ACL in the dialog box.

----End

4.4.4 Setting the Password Policy

To improve U2000 security, a user of the SMMangers group can set the password policy to prevent the user from using insecure passwords.

Context

- After the password policy is modified, the modification takes effect immediately for all user of the U2000. For example, after the minimum length of the user password is changed, when the online user changes a password, the minimum password length must comply with the password policy.
- The password policy specifies the password complexity, update period, and character restrictions. Using the password policy prevents users from setting a very simple password or using the same password for a long time.

Procedure

- 1 Choose **Administration > NMS Security > Security Policies** from the main menu.
- 2 In the **Security Policy** dialog box, click the **Password Policy** tab.

3 Set the basic and advanced parameters of the password policy as required.

4 Click **OK**.

----End

4.4.5 Setting the Account Policy

A user of the SMMangers group can set the account policy to ensure account security.

Procedure

1 Choose **Administration > NMS Security > Security Policies** from the main menu.

2 In the **Security Policy** dialog box, click the **Account Policy** tab.

3 Set the account policy as required.

4 Click **OK.**

----End

5 Commissioning the Communication Between the Server and an Independent Client

By logging in to an independent client, you must ensure that the independent client properly communicates with the server. Log in to a U2000 using the client, and then perform management operations in the GUI of the U2000 client.

Prerequisite

Before logging in to the U2000 client, ensure that the following conditions are met:

- The U2000 processes are started.
- The network communication between the U2000 client and the U2000 is available.

NOTE

Run the **ping peer_IP_address** command to check network communication.

- In a single-server system (centralized), the IP address is the system IP address of the server.
- In a single-server system (distributed), the IP address is the system IP address of the master server.
- In a high availability system (centralized), the IP address is the IP address of NMS application network in the active site server.
- In a high availability system (distributed), the IP address is the IP address of NMS application network in the master server of active site.
- The ports used between the U2000 client and the U2000 are opened by the firewall. See [F.3 Ports Between the U2000 Server and the Clients](#).
- The IP address of the client must be contained in the access control list (ACL) that is configured on the U2000.

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 [4.4.3 Setting the Access Control List](#).

- The legitimate U2000 user account and password must be allocated.

Context

Here, the U2000 client is an independent client. An independent client refers to the system where only the U2000 client program is installed.

By default, after you enter an incorrect password for three consecutive times, the user account that you use is locked by the U2000. The super user **admin** can unlock the account of a common user. In addition, the system can automatically unlock the account in 30 minutes.

Procedure

- 1 Log in to the OS where the client program is installed.
 - On Windows OS, log in to the OS as user **administrator**.
 - On Solaris OS, log in to the GUI as user **nmsuser**.
- 2 On the OS desktop, double-click the **U2000 Client** shortcut icon. The **Login** dialog box is displayed.

 **TIP**

 - In the case of a Windows OS, you can double-click the **startup_all_global.bat** file in the **D:\U2000\client** directory to start the client.
 - In the case of a Solaris OS, you can run the command of **./startup_all_global.sh** in the **/opt/U2000/client** directory to start the client.
- 3 In the **Server** drop-down list, select the server to be logged in to. Then, set **User Name** and **Password** to the valid values, and click **Login**.
 - If the intended server is not configured, perform the following operations to add a server:
 1. Click the **...** button. In the **Server List** dialog box, click **Add**.
 2. In the **Add Server Information** dialog box, set the parameters of the U2000 server to be added, and then click **OK**.

Table 5-1 Server parameter settings

Parameter	Settings
Name	It is recommended that you set this parameter to the IP address for login or the related host name.
Server Name (or IP Address)	It is recommended that you set this parameter to an IP address. ● In a single-server system (centralized), the IP address is the system IP address of the server. ● In a single-server system (distributed), the IP address is the system IP address of the master server. ● In a high availability system (centralized), the IP address is the IP address of NMS application network in the active site server. ● In a high availability system (distributed), the IP address is the IP address of NMS application network in the master server of active site.

Parameter	Settings
Port	There are two data transmission modes, namely, Common and Security(SSL) . By default, port 31037 is used in Common mode and port 31039 is used in Security(SSL) mode.
Mode	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. ● For details about how to set the communication mode on the U2000 server for the single-server system (Windows), see A.9.50 How to Set the Communication Mode on the U2000 server for the Single-Server System (Windows). ● For details about how to set the communication mode on the U2000 server for the single-server system (Solaris), see A.9.51 How to Set the Communication Mode on the U2000 server for the Single-Server System (Solaris). ● For details about how to set the communication mode on the U2000 server for the single-server system (Linux), see A.9.52 How to Configure the Communication Mode for a Linux-based U2000 Server?. ● For details about how to set the communication mode on the U2000 server for the High Availability System (Windows), see A.9.53 How to Set the Communication Mode on the U2000 Server for the High Availability System (Windows). ● For details about how to set the communication mode on the U2000 server for the High Availability System (Solaris), see A.9.54 How to Set the Communication Mode of the Server in a High Availability System (Solaris)?. ● For details about how to set the communication mode on the U2000 server for the High Availability System (Linux), see A.9.55 How to Set the Communication Mode of the Server in a High Availability System (SUSE Linux-Distributed). NOTE ● If the client and server applications are on the same host and the server uses the SSL mode, then the client can use the Common or SSL mode. The client can only use the Common mode if the server uses the Common mode. ● If the client and server applications are not on the same host, the client can log in to the server only when it uses the same mode as the server.

3. In the **Server List** dialog box, select a record from the record list. Then, click **OK**.
- When you log in to the U2000 client, if the system detects that the local version is earlier than the server version, a prompt is displayed, asking you whether to upgrade the client.
 - Click **Yes** to upgrade the client.

- Click **No** to log in to the client.

----End

Result

After the login to the U2000 client is successful, the U2000 client obtains related data from the U2000.

6 Commissioning the Communication Between the NMS and NEs

About This Chapter

By commissioning the communications between a U2000 and NEs, you must ensure that the U2000 can manage all added NEs. For the details about NE management, see the Help.

[6.1 Pre-configuration Requirements on the NE Side](#)

This topic describes the pre-configuration requirements on the NE side. An NE to be added to the U2000 must be running normally so that it can be managed by the U2000 after being added.

[6.2 Setting the Parameters for the Communication Between the U2000 and NEs](#)

This topic describes how to set parameters for the communication between the U2000 and NEs. Properly setting these parameters is the prerequisite to the normal communication between the U2000 and NEs. You need to set these parameters in time.

[6.3 Creating a Topology Subnet](#)

The subnet created here is based on a topological concept to facilitate management. In the case of topology objects in the same network area or with similar attributes, you can allocate them in one topology subnet.

[6.4 Creating a Single NE](#)

You need to create an NE before you can manage it by using the U2000. Although creating a single NE is not as fast and accurately as creating NEs in batches. The method of creating the NE of different types cannot be the same.

[6.5 Creating Optical NEs](#)

The U2000 manages the WDM equipment and OptiX BWS 1600S by using optical NEs. There are four types of optical NEs. They are WDM_OADM, WDM_OEQ, WDM_OLA and WDM_OTM. OptiX OSN 1800 only supports WDM_OTM and WDM_OADM. OptiX BWS 1600S only supports WDM_OTM.

[6.6 Creating NEs In Batches](#)

The U2000 supports the ability to search out all NEs according to the IP addresses of NEs, IP address or IP network segment of the GNE, or NSAP addresses of the NEs, and create the NEs in batches. The U2000 also can import and create in batches the NEs that register with the U2000 according to the active registration information of the NEs. Creating NEs by using this method is faster and more reliable than creating the NEs manually.

[6.7 Viewing an NE in the Topology View](#)

This topic describes how to view an NE in the topology view. After an NE is added to the U2000, you can view the NE status in the topology view.

6.1 Pre-configuration Requirements on the NE Side

This topic describes the pre-configuration requirements on the NE side. An NE to be added to the U2000 must be running normally so that it can be managed by the U2000 after being added.

Install and commission the NE according to the manuals delivered along with the NE, ensure the normal running of the NE, and then add the NE to the U2000 for management.

The pre-configuration requirements on the NE side vary according to the NE type.

- Router, switch, Metro Ethernet service, broadband access, voice gateway, WLAN, security gateway, service interception gateway, and SVN series equipment
 1. The NE must be powered on and running normally.
 2. An IP address must be set for the NE.
 3. Login parameters must be set for the NE.
 4. The route between the NE and the U2000 must be reachable.
 5. SNMP parameters must be set for the NE.
- MSTP, WDM, RTN, PTN, and submarine cable series equipment
 - Gateway NEs
 1. The NE must be powered on and running normally.
 2. An IP address must be set for the NE.
 3. The route between the NE and the U2000 must be reachable.
 - Non-gateway NEs
 1. The NE must be powered on and running normally.
 2. The non-gateway NE must set up communication with the gateway NE through the ECC channel or extended ECC channel.
 3. The gateway NE must be added to the NMS.

6.2 Setting the Parameters for the Communication Between the U2000 and NEs

This topic describes how to set parameters for the communication between the U2000 and NEs. Properly setting these parameters is the prerequisite to the normal communication between the U2000 and NEs. You need to set these parameters in time.

6.2.1 Protocols for Communications Between the U2000 and NEs

This topic describes the protocols for communications between the U2000 and NEs.

6.2.2 Setting SNMPv1/v2c Parameters on NEs

This topic describes how to set SNMPv1/v2c parameters on NEs. Before an NE is created on the U2000, you need to set SNMP parameters on the NE through commands. Generally, the applied SNMP version is v1 or v2c.

6.2.3 Setting SNMPv3 Parameters on NEs

This topic describes how to set SNMPv3 parameters on NEs. Before an NE is created on the U2000, you need to set SNMP parameters on the NE through commands. In comparison,

SNMPv3 features higher security than SNMPv1 or SNMPv2c. You can use SNMPv3 to ensure the communications between the U2000 and NEs.

6.2.4 Configuring the Default SNMP Parameters Template

This topic describes how to correctly set the default SNMP parameters on the U2000 to ensure the normal communication between the U2000 and the managed NEs.

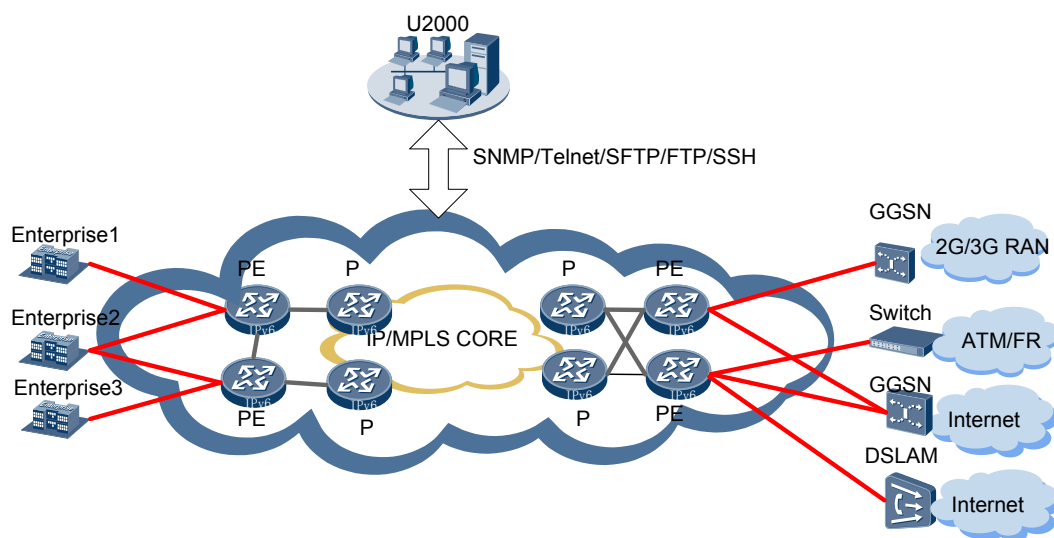
6.2.1 Protocols for Communications Between the U2000 and NEs

This topic describes the protocols for communications between the U2000 and NEs.

Communications between the U2000 and NEs in the IP/access domain

Figure 6-1 shows the topology for the communication between the U2000 and NEs in the IP domain.

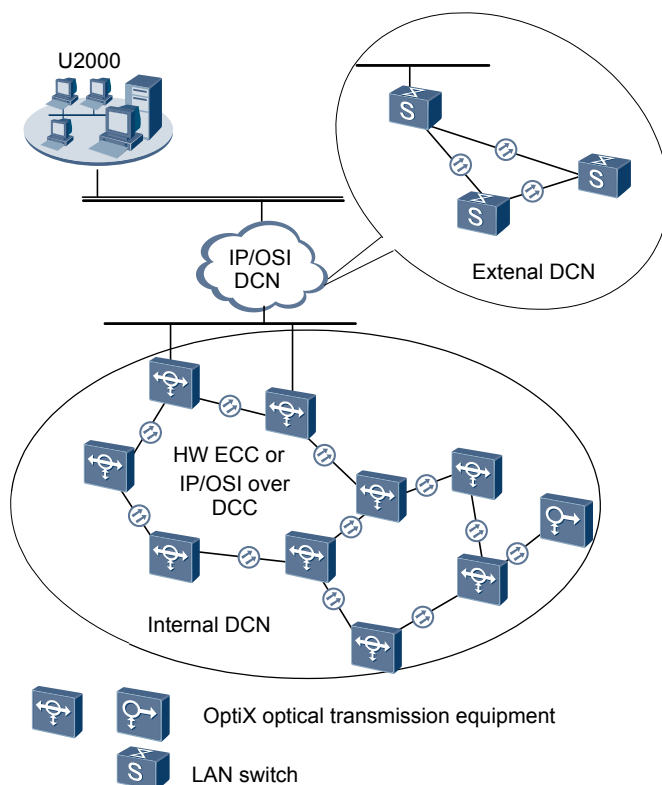
Figure 6-1 Topology for communications between the U2000 and NEs in the IP/access domain



The SNMP and Telnet parameters need to be set for the NEs such as routers, switches, Metro Ethernet, security gateways, service interception gateways, SVN NEs, and access NEs,.

Communications between the U2000 and NEs in the transport domain

The NMS manages and maintains NEs by communicating with NEs through TCP/IP and the OSI protocol. **Figure 6-2** shows the topological diagram of the communications between the NMS and NEs.

Figure 6-2 Topology for communications between the U2000 and NEs in the transport domain

The NEs in the transport domain support two types of protocols for communications with the U2000. The MSTP, WDM, RTN, PTN and Marine cable NEs support the TCP/IP, and OSI protocols. The NG WDM and the NA OTN, however, do not support the OSI protocol.

6.2.2 Setting SNMPv1/v2c Parameters on NEs

This topic describes how to set SNMPv1/v2c parameters on NEs. Before an NE is created on the U2000, you need to set SNMP parameters on the NE through commands. Generally, the applied SNMP version is v1 or v2c.

Context

It is applicable to the Router series, Switch series, Security series NEs.

The prerequisites for the U2000 to discover and manage NEs through SNMP are as follows:

- SNMP parameters must be set correctly on NEs.
- The default SNMP parameters on the U2000 must be consistent with the SNMP parameters set on NEs.

Procedure

- 1 To enter the system view, run the following command:

system-view

- 2 To start the SNMP Agent service, run the following command:

snmp-agent

- 3 To set the SNMP protocol version, run the following command:

snmp-agent sys-info version { { *v1* | *v2c* }* }



NOTE

For the meaning of every field in the command, see the command reference of the associated NE.

- 4 To set the read community name, run the following command:

snmp-agent community read *community-name* [[**mib-view** *view-name*]] [**acl** *acl-number*]]*

- 5 To set the write community name, run the following command:

snmp-agent community write *community-name* [[**mib-view** *view-name*]] [**acl** *acl-number*]]*

----End

Example

The following takes the setting of basic SNMPv1 parameters on a router as an example.

- Set **SNMP version** to **v1**.
- Set **Read community name** to **public**.
- Set **Write community name** to **private**.

After the CLI of the router is displayed, do as follows:

1. Enter the **system-view** command, and then press **Enter**.
2. Enter the **snmp-agent** command, and then press **Enter**.
3. Enter the **snmp-agent sys-info version v1** command, and then press **Enter**.
4. Enter the **snmp-agent community read public** command, and then press **Enter**.
5. Enter the **snmp-agent community write private** command, and then press **Enter**.

The setting of basic SNMPv1 parameters is complete.

```
<NE40E-81>system-view
Enter system view, return user view with Ctrl+Z.
[NE40E-81]snmp-agent sys-info version v1
[NE40E-81]snmp-agent community read public
[NE40E-81]snmp-agent community write private
[NE40E-81]
```

6.2.3 Setting SNMPv3 Parameters on NEs

This topic describes how to set SNMPv3 parameters on NEs. Before an NE is created on the U2000, you need to set SNMP parameters on the NE through commands. In comparison, SNMPv3 features higher security than SNMPv1 or SNMPv2c. You can use SNMPv3 to ensure the communications between the U2000 and NEs.

Context

It is applicable to the Router series, Switch series, Security series NEs.

The prerequisites for the U2000 to discover and manage NEs through SNMP are as follows:

- SNMP parameters must be set correctly on NEs.
- The default SNMP parameters on the U2000 must be consistent with the SNMP parameters set on NEs.

Procedure

- 1 To enter the system view, run the following command:

system-view

- 2 To start the SNMP Agent service, run the following command:

snmp-agent

- 3 To set the SNMP protocol version, run the following command:

snmp-agent sys-info version v3

- 4 To set the SNMP user group, run the following command:

snmp-agent group v3 group-name [authentication | privacy] [read-view read-view] [write-view write-view] [notify-view notify-view] [acl acl-number]



NOTE

For the meaning of every field, see the command reference of the corresponding NE.

- 5 To add a new user to the SNMPv3 group, run the following command:

snmp-agent usm-user v3 user-name group-name [[authentication-mode { md5 | sha } password] [privacy-mode des56 password]] [acl acl-number]

----End

Example

The following takes the setting of basic SNMPv3 parameters on a router as an example.

- Set **SNMP version** to **v3**.
- Set **SNMP user group** to **routergroup**.
- Set **new SNMPv3 group user** to **routeruser1**.

After the CLI of the router is displayed, do as follows:

1. Enter the **system-view** command, and then press **Enter**.
2. Enter the **snmp-agent** command, and then press **Enter**.
3. Enter the **snmp-agent sys-info version v3** command, and then press **Enter**.
4. Enter the **snmp-agent group v3 routergroup** command, and then press **Enter**.
5. Enter the **snmp-agent usm-user v3 routeruser1 routergroup** command, and then press **Enter**. The setting of basic SNMPv3 parameters is complete.

```
<NE40E-81>system-view
Enter system view, return user view with Ctrl+Z.
[NE40E-81]snmp-agent
[NE40E-81]snmp-agent sys-info version v3
[NE40E-81]snmp-agent group v3 routergroup
[NE40E-81]snmp-agent usm-user v3 routeruser1 routergroup
[NE40E-81]
```

6.2.4 Configuring the Default SNMP Parameters Template

This topic describes how to correctly set the default SNMP parameters on the U2000 to ensure the normal communication between the U2000 and the managed NEs.

Prerequisite

- You must be an NM user with the "Topo Maintainer" authority or higher.
- This operation is applicable to the Router series, Switch series, Security series, Access series NEs.

Context

It is forbidden to delete the default access protocol parameter template.

Procedure

- 1 Choose **Administration > NE Communicate Parameter > Default Access Protocol Parameters** from the main menu. Click **Display**.
- 2 In the **Default Access Protocol Parameters** dialog box, click the related tab to switch to the page for configuring protocol parameters. The following figure shows how to set SNMPv3 parameters.

Template Name ^	Version ^	Timeout Interval(s) ^	Retries ^	Poll Interval(s) ^	NE Port ^
default	SNMPv3	10	5	1800	161

Template Name: *

Common parameters:

Retries: Poll Interval(s):

Timeout Interval(s): NE Port:

SNMPv3 Security Parameters

NE User: *

Context Name: Context Engine ID:

Private Protocol: Auth Protocol:

- 3 Configure the NE SNMP parameter template as follows:
 - Add a parameter template.

Click **Add**. After setting all the parameters in the parameter setting area at the bottom of the window, click **OK**.
 - Modify a parameter template.

Double-click the template to be modified in the parameter template list. Modify the related parameters in the **Common parameters** and **SNMP v3 Security Parameters** areas. Then, click **Apply**.

 NOTE

- Associated parameters in only the **Common parameters** area need to be modified for SNMPv1 and SNMPv2.
- The **Template Name** parameter cannot be modified.
- Delete a parameter template.
Select the template to be deleted in the parameter template list and then click **Delete**. In the **Confirm** dialog box, click **Yes**.

----End

6.3 Creating a Topology Subnet

The subnet created here is based on a topological concept to facilitate management. In the case of topology objects in the same network area or with similar attributes, you can allocate them in one topology subnet.

Prerequisite

You must be an NM user with "NE operator" authority or higher.

Background Information

A topology subnet is created only to simplify the user interface and has no impact on the NEs.

Procedure

- 1 Right-click in the blank space of the Main Topology and choose **New > Subnet** from the shortcut menu.
- 2 In the displayed dialog box, click the **Property** tab. Enter the attributes of the subnet.
- 3 Click the **Select Objects** tab. Select the created NEs or subnet from the **Available Objects** pane and click  to add the NEs or subnet to the **Selected Objects** pane.

 NOTE

In the case of a similar dialog box for selecting objects,

-  indicates that to select the objects to be selected on the left to the selected objects on the right.
-  indicates that to select all the objects to be selected on the left to the selected objects on the right.

- 4 Click **OK**.

----End

6.4 Creating a Single NE

You need to create an NE before you can manage it by using the U2000. Although creating a single NE is not as fast and accurately as creating NEs in batches. The method of creating the NE of different types cannot be the same.

Prerequisite

When creating an NE on the U2000, ensure that the IP address of the NE does not conflict with the IP address of any existed NE. If the IP addresses conflict with each other, the NE will fail to be created.

[6.4.1 Creating a Single Transport NE](#)

This topic describes how to create a single transport NE.

[6.4.2 Creating a Single PTN NE](#)

After the NE is created, you can use the U2000 to manage the NE. Although creating a single NE is not as fast and exact as creating NEs in batches, you can use this method regardless of whether the data is configured on the NE or not.

[6.4.3 Creating a Single Router NE](#)

This topic describes how to create a single router NE.

[6.4.4 Creating a Single Switch NE](#)

This topic describes how to create a single switch NE.

[6.4.5 Creating a Single Security Gateway NE](#)

This topic describes how to create a single security gateway NE.

[6.4.6 Creating a Single Access NE](#)

This topic describes how to create a single access NE.

6.4.1 Creating a Single Transport NE

This topic describes how to create a single transport NE.

Prerequisite

- You must be an NM user with "NE operator" authority or higher.
- It is applicable to MSTP, WDM, NA WDM, RTN, Marine series NEs.
- The license file that supports the NE type must be installed.
- The NE Explorer instance of the NE must be created.

Context

- Before creating a non-gateway NE, you need to create a GNE first.
- For the WDM equipment except for the OptiX OSN 6800, OptiX OSN 8800 T32, OptiX OSN 8800 T64, to facilitate management, create an optical NE before creating an NE. Otherwise, the new NE is allocated to an idle optical NE automatically.
- If the NE is not created properly or the communication between the NE and the U2000 is abnormal, the NE is displayed in gray.
- If you do not know the IP address of the NE which you want to create, you can use the IP auto discovery. You can view [6.6.1 Creating Transport/PTN NEs in Batches](#)

Procedure

- 1 Right-click in the Main Topology and choose **New > NE** from the shortcut menu.
- 2 On the Object Type tree of the displayed dialog box, select the equipment type of the NE to be created.

3 Set the attributes of the NE.

For example, add the OptiX 2500 in the product family of SDH series equipment. The NE attributes are shown in the following figure:

Attribute	Value
Type	OptiX 2500
ID	81
Extended ID	9
Name	NE81
Remarks	
Gateway Type	Non-Gateway
Affiliated Gateway	NE158
Affiliated Gateway Protocol	IP
NE User	root
Password	
NE Preconfiguration	☐ Yes

NOTE

When you create an NE, its default name is expressed in the NE(extended ID-NE ID) format, such as NE (9-81).

4 To create a GNE or non-gateway NE, do as follows:

- Select the gateway type and protocol, and set the IP or NSAP address.

NOTE

If the NE of the version does not support the OSI protocol, you cannot create a communication connection between the U2000 and the NE even if you select the OSI protocol when you create the NE.

1. Select **Gateway** from the **Gateway Type** drop-down list.
2. Select the protocol type of the gateway.

If the U2000 communicates with NEs through	Do...
IP protocol	Select IP from the Protocol drop-down list. Enter the IP Address and use the default value for the Port number of the GNE.
OSI protocol	Select OSI from the Protocol drop-down list. Enter the NSAP Address of the GNE.

NOTE

The NSAP address consists of hexadecimal digits of a maximum of 20 bytes, and is of the following format: domain address+08003e+NE ID+NSEL. The **Domain Address** comprises of 13 bytes and is entered by the user. **NSEL** is the port number of the network-layer protocol, with a fixed value of 1d (one byte).

- Select **Non-Gateway** from the **Gateway Type** drop-down list, and select the GNE for the NE.

5 **Optional:** In the case of a WDM NE, select an optical NE for the WDM NE.

6 Specify **NE User** and **Password**.

 NOTE

The default NE user is **root** and the default password is **password**.

7 **Optional:** If the NE data on the U2000 is not delivered to the NE, select the **NE Preconfiguration** check box, and set **NE Software Version**.

 NOTE

- If the configuration data of a preconfigured NE is inconsistent with the configuration data of the actual NE, delivering the configuration data of the preconfigured NE affects the actual services on the NE.
- The SONET, RTN, NG WDM, NA WDM, and Marine series equipment do not support NE preconfiguration.

8 Click **OK**. Then, click in the blank space of the Main Topology and the NE icon appears in the position where you clicked.

----End

Result

After you create the NE successfully, the system automatically saves the IP address, NSAP address, subnet mask, and ID of the NE to the U2000 database.

Follow-up Procedure

If you fail to log in to an NE after you create it, the probable causes are as follows:

- The communication between the U2000 and the NE is abnormal. Check the settings of communication parameters, such as IP address and ID of the NE.
- The password of the NE user is incorrect. Enter the correct password.
- The NE user is invalid or is already logged in. Specify a valid NE user.

6.4.2 Creating a Single PTN NE

After the NE is created, you can use the U2000 to manage the NE. Although creating a single NE is not as fast and exact as creating NEs in batches, you can use this method regardless of whether the data is configured on the NE or not.

Prerequisite

- You must be an NM user with "NM operator" authority or higher.
- The license file that supports the NE type must be installed.
- The NE Explorer instance of the NEs must be created.

Context

First create a GNE, and then create a non-gateway NE.

If the NE is not created properly or the communication between the NE and the U2000 is abnormal, the NE is displayed in gray color.

Procedure

- 1 Right-click in the blank space of the Main Topology and choose **New > NE** from the shortcut menu.
- 2 On the Object Type tree of the displayed dialog box, select the NE type to be created.
- 3 Complete the following information: **ID**, **Extended ID**, **Name** and **Remarks**.

For example, add the OptiX PTN 3900 in the product family of PTN series equipment. The NE attributes are shown in the following figure:

Attribute	Value
Type	OptiX PTN 3900
ID	81
Extended ID	9
Name	NE(9-81)
Remarks	
Gateway Type	Gateway ▼
Protocol	IP ▼
IP Address	129.9.0.81
Connection Mode	Common ▼
Port	1400
NE User	root
Password	••••••

NOTE

When you create an NE, its default name is expressed in the NE(extended ID-NE ID) format, such as NE(9-81).

- 4 To create a GNE, proceed to Step 5. To create a non-gateway NE, proceed to Step 6.
- 5 Choose **Gateway Type**, **Protocol** and set the IP address and NSAP address.

NOTE

If the NE of the version does not support the OSI protocol, you cannot create a communication connection between the U2000 and the NE even if you select the OSI protocol when you create the NE.

1. Select **Gateway** from the **Gateway Type** drop-down list.
2. Select the **Protocol** type.

If the U2000 communicates with NEs through	Do...
IP protocol	Select IP from the Protocol drop-down list. Enter the IP Address and use the default value for the Port number of the GNE.
OSI protocol	Select OSI from the Protocol drop-down list. Enter the NSAP Address of the GNE.

 NOTE

The NSAP address is a hexadecimal number that contains a maximum of 20 bytes. Its format is: domain address+08003e+NE ID+NSEL. The **domain address** that contains a maximum of 13 bytes is entered by the user. **NSEL** is the port number of the network-level protocol, with a fixed value of 1d (one byte).

- 6 Select **Non-Gateway** from the **Gateway Type** drop-down list. Select the GNE to which the NE is associated to from the **Affiliated Gateway** drop-down list.

- 7 Enter the **NE User** and **Password**.

 NOTE

The default NE user is **root**, and the default password is **password**.

- 8 Click **OK**. Then, click in the blank space of the Main Topology and the NE icon appears in the position where you clicked.

----End

Result

After an NE is successfully created, the system automatically saves the information, such as the IP address, NSAP address, subnet mask, and NE ID to the U2000 database.

Follow-up Procedure

After an NE is created, if you fail to log in to the NE, possible causes are listed as follows:

- The communication between the U2000 and the NE is abnormal. Check the settings of communication parameters, such as the IP address of the NE and NE ID.
- The password for the NE user is incorrect. Enter the correct password for the NE user.
- The NE user is invalid or the NE user is already logged in. Change to use a valid NE user.

6.4.3 Creating a Single Router NE

This topic describes how to create a single router NE.

Prerequisite

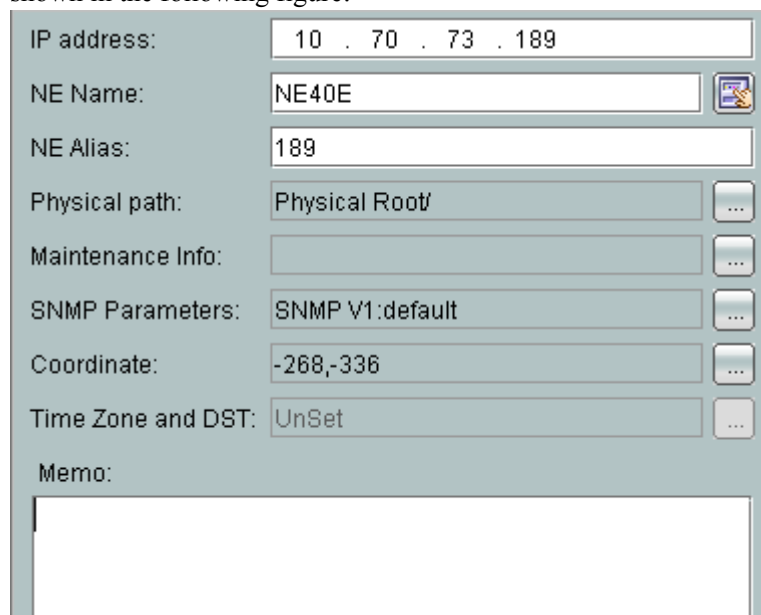
It is applicable to router NEs, such as NE series routers and CX series routers.

In the case of switch and router NEs, the function of creating an NE uses the license for dedicated upgrade items or the license for NE resources. If there is no remaining license for dedicated upgrade items or license for NE resources, a message is displayed indicating that NE creation fails. It is recommended that you apply for a new license for NE resources.

Procedure

- 1 Right-click in the Main Topology and choose **New > NE** from the shortcut menu.
- 2 On the Object Type tree of the displayed dialog box, select the equipment type of the NE to be created.
- 3 Set the attributes of the NE.

For example, add the NE40E in the product family of NE series routers. The NE attributes are shown in the following figure:



The screenshot shows a configuration window for a Network Element (NE). The fields are as follows:

Field	Value
IP address:	10 . 70 . 73 . 189
NE Name:	NE40E
NE Alias:	189
Physical path:	Physical Root/
Maintenance Info:	
SNMP Parameters:	SNMP V1:default
Coordinate:	-268,-336
Time Zone and DST:	UnSet
Memo:	

4 Click **OK**.

----End

Result

After you create the NE successfully, the system saves the NE information to the U2000 database automatically.

6.4.4 Creating a Single Switch NE

This topic describes how to create a single switch NE.

Prerequisite

It is applicable to switch NEs, such as CX200D and S series NEs.

In the case of switch and router NEs, the function of creating an NE uses the license for dedicated upgrade items or the license for NE resources. If there is no remaining license for dedicated upgrade items or license for NE resources, a message is displayed indicating that NE creation fails. It is recommended that you apply for a new license for NE resources.

Procedure

- 1 Right-click in the Main Topology and choose **New > NE** from the shortcut menu.
- 2 On the Object Type tree of the displayed dialog box, select the NE type of the NE to be created.
- 3 Set the attributes of the NE.

For example, add the S8016 in the product family of S series NE. The NE attributes are shown in the following figure:

IP address:	10 . 71 . 25 . 3
NE Name:	S8016
NE Alias:	3
Physical path:	Physical Root
Maintenance Info:	
SNMP Parameters:	SNMP V1:default
Coordinate:	-268,-336
Time Zone and DST:	UnSet
Memo:	

4 Click **OK**.

----End

Result

After you create the NE successfully, the system saves the NE information to the U2000 database automatically.

6.4.5 Creating a Single Security Gateway NE

This topic describes how to create a single security gateway NE.

Prerequisite

It is applicable to security gateway NEs, such as USG series equipment.

Procedure

- 1 Right-click in the Main Topology and choose **New > NE** from the shortcut menu.
- 2 On the Object Type tree of the displayed dialog box, select the equipment type of the NE to be created.
- 3 Set the attributes of the NE.

For example, add the USG50 in the product family of USG series gateways. The NE attributes are shown in the following figure:

IP address:	10 . 71 . 25 . 9
NE Name:	USG50
NE Alias:	8
Physical path:	Physical Root/
Maintenance Info:	
SNMP Parameters:	SNMP V1:default
Coordinate:	-268,-336
Time Zone and DST:	UnSet
Memo:	

- 4 Click **OK**.

----End

Result

After you create the NE successfully, the system saves the NE information to the U2000 database automatically.

6.4.6 Creating a Single Access NE

This topic describes how to create a single access NE.

Prerequisite

It is applicable to access NEs. For example, multi-service access modules.

Procedure

- 1 Right-click in the Main Topology and choose **New > NE** from the shortcut menu.
- 2 On the Object Type tree of the displayed dialog box, select the equipment type of the NE to be created.
- 3 Set the attributes of the NE.

For example, add the Access NE in the product family of **Access NE**. The NE attributes are shown in the following figure:

4 Click **OK**.

----End

Result

After you create the NE successfully, the system saves the NE information to the U2000 database automatically.

6.5 Creating Optical NEs

The U2000 manages the WDM equipment and OptiX BWS 1600S by using optical NEs. There are four types of optical NEs. They are WDM_OADM, WDM_OEQ, WDM_OLA and WDM_OTM. OptiX OSN 1800 only supports WDM_OTM and WDM_OADM. OptiX BWS 1600S only supports WDM_OTM.

Prerequisite

- You must be an NM user with "NE operator" authority or higher.
- The license must be installed and the license must support creating the NE of the type.
- Applies to the WDM equipment and OptiX BWS 1600S.

Procedure

- 1 Right-click in the blank space of the Main Topology and choose **New > NE** from the shortcut menu.
- 2 Select the optical NE type for the optical NE in the displayed dialog box.
- 3 In the **General Attributes** tab, set the attributes of the optical NE.

 NOTE

An OEQ NE is an OLA NE that enables the equalization of optical power and dispersion. If an OLA NE has the boards for dispersion compensation and power compensation, the OLA NE should be changed to an OEQ NE.

- 4 Click the **Resource Division** tab. Select NEs or boards from the Idle ONE and click .
- 5 Click **OK**.
- 6 Click in the blank space of the Main Topology and the NE icon appears in the position where you clicked.

----End

6.6 Creating NEs In Batches

The U2000 supports the ability to search out all NEs according to the IP addresses of NEs, IP address or IP network segment of the GNE, or NSAP addresses of the NEs, and create the NEs in batches. The U2000 also can import and create in batches the NEs that register with the U2000 according to the active registration information of the NEs. Creating NEs by using this method is faster and more reliable than creating the NEs manually.

6.6.1 Creating Transport/PTN NEs in Batches

When the U2000 communicates with a GNE normally, the U2000 supports the ability to search out all NEs that communicate with the GNE according to the IP address or IP network segment of the GNE, or NSAP addresses of the NEs, and create the NEs in batches.

6.6.2 Creating SNMP/ICMP NEs in Batches

SNMP/ICMP NEs include Router series, Switch series, Security series, Access series NEs. When the U2000 communicates with SNMP/ICMP NEs normally, the U2000 supports the ability to search out all SNMP/ICMP NEs according to the IP addresses or IP network segments of the NEs, and create them in batches.

6.6.1 Creating Transport/PTN NEs in Batches

When the U2000 communicates with a GNE normally, the U2000 supports the ability to search out all NEs that communicate with the GNE according to the IP address or IP network segment of the GNE, or NSAP addresses of the NEs, and create the NEs in batches.

Prerequisite

- You must be an NM user with "NE administrator" authority or higher.
- U2000 communicates with the GNE normally.

Context

Except the OptiX OSN 6800, OptiX OSN 8800 T32, OptiX OSN 8800 T64 equipment, to facilitate management, create optical NEs before creating NEs in batches. Otherwise, the new NEs are allocated to idle optical NEs automatically.

Procedure

- 1 Choose **File > Discovery > NE** from the main menu.

- 2 Click the **Transport NE Search** tab.
- 3 Select the search mode from the drop-down list of **Search Mode**.
 - Sets the **Search Mode** is **Search for NE**:
 1. Enter the network segment or IP addresses NEs to search for the NEs.
 - a. Click **Add** and the **Input Search Domain** dialog box is displayed.
 - b. Set the address type to **IP Address Range of GNE**, **IP Address of GNE**, or **NSAP Address**. Enter the **Search Address**, **User Name**, and **Password**. Click **OK**.

NOTE

Repeat the above steps to add more search domains. You can also delete the system-default search domain.

- If you search by IP address,
 - only the NEs (not across routers) in the same network segment can be searched out in normal conditions if you select the **IP Address Range of GNE** because broadcasting is usually disabled for the routers in the network (to prevent network storm).
 - search out the NEs in the network segment by using the **IP Address of GNE** if you need to search for the NEs across routers.
 - If you search for NEs by using the NSAP address, you can only select **NSAP Address**.
2. In the **Search for NE** area, perform the following operations:
 - Select **Create device after search**, enter the **NE User** and **Password**.

NOTE

- The default NE user is **root**.
 - The default password is **password**.
- Select **Upload after create**. The data related to the NEs are uploaded to the U2000 after the NEs are created.

NOTE

You can select all options in the **Search for NE** area to search for NEs, create NEs, and upload the NE data at a time.

- Sets the **Search Mode** is **IP auto discovery**:

 NOTE

If you fail to enter a network segment correctly, enable **IP auto discovery**. After enabling **IP auto discovery**, you can obtain the IP address of the GNE and search out all the NEs related to the GNE.



CAUTION

In the case of NEs that are connected to the NMS through the router, these NEs cannot be searched out by **IP auto discovery**. They can be searched out only by network segment.

- 4 Click **Next** and the **Result** area is displayed.

Result							
No.	NE ID ^	GNE Address v	GNE ID ^	Created As GNE ^	Connection Mode ^	Port ^	NE Status ^
1	NE71-7183	10.71.227.183	NE71-7183 v	Yes	Common v	1400	Uncreated

- 5 **Optional:** Click **Change NE ID**. Then, the **Change NE ID** dialog box is displayed. Users can check against the Bar Code List by the value of **Bar Code**, and then modify the **NE Name**, **Extend NE ID**, **Base NE ID**, and **IP Address** fields accordingly.

NE Bar Code				
Bar Code ^	NE Name ^	Extend NE ID ^	Base NE ID ^	IP Address ^
2102112894N092000105	NE14	8	14	129.9.1.14

 NOTE

The Bar Code List is provided by the hardware installation personnel to the software commissioning personnel. The list contains the bar codes of stations.

- 6 **Optional:** If you select only **Search for NE**, after the U2000 completes the search, you can select the uncreated NEs from the **Relust** list and click **Create**. The **Create** dialog box is displayed. Enter the **NE User** and **Password**. Click **OK**.

----End

Follow-up Procedure

If you fail to log in to an NE after you create it, the probable causes are as follows:

- The password of the NE user is incorrect. Enter the correct password.
- The NE user is invalid or is already logged in. Specify a valid NE user.

6.6.2 Creating SNMP/ICMP NEs in Batches

SNMP/ICMP NEs include Router series, Switch series, Security series, Access series NEs. When the U2000 communicates with SNMP/ICMP NEs normally, the U2000 supports the ability to search out all SNMP/ICMP NEs according to the IP addresses or IP network segments of the NEs, and create them in batches.

Prerequisite

- You must be an NM user with "NE administrator" authority or higher.

- U2000 communicates with the router NEs normally.
- Only one client can use the automatic discovery function at a time.
- The existing NEs are excluded for the automatic discovery. In the **More Information** dialog box, those NEs are displayed as the existing NEs.
- If you clear the selection of **Automatically Create NEs**, the NEs that are searched out are not automatically created. You need to manually create the NEs as required.

Context

In the case of switch and router NEs, the function of creating an NE uses the license for dedicated upgrade items or the license for NE resources. If there is no remaining license for dedicated upgrade items or license for NE resources, a message is displayed indicating that NE creation fails. It is recommended that you apply for a new license for NE resources.

Procedure

- 1 Choose **File > Discovery > NE** from the main menu.
- 2 Click the **SNMP/ICMP NE Search** tab.

- 3 Set the search parameters, such as **NE Type** and **Ping Times**. If you select the **Automatically Create NEs** check box, the equipment that is searched out is created automatically. Otherwise, you need to create the equipment manually.
- 4 Click **Default SNMP Parameter** to set the SNMP parameters to values that are consistent with the parameter values on the equipment side.



CAUTION

If the settings of the SNMP parameters are inconsistent with the parameter settings on the equipment side, the equipment cannot be searched out.

- 5 In the **IP Address Range (History Records are already loaded)** area, click **Add** and the **IP Address Range** dialog box is displayed. Enter the **Start IP Address**, **End IP Address**, and **Subnet Mask**. Click **OK**.
- 6 Click **Next**. The **SNMP/ICMP NE Search** tab page of the **Auto Discovery** dialog box displays the equipment data that is searched out and the operation records.

The screenshot shows the 'Auto Discovery' dialog box with the 'SNMP/ICMP NE Search' tab selected. It is divided into two main sections: 'NE Data' and 'Operation Results'.

NE Data (Top Section):

System Name ^	IP ^	Mode ^	System Description ^	Status ^
USG50-166	10.112.58.166	SNMPv1	Huawei Versatile Ro...	To be created
Bingjiang_PetrolStat...	10.112.58.168	SNMPv1	Huawei Versatile Ro...	To be created
USG5350-203	10.112.58.169	SNMPv1	Huawei Versatile Ro...	To be created
usg9100-170-B016	10.112.58.170	SNMPv1	Huawei Versatile Ro...	To be created
E8000E-171-test	10.112.58.171	SNMPv1	Quidway Eudemon8...	To be created
USG5350-173	10.112.58.173	SNMPv1	Huawei Versatile Ro...	To be created
E1000-176	10.112.58.176	SNMPv1	Quidway E1000 Fire...	To be created
USG2130	10.112.58.177	SNMPv1	Huawei Versatile Ro...	To be created
USG5360-178	10.112.58.178	SNMPv1	Huawei Versatile Ro...	To be created

Operation Results (Top Section):

Consumed Time: 2 minutes 21 seconds
Total discovered NEs:49
Total undiscovered NEs:40
After the data is loaded successfully, the topology view will be refreshed automatically.

NE Data (Bottom Section):

System Name ^	IP address ^	Mode ^	System Description ^	Status ^
ME60-12	10.112.57.12	SNMPv1	Huawei Versatile Ro...	This device can not ...
MA5200G-20	10.112.57.20	SNMPv1	Quidway MA5200G-...	This device can not ...

Operation Results (Bottom Section):

Consumed Time: 48 seconds
Total discovered NEs:2
Total undiscovered NEs:45
After the data is loaded successfully, the topology view will be refreshed automatically.

NOTE

- When setting the parameters for NE search, if you select **Automatically Create NEs**, NEs are automatically created and added to the physical topology tree of the U2000.
- When setting the parameters for NE search, if you deselect **Automatically Create NEs**, you need to manually create NEs. In the **NE Data**, select a NE that to create, click **Create**.

- 7 **Optional:** Click **More** and the **More Information** dialog box is displayed. View the details of **Undiscovered Equipment** in the operation records.

----End

6.7 Viewing an NE in the Topology View

This topic describes how to view an NE in the topology view. After an NE is added to the U2000, you can view the NE status in the topology view.

Prerequisite

The NE must be added to the U2000.

Procedure

- 1 View an NE in the topology view.
 - If the NE is in the Main Topology, you can directly view it in the Main Topology.
 - If the NE is in a subnet, double-click the subnet icon in the Main Topology, and then view the NE in the subnet.



NOTE

The icons vary according to the NE type.

- 2 Determine the NE status based on the color of the NE icon.
 1. Choose **View > Display Setting > Legend** from the main menu. The **Legend** tab page is displayed on the right of the topology view.
 2. Click the **Legend** tab and determine the NE status based on the legend description.

----End

7 Commissioning the Communication Between the NMS and the OSS

About This Chapter

The U2000 supports NBIs including CORBA NBI, XML NBI, SNMP NBI, TL1 NBI, and FTP performance NBI. By commissioning the communications between a U2000 and OSSs according to the NBI to be used, you must ensure that the NBI function is available for the U2000.

[7.1 Commissioning a CORBA NBI](#)

This topic describes how to commission a CORBA NBI. Before connecting the U2000 to the OSS through a CORBA NBI, you need to ensure that the CORBA NBI function of the U2000 is available.

[7.2 Commissioning an XML NBI](#)

This topic describes how to commission an XML NBI. Before connecting the U2000 to the OSS through an XML NBI, you need to ensure that the XML NBI function of the U2000 is available.

[7.3 Commissioning an SNMP NBI](#)

This topic describes how to commission an SNMP NBI. Before connecting the U2000 to the OSS through an SNMP NBI, you need to ensure that the SNMP NBI function of the U2000 is available.

[7.4 Commissioning an TL1 NBI](#)

This topic describes how to commission an TL1 NBI. Before connecting the U2000 to the OSS through an TL1 NBI, you need to ensure that the TL1 NBI function of the U2000 is available.

[7.5 Commissioning an FTP Performance NBI](#)

This topic describes how to commission an FTP performance NBI. The U2000 server can be set as an FTP server. As an FTP client, an upper layer NMS or a third-party NMS accesses the U2000 server and obtains the performance NBI files.

7.1 Commissioning a CORBA NBI

This topic describes how to commission a CORBA NBI. Before connecting the U2000 to the OSS through a CORBA NBI, you need to ensure that the CORBA NBI function of the U2000 is available.

The OSS can manage the U2000 through the CORBA NBI.

Before connecting the U2000 to the OSS, you must ensure that the CORBA NBI of the U2000 has been correctly configured and enabled, and the serving ports used by the CORBA NBI cannot be disabled.

NOTE

For detailed configurations of the CORBA NBI, see the *iManager U2000 Northbound CORBA Interface User Guide*.

1. The CORBA NBI component must be installed or added.
If the component is not installed or added, add the component by using the network management system maintenance suite. To add a component, see [D.4.1 Adding a Component](#).
2. The CORBA NBI instance must be added.
If the instance is not added, add the instance by using the network management system maintenance suite. To add a instance, see [D.4.3 Adding an Instance](#).
3. The CORBA NBI function must be included in the configuration items in the license file.
On the U2000 client, choose **Help > License Information** from the main menu. Choose **Function Control Item** tab page in the dialog box that is displayed to view the license information.
4. The CORBA NBI component process must be started.
On the **Process Monitor** tab page on the System Monitor client, view the process start information.
5. The serving ports for the communication between the U2000 and the OSS cannot be used and closed.

You can run the **netstat -an** command to view the serving ports opened by the system.

- In the Solaris or SUSE Linux OS, you can run the **netstat -an | grep port_number** command to view the status of specified ports.

For example, you can run the **netstat -an | grep 445** command to view port 445.

- In the Windows OS, you can run the **netstat -an | find "port_number"** command to view the status of specified ports.

For example, you can run the **netstat -an | find "445"** command to view port 445.

NOTE

If any router or firewall is located on the network between the U2000 and the OSS, you need to check the ports used by the U2000 and the OSS to ensure that these ports can be opened for normal communication.

Table 7-1 Serving ports of the CORBA NBI

Service Name	Serving Port/ Protocol Type	Direction (with the Server as the Reference Object)	Description
CORBA naming service	12001/TCP	IN	This port is used to monitor the CORBA access of the upper- layer NMS.
CORBA notification service	12002/TCP	IN	This port is used to monitor the CORBA access of the upper- layer NMS.
CORBA agent	12003/TCP	IN	This port is used to monitor the CORBA access of the upper- layer NMS.
CORBA naming service (SSL)	22001/TCP	IN	This port is used to monitor the CORBA access of the upper- layer NMS in SSL mode.
CORBA notification service (SSL)	22002/TCP	IN	This port is used to monitor the CORBA access of the upper- layer NMS in SSL mode.
CORBA agent (SSL)	22003/TCP	IN	This port is used to monitor the CORBA access of the upper- layer NMS in SSL mode.

7.2 Commissioning an XML NBI

This topic describes how to commission an XML NBI. Before connecting the U2000 to the OSS through an XML NBI, you need to ensure that the XML NBI function of the U2000 is available.

The OSS can manage the U2000 through the XML NBI.

Before connecting the U2000 to the OSS, you must ensure that the XML NBI of the U2000 has been correctly configured and enabled, and the serving ports used by the XML NBI cannot be disabled.

 NOTE

For detailed configurations of the XML NBI, see the *iManager U2000 Northbound XML Interface User Guide*.

1. The XML NBI component must be installed or added.

If the component is not installed or added, add the component by using the network management system maintenance suite. To add a component, see [D.4.1 Adding a Component](#).

2. The XML NBI instance must be added.

If the instance is not added, add the instance by using the network management system maintenance suite. To add a instance, see [D.4.3 Adding an Instance](#).

3. The XML NBI function must be included in the configuration items in the license file.

On the U2000 client, choose **Help > License Information** from the main menu. Choose **Function Control Item** tab page in the dialog box that is displayed to view the license information.

4. The XML NBI component process must be started.

On the **Process Monitor** tab page on the System Monitor client, view the process start information.

5. The serving ports for the communication between the U2000 and the OSS cannot be used and closed.

You can run the **netstat -an** command to view the serving ports opened by the system.

- In the Solaris or SUSE Linux OS, you can run the **netstat -an | grep port_number** command to view the status of specified ports.

For example, you can run the **netstat -an | grep 445** command to view port 445.

- In the Windows OS, you can run the **netstat -an | find "port_number"** command to view the status of specified ports.

For example, you can run the **netstat -an | find "445"** command to view port 445.

 NOTE

If any router or firewall is located on the network between the U2000 and the OSS, you need to check the ports used by the U2000 and the OSS to ensure that these ports can be opened for normal communication.

Table 7-2 Serving ports of the XML NBI

Service Name	Serving Port/ Protocol Type	Direction (with the Server as the Reference Object)	Description
HTTP service	80/TCP	IN	This port is used to monitor the XML access of the upper-layer NMS.
HTTPS service	443/TCP	IN	This port is used to monitor the XML access of the upper-layer NMS.
JMS service	61616/TCP	IN	This port is used to monitor the XML access of the upper-layer NMS.

Service Name	Serving Port/ Protocol Type	Direction (with the Server as the Reference Object)	Description
JMS service (SSL)	61617/TCP	IN	This port is used to monitor the XML access of the upper-layer NMS in SSL mode.

7.3 Commissioning an SNMP NBI

This topic describes how to commission an SNMP NBI. Before connecting the U2000 to the OSS through an SNMP NBI, you need to ensure that the SNMP NBI function of the U2000 is available.

The OSS can manage the U2000 through the SNMP NBI.

Before connecting the U2000 to the OSS, you must ensure that the SNMP NBI of the U2000 has been correctly configured and enabled, and the serving ports used by the SNMP NBI cannot be disabled.

NOTE

For detailed configurations of the SNMP NBI, see the *iManager U2000 Northbound SNMP Interface User Guide*.

1. The SNMP NBI component must be installed or added.
If the component is not installed or added, add the component by using the network management system maintenance suite. To add a component, see [D.4.1 Adding a Component](#).
2. The SNMP NBI instance must be added.
If the instance is not added, add the instance by using the network management system maintenance suite. To add a instance, see [D.4.3 Adding an Instance](#).
3. The SNMP NBI function must be included in the configuration items in the license file.
On the U2000 client, choose **Help > License Information** from the main menu. Choose **Function Control Item** tab page in the dialog box that is displayed to view the license information.
4. The SNMP NBI component process must be started.
On the **Process Monitor** tab page on the System Monitor client, view the process start information.
5. The serving ports for the communication between the U2000 and the OSS cannot be used and closed.
You can run the **netstat -an** command to view the serving ports opened by the system.
 - In the Solaris or SUSE Linux OS, you can run the **netstat -an | grep port_number** command to view the status of specified ports.
For example, you can run the **netstat -an | grep 445** command to view port 445.
 - In the Windows OS, you can run the **netstat -an | find "port_number"** command to view the status of specified ports.

For example, you can run the **netstat -an | find "445"** command to view port 445.

 NOTE

If any router or firewall is located on the network between the U2000 and the OSS, you need to check the ports used by the U2000 and the OSS to ensure that these ports can be opened for normal communication.

Table 7-3 Serving ports of the SNMP NBI

Service Name	Serving Port/ Protocol Type	Direction (with the Server as the Reference Object)	Description
SnmpAgent	982/TCP	OUT	SNMP trap sending
SnmpAgent	9812/TCP	IN	SNMP trap receiving

7.4 Commissioning an TL1 NBI

This topic describes how to commission an TL1 NBI. Before connecting the U2000 to the OSS through an TL1 NBI, you need to ensure that the TL1 NBI function of the U2000 is available.

The OSS can manage the U2000 through the TL1 NBI.

Before connecting the U2000 to the OSS, you must ensure that the TL1 NBI of the U2000 has been correctly configured and enabled, and the serving ports used by the TL1 NBI cannot be disabled.

 NOTE

For detailed configurations of the TL1 NBI, see the *iManager U2000 TL1 NBI User Guide*.

1. The TL1 NBI component must be installed or added.
If the component is not installed or added, add the component by using the network management system maintenance suite. To add a component, see [D.4.1 Adding a Component](#).
2. The TL1 NBI instance must be added.
If the instance is not added, add the instance by using the network management system maintenance suite. To add a instance, see [D.4.3 Adding an Instance](#).
3. The TL1 NBI function must be included in the configuration items in the license file.
On the U2000 client, choose **Help > License Information** from the main menu. Choose **Function Control Item** tab page in the dialog box that is displayed to view the license information.
4. The TL1 NBI component process must be started.
On the **Process Monitor** tab page on the System Monitor client, view the process start information.
5. The serving ports for the communication between the U2000 and the OSS cannot be used and closed.

You can run the **netstat -an** command to view the serving ports opened by the system.

- In the Solaris or SUSE Linux OS, you can run the **netstat -an | grep port_number** command to view the status of specified ports.

For example, you can run the **netstat -an | grep 445** command to view port 445.

- In the Windows OS, you can run the **netstat -an | find "port_number"** command to view the status of specified ports.

For example, you can run the **netstat -an | find "445"** command to view port 445.

 NOTE

If any router or firewall is located on the network between the U2000 and the OSS, you need to check the ports used by the U2000 and the OSS to ensure that these ports can be opened for normal communication.

Serving ports of the TL1 NBI is **9819**.

7.5 Commissioning an FTP Performance NBI

This topic describes how to commission an FTP performance NBI. The U2000 server can be set as an FTP server. As an FTP client, an upper layer NMS or a third-party NMS accesses the U2000 server and obtains the performance NBI files.

The FTP NBI saves the original performance data in the U2000 database as files to a specified directory. As the FTP client, a third party NMS or an upper layer NMS can obtain the required data from the specified directory for analysis and use.

The FTP performance NBI can collect performance data from routers, switches, security devices, access equipment, and PTN equipment. Only users with the FTP access rights can obtain the performance NBI files.

1. The FTP performance NBI component must be installed or added.

If the component is not installed or added, add the component by using the network management system maintenance suite. To add a component, see [D.4.1 Adding a Component](#).

2. The FTP performance NBI instance must be added.

If the instance is not added, add the instance by using the network management system maintenance suite. To add a instance, see [D.4.3 Adding an Instance](#).

3. The FTP performance NBI function must be included in the configuration items in the license file.

On the U2000 client, choose **Help > License Information** from the main menu. Choose **Function Control Item** tab page in the dialog box that is displayed to view the license information.

4. The FTP performance NBI component process must be started.

On the **Process Monitor** tab page on the System Monitor client, view the process start information.

5. Configuring the FTP server on U2000 server.

 NOTE

For detailed configuring the FTP server, configuring the FTP performance NBI, and obtaining performance NBI files see the *iManager U2000 FTP Performance NBI User Guide*.

6. Configuring the FTP performance NBI.
7. Obtaining performance NBI files.

8 Commissioning the Alarm Function

About This Chapter

As an important information source for learning the equipment running status and locating faults, alarms need to be obtained and managed in an effectively manner. By setting alarm parameters, you must ensure that equipment alarms can be reported to a U2000. In this manner, the U2000 can monitor and manage the live network in real time. For details about alarm management, see the Help. For details about how to commission the alarm box, see the associated documents delivered with the alarm box.

[8.1 Alarm Reporting Process](#)

The alarm reporting process starts with the detection of the alarm on a board, and ends with the U2000 notifying the alarm to a user. The alarm reporting process is instructive in guiding a user to handle alarms.

[8.2 Setting Trap Parameters on the NE](#)

A trap receiver receives trap messages of the NE. This describes how to set trap parameters on the NE. The NE actively sends fault information to the U2000 through trap packets defined by SNMP. After the trap function is configured, the NE can actively send fault information.

[8.3 Setting Automatic Alarm Reporting](#)

If you set alarms on an NE to be automatically reported, once the alarm is raised on the NE, it is automatically reported to the U2000. You can disable the automatic reporting for unimportant alarms to reduce the impact on the U2000 performance. A large volume of alarm information affects the performance of the U2000.

[8.4 Monitoring Alarms](#)

This topic describes how to monitor alarms. You can view the alarms reported to the U2000 in the topology view, alarm panel, and alarm list. On condition that network services are not affected, it is recommended that you make the NEs offline and then view the alarm reporting information on the U2000.

8.1 Alarm Reporting Process

The alarm reporting process starts with the detection of the alarm on a board, and ends with the U2000 notifying the alarm to a user. The alarm reporting process is instructive in guiding a user to handle alarms.

Alarm reporting flow chart

- For Router series, Switch series, Security series, Access series NEs, [Figure 8-1](#) shows the activities performed to report an alarm.
- For MSTP, WDM, NA WDM, RTN, PTN, Marine series NEs, [Figure 8-2](#) shows the activities performed to report an alarm.

[Figure 8-1](#) shows the activities performed to report an alarm.

Figure 8-1 Alarm reporting flow chart 1

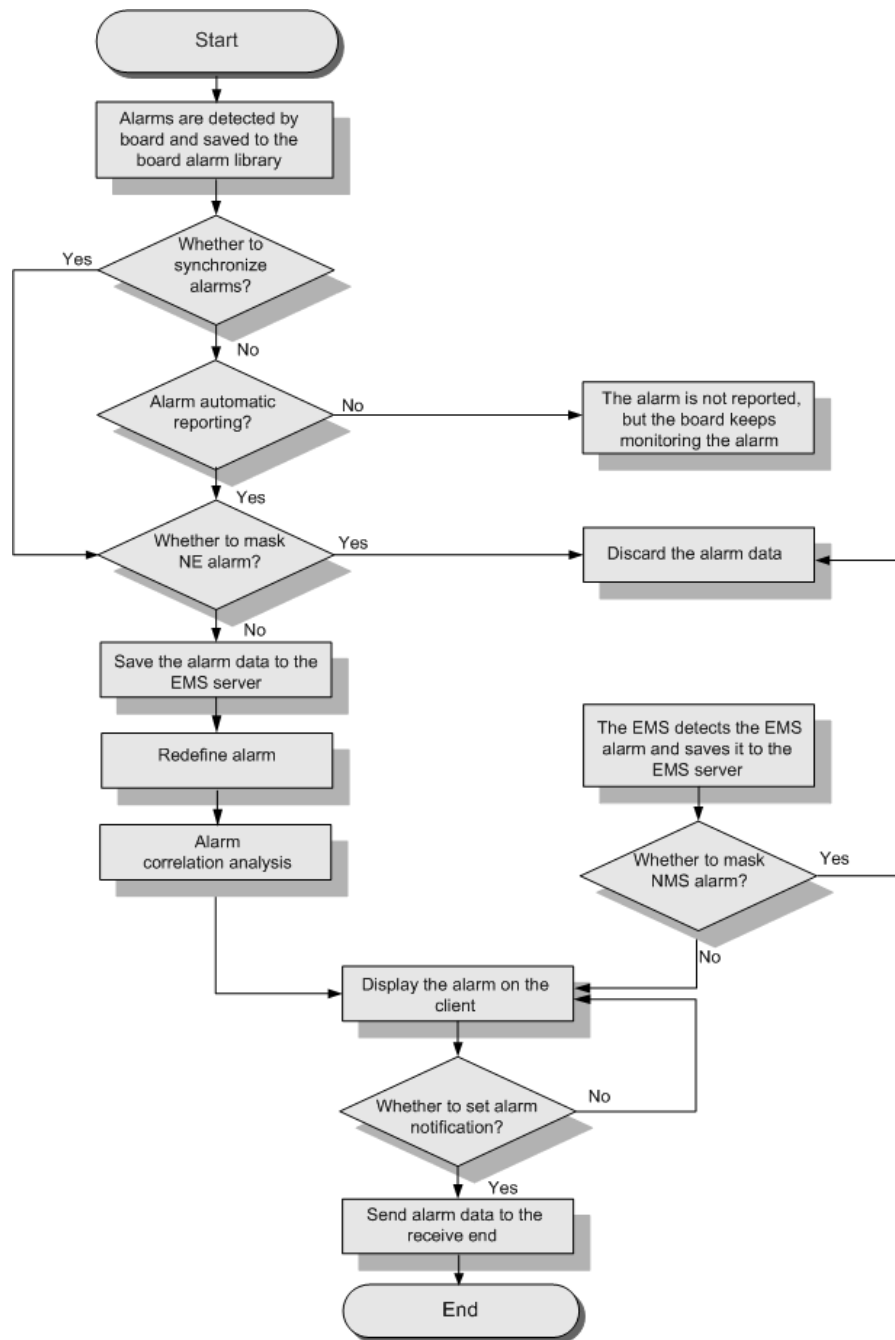


Figure 8-2 Alarm reporting flow chart 2

Alarm Monitoring by Board

When monitoring an alarm, the board immediately reports the alarm to the SCC continuously. If the alarm database of the SCC does not have this alarm, the alarm data is saved into the database and a notification is reported. Otherwise, the alarm data is discarded directly.

Automatic Alarm Reporting

When the SCC receives a new alarm notification, it determines whether to report the alarm to the U2000 according to the settings of the alarm automatic reporting. After the U2000 receives an alarm notification, it responds to the SCC a confirm message. If the SCC does not receive any confirm message within a time period, it reports the alarm to the U2000 again. This scheme ensures the reliability of the alarm reporting.

If the communication between the U2000 and the NE is interrupted, when the U2000 is restarted, it automatically synchronizes the alarm library of the SCC to keep the alarm data on the U2000 synchronous with the alarm data on NE.

U2000 Alarm Notification

Based on the user-defined alarm filter criteria, the U2000 decides whether to discard the alarm reported from an NE. As for the alarms saved in the U2000 database, the U2000 analyzes them according to the alarm correlation rules. Then it presents the analysis result on the U2000 client and notifies the information to the user.

8.2 Setting Trap Parameters on the NE

A trap receiver receives trap messages of the NE. This describes how to set trap parameters on the NE. The NE actively sends fault information to the U2000 through trap packets defined by SNMP. After the trap function is configured, the NE can actively send fault information.

Context

- This operation is applicable to the following SNMP NE: Router series, Switch series, Security series, Access series NEs.
- Make sure that the source port and interface of trap packets configured on the NMS is consistent with the source port and interface for sending packets configured on the NE. Otherwise, the NMS cannot receive trap packets.
- To start the trap receiver on the U2000, ensure that **Trap Receiver Process** on the **Process Monitor** tab page is in the running state. This process is automatically started by default. If it is not automatically started, log in to the System Monitor client, click the **Process Monitor** tab, right-click **Trap Receiver Process**, and then choose **Start the Process** from the shortcut menu.



NOTE

The following section considers routers as an example to describe how to set trap parameters on the NE.
For details, see the documents relevant to the NE.

Procedure

- 1 Run the following command to telnet to the host.
telnet Host name of the server
- 2 Run the following command to enter the system view.
system-view
- 3 Run the following command to enable the function of sending trap packets:
snmp-agent trap enable [trap-type [trap-list]]

If no parameter is carried in this command, it indicates that all modules can send all types of trap packets.

- 4 Run the following command to set the target host, that is, the NMS server:

```
snmp-agent target-host trap address udp-domain ip-address [ udp-port port-number ]  
[ vpn-instance vpn-instance-name ] params securityname security-string [ v1 | v2c | v3  
[ authentication | privacy ] ]
```

- 5 Run the following command to specify the source interface for sending trap packets:

```
snmp-agent trap source interface-type interface-number
```

----End

8.3 Setting Automatic Alarm Reporting

If you set alarms on an NE to be automatically reported, once the alarm is raised on the NE, it is automatically reported to the U2000. You can disable the automatic reporting for unimportant alarms to reduce the impact on the U2000 performance. A large volume of alarm information affects the performance of the U2000.

8.3.1 Setting Automatic Reporting Status for Alarms of an NE

You can set the automatic reporting status of the alarms of specific boards so that the U2000 only monitors important alarms, thus improving the network maintenance efficiency. To implement automatic reporting of the alarms of an NE, you can apply an alarm attribute template to the NE.

8.3.2 Setting Automatic Reporting Status for Alarms of a Board

You can set the automatic reporting status of the alarms of specific boards so that the U2000 only monitors important alarms, thus improving the network maintenance efficiency. To implement the function, you can manually set the automatic reporting status for each alarm or apply the alarm attribute template to a board.

8.3.1 Setting Automatic Reporting Status for Alarms of an NE

You can set the automatic reporting status of the alarms of specific boards so that the U2000 only monitors important alarms, thus improving the network maintenance efficiency. To implement automatic reporting of the alarms of an NE, you can apply an alarm attribute template to the NE.

Prerequisite

- You must be an NM user with the "NE maintainer" and "NM monitor" authority or higher.
- The alarm attribute template that has the alarm reporting status configured as required must be customized first.
- Applies to the MSTP, WDM, NA WDM, RTN, PTN, Marine series NEs.

Context

After you set alarms not to be automatically reported, if alarms are generated in an NE, the NE does not automatically report them to the U2000. You can use the U2000, however, to synchronize and query the alarms so that the alarms are reported to the U2000.

 NOTE

The following steps are not applicable to the OptiX PFE 1670. The navigation path to this function for the OptiX PFE 1670 is as follows: In the NE Panel, select the NE, right-click, and then choose **NE Report Status** from the shortcut menu.

Procedure

- 1 Choose **Fault > Settings > NE Alarm/Event Config** from the main menu.
The **NE Alarm/Event Config** tab page is displayed.
- 2 Choose **SDH/WDM/NAWDM** from the Function Tree. In the right pane, select the pre-customized template from the **Template** drop-down list and click **Apply to**. The **Apply Alarm Attribute Template to NE** dialogue box is displayed.

 NOTE

If the appropriate alarm attribute template is not available, you need to customize a template first.

- 3 Check the **Alarm Auto-Report** in the **Alarm Attribute** group box.
- 4 Select the NE you need from the **List of Optional Objects**, and move it to **List of Selected Objects**. Click **OK**.
Wait for a few seconds and the **Operation Result** dialog box is displayed.
- 5 Click **Close**.

----End

8.3.2 Setting Automatic Reporting Status for Alarms of a Board

You can set the automatic reporting status of the alarms of specific boards so that the U2000 only monitors important alarms, thus improving the network maintenance efficiency. To implement the function, you can manually set the automatic reporting status for each alarm or apply the alarm attribute template to a board.

Prerequisite

- You must be an NM user with "NE operator" authority or higher.
- If you use the template to set the alarm suppression status, You must be an NM user with "NM monitor" authority or higher.
- Applies to the MSTP, WDM, NA WDM, RTN, PTN, Marine series NEs.

Context

After you set alarms not to be automatically reported, if alarms are generated in an NE, the NE does not automatically report them to the U2000. You can use the U2000, however, to synchronize and query the alarms so that the alarms are reported to the U2000.

Procedure

- 1 In the NE Explorer, select a board and choose **Alarm > Alarm Severity and Auto Reporting** from the Function Tree.
- 2 Set the **Auto Reporting Status** for the alarms and click **Apply**. The **Operation Result** dialog box is displayed.

**NOTE**

If you have already created an alarm attribute template, you can click **Use Template** to set the automatic reporting status of the alarms.

3 Click Close.

----End

8.4 Monitoring Alarms

This topic describes how to monitor alarms. You can view the alarms reported to the U2000 in the topology view, alarm panel, and alarm list. On condition that network services are not affected, it is recommended that you make the NEs offline and then view the alarm reporting information on the U2000.

8.4.1 Monitoring Alarms Through the Topology View

You can monitor the alarm data of NEs in real time through the topology view.

8.4.2 Monitoring Alarms Through the Alarm Panel

On the alarm panel on the U2000 client, you can view the number of alarms of different severities, and know the latest alarm information by using the alarm panel functions of automatic display or automatic flash of the alarm indicator. In addition, you can open the alarm browse windows through the alarm panel.

8.4.3 Browsing the Current Alarm

You can browse the alarms that require attention and processing by setting the filtering conditions of the current alarm.

8.4.1 Monitoring Alarms Through the Topology View

You can monitor the alarm data of NEs in real time through the topology view.

Context

- In the topology view, the color of an NE icon depends on the alarm severity. If an NE generates multiple alarms at the same time, its icon displays the color of the highest severity among these generated alarms.
- When you move the pointer to the icon of the NE that generates alarms, a tip is displayed, prompting the alarm state, severity, and count.
- After choosing **File > Preferences > Topology Status Display**, if you set **Display Style of Alarm States** to **Use state icons**, the upper left corner of the NE that generates an alarm displays the alarm state icon and alarm severity icon.
- In the **Main Topology** window, click  on the toolbar. An current alarm is displayed in the lower area of the topology view. Click  again. The current alarm is hidden. Select a topology object in the topology view, and then select the **Display alarms of selected objects** check box. The current alarm displays the alarms of the selected object only.

Procedure

- 1 Choose **View > Main Topology** from the main menu.
- 2 In the **Main Topology** window, right-click the icon of an NE that generates alarms. From the displayed shortcut menu, choose menu items such as **Browse Alarm**.

 NOTE

In the window such as **Browse Current Alarm-Alarm Source**, all alarms generated by the NE are displayed.

----End

8.4.2 Monitoring Alarms Through the Alarm Panel

On the alarm panel on the U2000 client, you can view the number of alarms of different severities, and know the latest alarm information by using the alarm panel functions of automatic display or automatic flash of the alarm indicator. In addition, you can open the alarm browse windows through the alarm panel.

Procedure

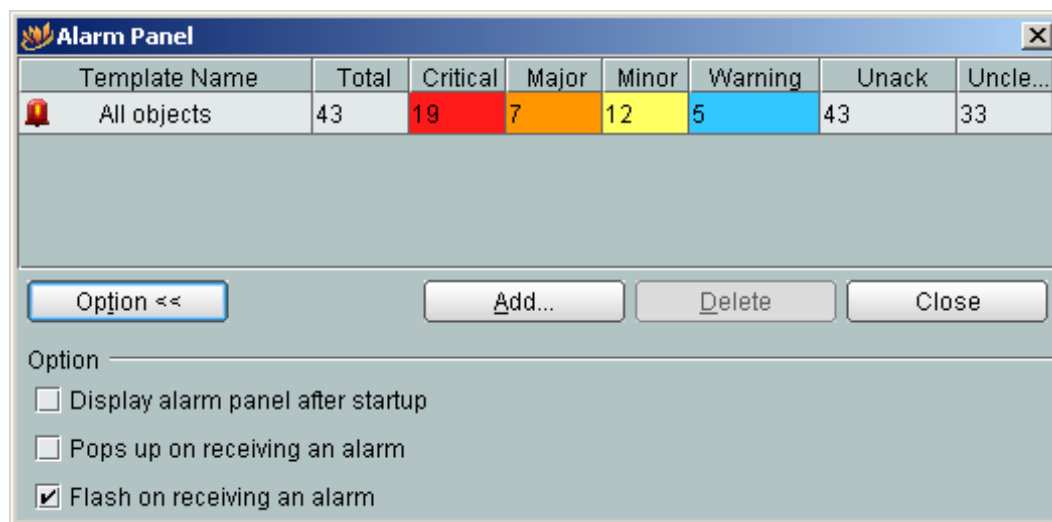
- Monitoring alarms through the alarm panel

Choose **Fault > Display Alarm Board** from the main menu or click the  icon on the menu bar to display the alarm panel. See [Figure 8-3](#). You can add current alarm templates to the alarm panel. The alarm panel displays alarm information according to the preset template.

 NOTE

The bar charts in the **Query Alarm Bar Chart** window correspond to the template displayed on the alarm panel. When you add or delete a alarm bar chart (alarm template) in the **Query Alarm Bar Chart** window, the corresponding alarm template is automatically added or deleted on the alarm panel. In the same way, when you perform add or delete operation on the alarm panel, the bar chart in the **Query Alarm Bar Chart** window is modified accordingly.

Figure 8-3 Alarm panel



- Opening the alarm browse windows through the alarm panel

When monitoring alarms through the alarm panel, you can double-click specific current alarm templates on the alarm panel and open the alarm browsing windows and view alarm details.

----End

8.4.3 Browsing the Current Alarm

You can browse the alarms that require attention and processing by setting the filtering conditions of the current alarm.

Context

- The current alarm displays the merged alarm logs. The alarm merging rule is that alarm logs with the same alarm ID, alarm location information, and alarm source are merged into one record in the current alarm.
- For a newly reported alarm log, if the current alarm contains the record that meets the alarm merging rule, the alarm log is merged into the previous record in the current alarm regardless of the acknowledgement and clearance status of the record. After merging, the frequency of the record is added by 1. The displayed acknowledgement and clearance state of the record is subject to that of the latest alarm log.
- You can query details of every alarm in the alarm log browse window.
- When you filter current alarm based on the template, if a user has modified the parameters in the template, you can click **No** in the **Confirm** window that is displayed after you close the **Browse Alarm List** window to revoke the template modification.

Procedure

- 1 Choose **Fault > Browse Current Alarm** from the main menu, or click  on the toolbar.
- 2 In the **Filter** dialog box, set the alarm query conditions.

 NOTE

If you set the default template, you need to click **Filter** to access the **Filter** dialog box.

- 3 Click **OK**.

The result is displayed in the window.

 NOTE

-  indicates an intermittent alarm.
-  indicates a high-frequency intermittent alarm.
-  indicates a correlative alarm.
-  indicates a root alarm.
- If you sort alarms by **Alarm Source**, alarms are sorted by the NE FDN (A NE identity) of alarm source, rather than the name of alarm source.
- Select **Display Latest Alarm** to refresh alarms displayed in the window in real time.
- Select **Scroll Lock** to keep the alarms displayed in the window unchanged.
- Click **Template** and choose **Open**. In the **Choose** window, you can re-select a template for filtering.
- Click **Filter** to reset the conditions for filtering alarms.
- Click **Refresh** to refresh alarms displayed in the window.
- Select one or more alarms in the window, and click **Acknowledge** to acknowledge the alarms.
- Select one or more alarms in the window, and click **Clear** to clear the alarms.
- Select one or more alarms in the window, and press **Ctrl+C** to copy the contents to the clipboard.
- Click  in the browse window. The **Details** and **Handling Suggestion** panels are hidden. Click  in the browse window. The **Details** and **Handling Suggestion** panels are shown.

----End

A FAQs

This topic provides answers to the most frequent questions concerning the installation.

[A.1 Windows OS](#)

This topic provides answers to FAQs about clients installed on Windows OS.

[A.2 SUSE Linux OS](#)

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

[A.3 Solaris OS](#)

This topic provides answers to FAQs about clients installed on Solaris OS.

[A.4 Veritas HA System](#)

This topic covers FAQs about the Veritas HA system.

[A.5 SQL Server Database](#)

This topic describes the FAQs about the SQL server database.

[A.6 Sybase Database](#)

This topic covers FAQs about the Sybase database.

[A.7 Oracle Database](#)

This topic describes the FAQs about the Oracle database.

[A.8 MSuite](#)

This topic covers FAQs about the MSuite.

[A.9 U2000 System](#)

This topic covers FAQs about the U2000 system.

A.1 Windows OS

This topic provides answers to FAQs about clients installed on Windows OS.

[A.1.1 How to Add a Static Route](#)

[A.1.2 How to Change the Password of the OS Administrator?](#)

[A.1.3 How to Configure the FTP Server in the Windows OS](#)

[A.1.4 How to Verify That the Video Driver Is Correctly Installed](#)

[A.1.5 How to Configure the Remote Login to the Windows OS](#)

[A.1.6 How to Forcibly End a Process](#)

[A.1.7 How to Configure the FTP, SFTP, or TFTP Service on Windows OS](#)

[A.1.8 How to Set the Virtual Memory to the System Managed Size](#)

A.1.1 How to Add a Static Route

Question

If the network connection is unstable, intermittently disconnected, or unreachable, the static route may be not added. How do I add a static route?



CAUTION

If there are multiple network interfaces and their IP addresses are within different network segments, the default gateway can be configured on only one of these network interfaces. To prevent the failure of one network interface from causing the disconnection of the entire network, the static route needs to be added on other network interfaces.

Answer

- 1 Run the following command on the command prompt window to view the existing routes:

```
C:\> route print
```

- 2 Run the following command to add a route:

```
C:\> route -p add network_IP_address mask netmask gateway_IP_address
```



NOTE

To delete a route, run the following command:

```
C:\> route delete network_IP_address mask netmask gateway_IP_address
```

----End

A.1.2 How to Change the Password of the OS Administrator?

Question

How to change the password of the OS administrator?

Answer

- 1 Log in to the OS as the **administrator** user.
- 2 Ensure that the SQL server database is started.



NOTE

If the database is not started, manually start it. Otherwise, login to the database fails after the password is changed.

If the password of the administrator is changed when the SQL server database is not started, login to the database fails. In this case, you need to change the password to the original one, start the SQL server database, and then change the password of the administrator.

- 3 Press **Ctrl+Alt+Delete** to lock the current interface.
- 4 In the dialog box that is displayed, click **Change Password**.
- 5 In the dialog box that is displayed, enter the old password and the new password, and confirm the new password.
- 6 Click **OK**.
- 7 Right-click the database server node of the enterprise manager and choose **Properties** from the shortcut menu. In the dialog box that is displayed, click the **Security** tab, and then change the administrator password in the **Enable Service Account** area.

----End

A.1.3 How to Configure the FTP Server in the Windows OS

Question

How to Configure the FTP Server in the Windows OS?

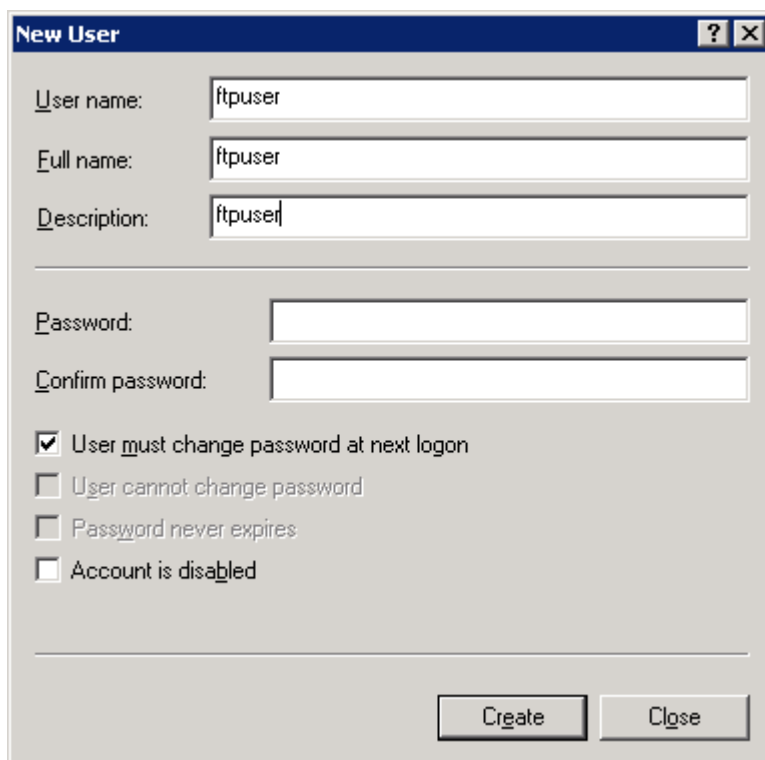


NOTE

This topic takes the FTP server function of the Windows 2003 OS as an example. A third-party tool, such as Wftp32, can also be used to configure the FTP server.

Answer

- 1 Click **Start > Settings > Control Panel**.
- 2 On the **Control Panel** window that appears, double-click the administrative tools icon to open the **Administrative Tools** window.
- 3 Double-click the **Computer Management** icon in the **Administrative Tools** window.
- 4 In the **Computer Management** window that appears, unfold the **Local Users and Groups** node. Right click the **Users**, and select **New User** to open the **New User** dialog.

A screenshot of a 'New User' dialog box. The dialog has a title bar with a question mark and a close button. It contains several text input fields: 'User name:' with 'ftpuser', 'Full name:' with 'ftpuser', 'Description:' with 'ftpuser', 'Password:', and 'Confirm password:'. Below these fields are four checkboxes: 'User must change password at next logon' (checked), 'User cannot change password' (unchecked), 'Password never expires' (unchecked), and 'Account is disabled' (unchecked). At the bottom right are 'Create' and 'Close' buttons.

New User

User name: ftpuser

Full name: ftpuser

Description: ftpuser

Password:

Confirm password:

☒ User must change password at next logon

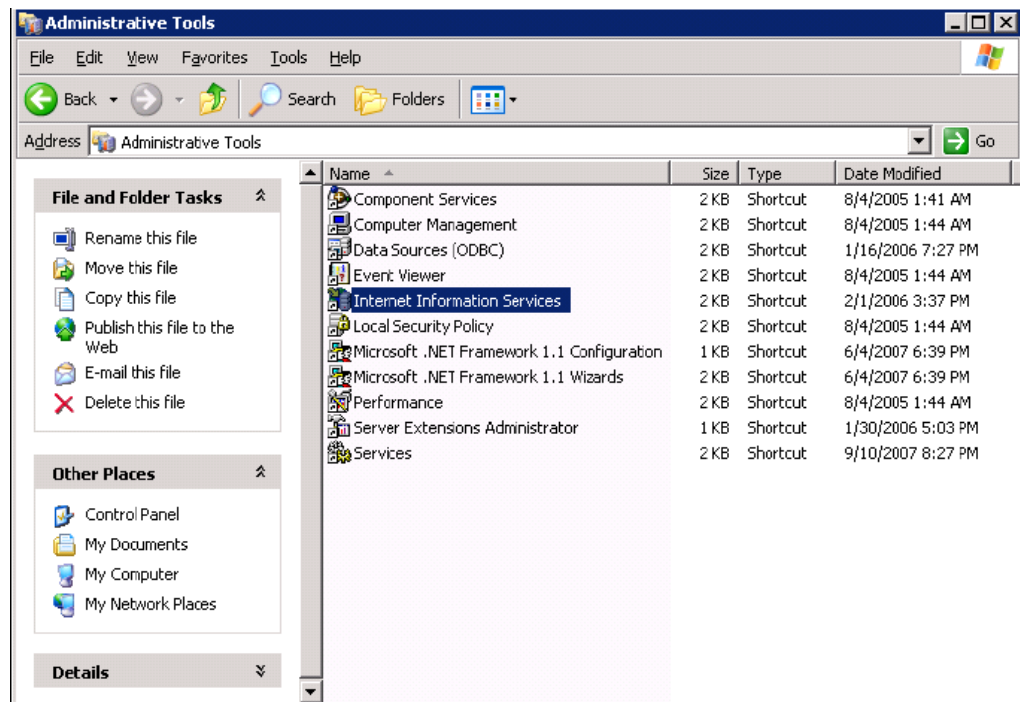
☐ User cannot change password

☐ Password never expires

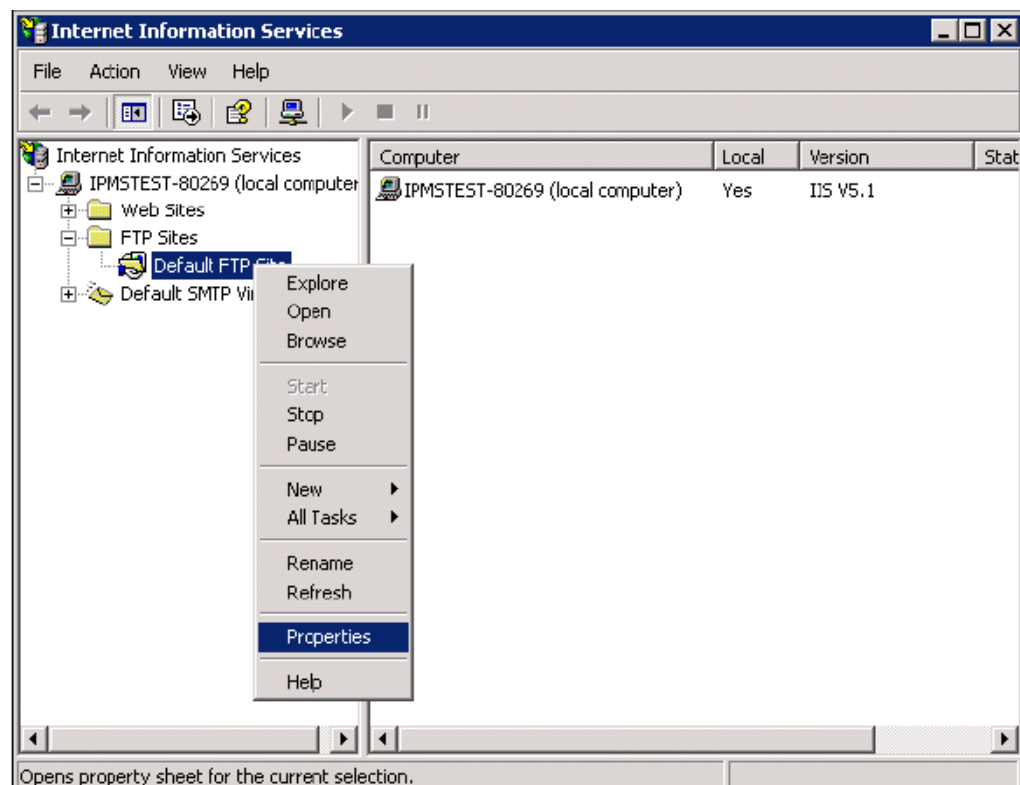
☐ Account is disabled

Create Close

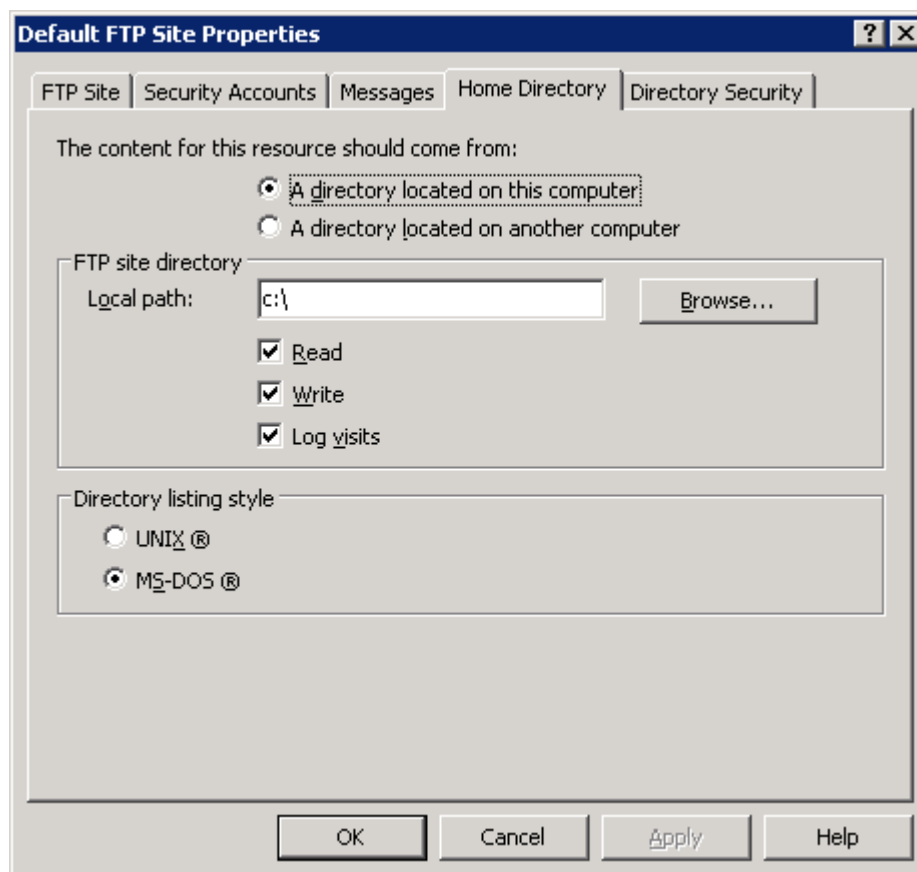
- 5 Enter the **User name** and the **Password**, click **Create** to create the **FTP** user account.
- 6 Click **Start > Settings > Control Panel**.
- 7 On the **Control Panel** window, double click **Add or Remove Programs** to display the **Add or Remove Programs** dialog box.
- 8 Click **Add/Remove Windows Components** in the **Add/Remove Programs** dialog. In the **Windows Component Wizard** dialog that appears, select the check box **Application Server** and click **Details** button to open the **Application Server** dialog.
- 9 Select the check box **Internet Information Services (IIS)** and click **Details** button to open the **Internet Information Services (IIS)** dialog. Select the check box **File Transfer Protocol (FTP) Service** in the **Internet Information Services (IIS)** dialog, click **OK** and click **Next** to configure the **FTP Server** on Windows.
- 10 On the control panel, double click the **Administrative Tools** icon. In the dialog that appears, double click the **Internet Services Manager** icon , as shown below.



- 11 In the **Internet Information Services** dialog that appears, right click **Default FTP Site**, and select **Properties**, as shown below.



- 12 Check the **Allow Anonymous Connections** check box, and input the user name and password.
- 13 Select the **Home Directory** tab, as shown below.



- 14 In the **FTP Site Directory** area, specify **Local Path** as the root directory storing the data and software, and then click **OK**.

----End

A.1.4 How to Verify That the Video Driver Is Correctly Installed

Question

How do I verify that the video driver is correctly installed?

Answer

- 1 Right-click **My Computer** on the desktop and choose **Properties** from the shortcut menu.
- 2 In the **System Properties** dialog box, click the **Hardware** tab.
- 3 On the **Hardware** tab page, click **Device Manager**.

In the **Device Manager** dialog box, expand **Display adapters** and check whether the video driver is correctly installed. If a question mask (?) or red cross (X) is displayed, the video driver is not correctly installed. Check and reinstall the video driver.

----End

A.1.5 How to Configure the Remote Login to the Windows OS

Question

How to configure the remote login to the Windows OS?

Answer

- 1 Log in to the OS as the administrator.
- 2 Right-click **My Computer** and choose **Properties** from the shortcut menu.
- 3 In the **System Properties** dialog box, click the **Remote** tab.
- 4 Select the **Enable Remote Desktop on this computer** check box and click **OK**.

----End

A.1.6 How to Forcibly End a Process

Question

How do I forcibly end a process?

Answer

- 1 Press **Ctrl+Shift+Esc**. The **Windows Task Manager** dialog box is displayed.
- 2 Click the **Processes** tab. Right-click the process needs to be ended, and choose **End Process**.

----End

A.1.7 How to Configure the FTP, SFTP, or TFTP Service on Windows OS

Question

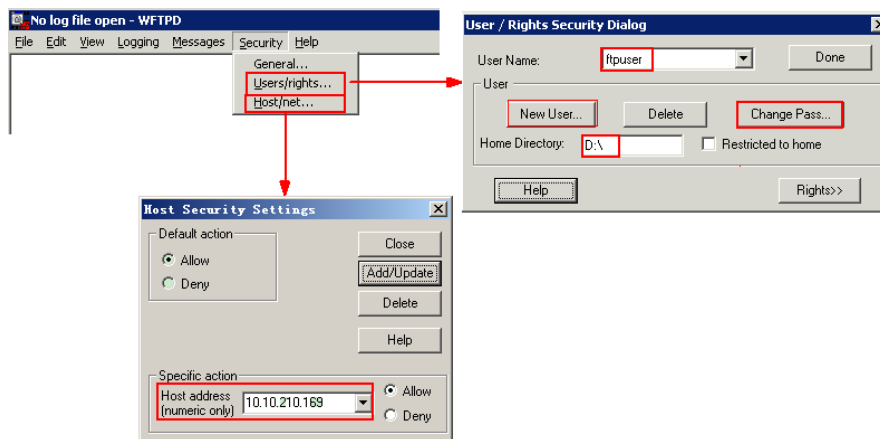
How do I configure the FTP, SFTP, or TFTP service on Windows OS?

NOTE

The third-party tool must be started after the FTP, SFTP, or TFTP server is configured.

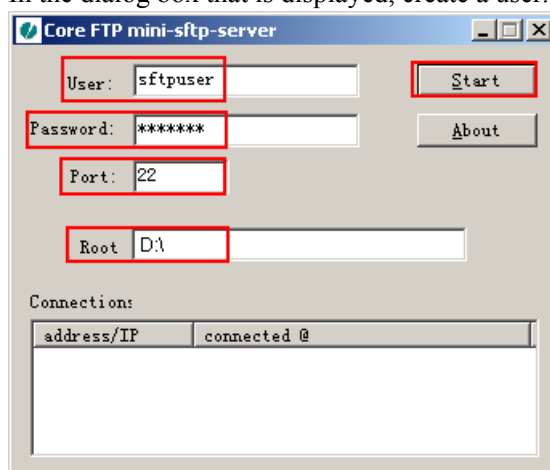
Answer

- **Configuring the FTP server using the third-party tool wftpd32.exe**
 1. Copy the **wftpd32.exe** file to the U2000 server and double-click the file.
 2. In the dialog box that is displayed, choose **Security > Users/rights** and create a user; choose **Security > Host/net** and enter the IP address of the FTP server.



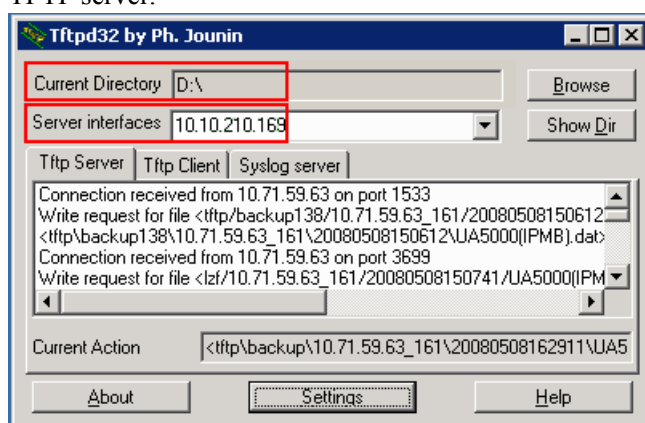
- **Configuring the SFTP server using the third-party tool msftpsrvr.exe**

1. Copy the **msftpsrvr.exe** file to the U2000 server and double-click the file.
2. In the dialog box that is displayed, create a user.



- **Configuring the TFTP server by using the third-party tool tftpd32.exe**

1. Copy the **tftpd32.exe** file to the U2000 server and double-click the file.
2. In the dialog box that is displayed, set the root directory and the IP address of the TFTP server.



----End

A.1.8 How to Set the Virtual Memory to the System Managed Size

Question

How to set the virtual memory to the system managed size?

Answer

- 1 Right-click **My Computer** and choose **Properties** from the shortcut menu.
- 2 In the **System Properties** dialog box, click the **Advanced** tab.
- 3 In the **Performance** area, click **Settings**.
- 4 In the **Performance Options** dialog box, click the **Advanced** tab.
- 5 In the **Virtual memory** area, click **Change**.
- 6 In the **Virtual Memory** dialog box, click the **System managed size** option button.
- 7 Click **Set**.
- 8 Click **OK**.

----End

A.2 SUSE Linux OS

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

[A.2.1 How to Start/Stop the FTP, TFTP, SFTP, and Telnet Services](#)

[A.2.2 How to Enable and Disable the FTP/Telnet Authority of the root User in the SUSE Linux OS?](#)

[A.2.3 How to Check the Remaining Space of a Disk](#)

[A.2.4 How to Monitor System Processes and Application Ports?](#)

[A.2.5 How to Log In to the OS Through the Remote Login Tools?](#)

[A.2.6 How to Query the Process Status](#)

[A.2.7 How to Forcibly End a Process](#)

[A.2.8 How to Use the vi Editor](#)

[A.2.9 How to Change the Time and Time Zone of the SUSE Linux OS?](#)

A.2.1 How to Start/Stop the FTP, TFTP, SFTP, and Telnet Services

Question

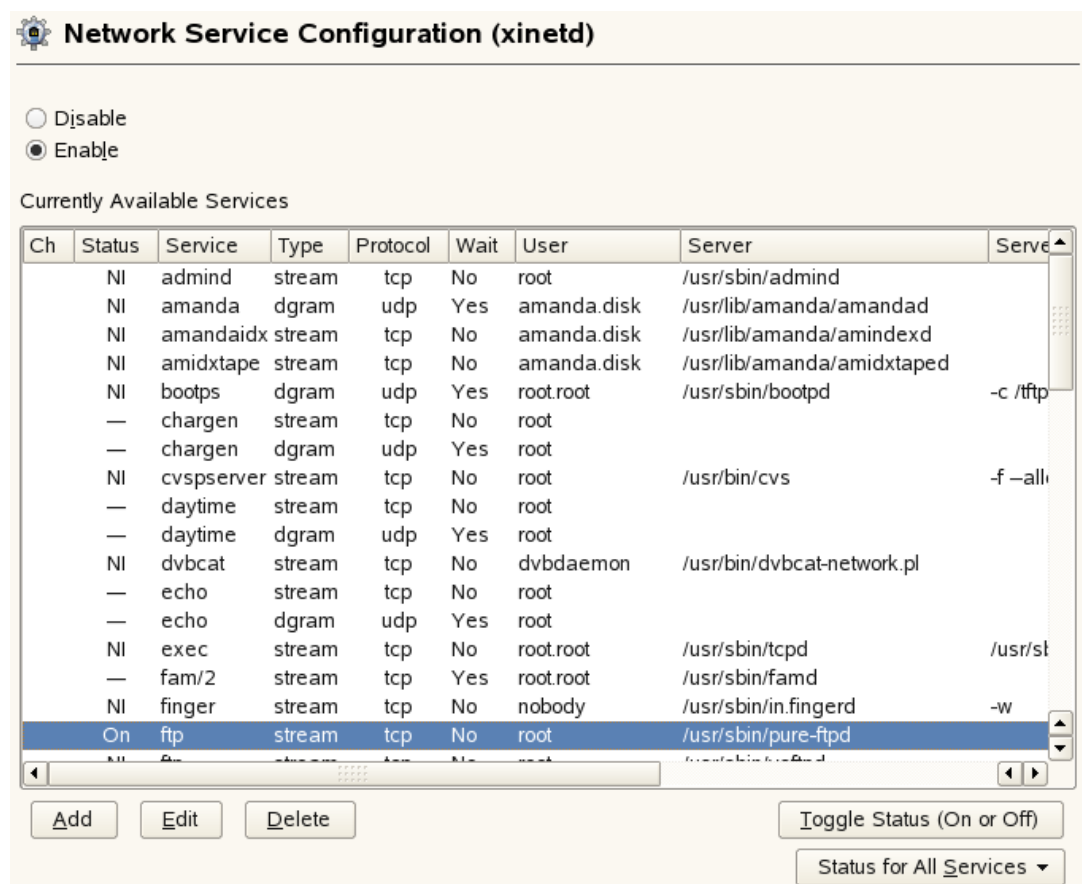
How to start/stop the FTP, TFTP, SFTP, and Telnet services in the SUSE Linux OS?

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 A-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

A.2.2 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

A.2.3 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.

A.2.4 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.

A.2.5 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
```

```
# rxdm restart
```
- 3 Use the remote login tools to log in to the U2000 server again.
----End

A.2.6 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.

A.2.7 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.

A.2.8 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.

Command	Function
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 A-1](#).

Table A-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.

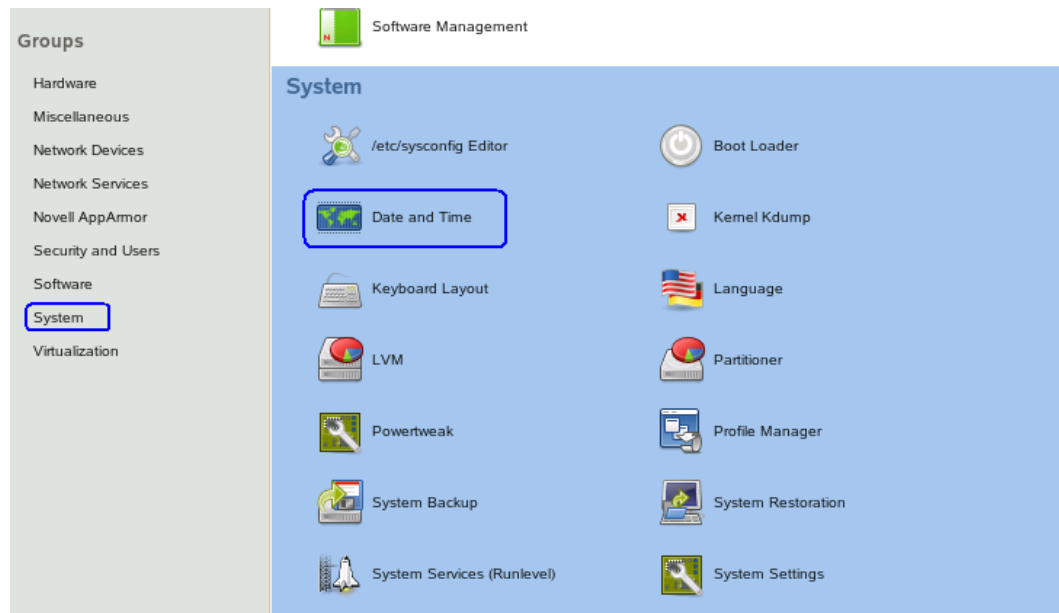
A.2.9 How to Change the Time and Time Zone of the SUSE Linux OS?

Question

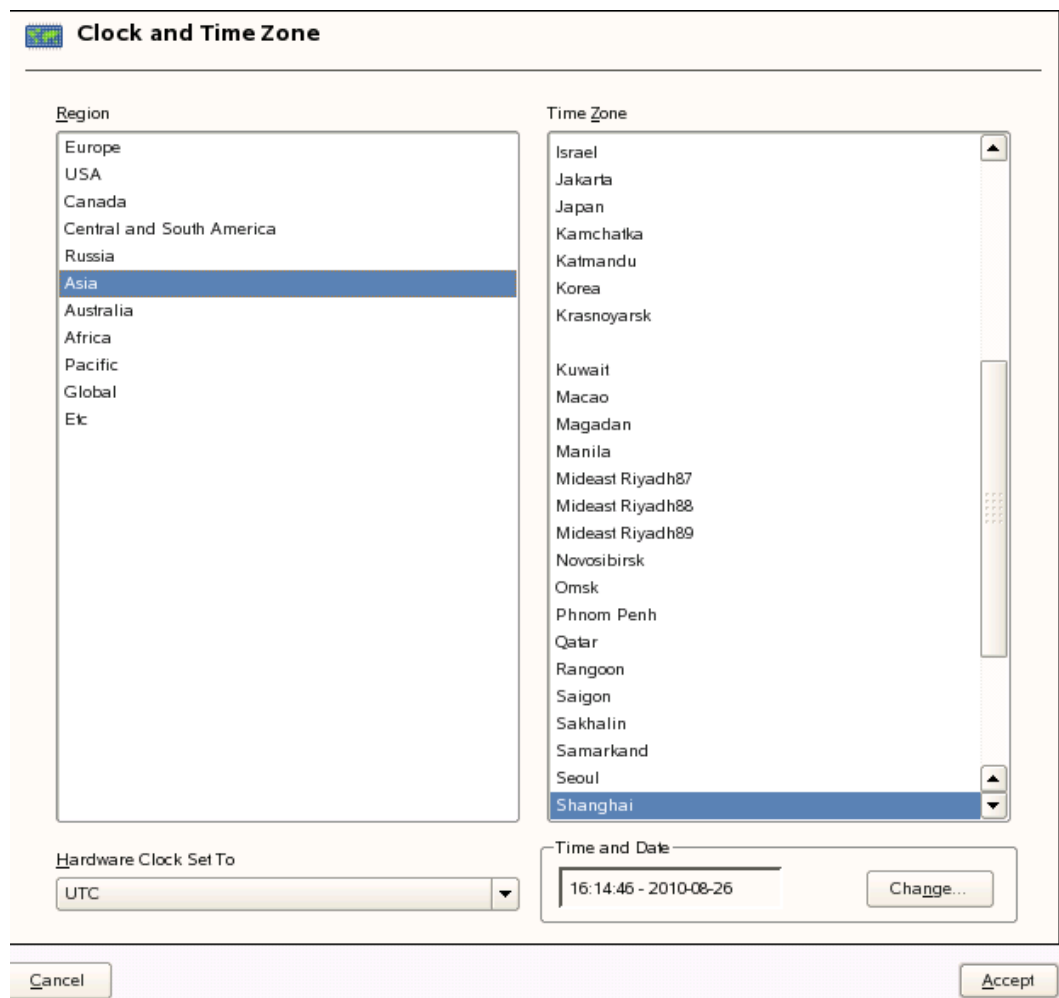
How to change the time and time zone of a SUSE Linux OS where the U2000 is not installed yet?

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

A.3 Solaris OS

This topic provides answers to FAQs about clients installed on Solaris OS.

[A.3.1 Network Configurations of the Workstation](#)

This topic provides answers to FAQs about the network configurations of the workstation.

[A.3.2 System Settings of the Workstation](#)

This topic covers FAQs about workstation system settings.

[A.3.3 FTP and Telnet Service Configuration](#)

This topic covers the FAQs about the FTP and Telnet service configuration.

[A.3.4 Usage and Maintenance of Workstation](#)

This topic covers the FAQs about the usage and maintenance of the workstation.

A.3.1 Network Configurations of the Workstation

This topic provides answers to FAQs about the network configurations of the workstation.

[A.3.1.1 How to Make the Devices Directly Connected to the two NICs of the Server Communicate with Each Other](#)

[A.3.1.2 How to Add the Default Route](#)

[A.3.1.3 How to Add a Static Route](#)

[A.3.1.4 How to Query the Gateway of a Sun Workstation](#)

[A.3.1.5 How to Configure the DNS on Solaris OS](#)

[A.3.1.6 How to Check the NIC Type of a Server](#)

A.3.1.1 How to Make the Devices Directly Connected to the two NICs of the Server Communicate with Each Other

Question

How do I make the devices directly connected to the two NICs of the server communicate with each other?

Answer

- 1 Log in the OS as user **root**.
- 2 Run the following command to enable the route forwarding function:

```
# ndd -set /dev/ip ip_forwarding 1
```

- 3 To prevent the command from being invalid after the workstation is restarted, create a file whose filename begins with an S in the `/etc/rc3.d` directory, and type **ndd -set /dev/ip ip_forwarding 1** into the file. Use the **Srouter** file as an example:

```
# vi /etc/rc3.d/Srouter
```

Write **ndd -set /dev/ip ip_forwarding 1** into the file.

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

 NOTE

When creating a file whose filename begins with an S in the `/etc/rc3.d` directory, run the following command to view the existing files in the `/etc/rc3.d` directory. Ensure that the filename is unique in the path.

```
# ls /etc/rc3.d
```

----End

A.3.1.2 How to Add the Default Route

Question

How do I add the default route?

Answer

- 1 Log in the OS as user **root**.
- 2 Open a terminal window in the Solaris OS.
- 3 Run the following command:

```
# vi /etc/defaultrouter
```
- 4 Enter an IP address as the default route in the file, for example, 129.9.1.254.
- 5 Run the **vi** command to save and close the file.
- 6 Run the following commands to restart the server:

```
# sync;sync;sync;sync  
# shutdown -y -g0 -i6
```
- 7 Log in to the Solaris OS as the **root** user. Run the **netstat -nr** command to view the default route of the system.

----End

A.3.1.3 How to Add a Static Route

Question

How do I add a static route?

Answer

- 1 Log in to the system as user **root**.
- 2 Run the following command in the **Terminal** window to view the existing routes in the system:

```
# netstat -nr
```

- 3 Run the following command to add a route:

```
# route add network_IP_address -netmask netmask gateway_IP_address
```

Routes added this way will disappear after the system reboots. To prevent this from happening, create the startup file **S98router** in the **/etc/rc3.d** directory and type the command **route add network_IP_address -netmask netmask gateway_IP_address** into the boot script.

After creating the **S98router** file, run the following command to set the **S98router** file to be executed:

```
# chmod a+x S98router
```

NOTE

Run the following command to delete a route:

```
# route delete network_IP_address -netmask netmask gateway_IP_address
```

----End

A.3.1.4 How to Query the Gateway of a Sun Workstation

Question

How do I query the gateway of a Sun workstation?

Answer

- 1 Log in to the OS as user **root** and open the terminal window.
- 2 Run the following command to query the workstation:

```
# netstat -nr
```

The following message will be displayed:

```
Routing Table: IPv4
  Destination      Gateway            Flags   Ref    Use  Interface
-----
10.71.224.0        10.71.225.24      U        1    1006   bge0
224.0.0.0          10.71.225.24      U        1        0   bge0
default            10.71.224.1       UG       1 114902
127.0.0.1          127.0.0.1         UH       6  25558   lo0
```

NOTE

- The contents displayed on the terminal will vary according to the route configuration.
- The gateway with **UG** listed in the **Flags** is the gateway of the workstation. In this example, the IP address of the workstation gateway is *10.71.224.1*. There are five flags (UGHDM) for a specified route.

----End

A.3.1.5 How to Configure the DNS on Solaris OS

Question

How do I configure the DNS on Solaris OS?

Answer

- 1 Log in to the OS as user **root**.
- 2 Run the following command to open the **nsswitch.conf** file:
`# vi /etc/nsswitch.conf`
- 3 In the **nsswitch.conf** file in the **/etc** directory, add **dns** to the end of the line where **hosts:file** is located. The following message will be displayed:
`hosts: files dns`
- 4 Create the **/etc/resolv.conf** file and add contents in the following format:
`domain domain name address nameserver DNS IP address`
For example:
`domain huawei.com nameserver 10.15.1.3`
- 5 Save the configuration and exit.

----End

A.3.1.6 How to Check the NIC Type of a Server

Question

How do I check the NIC type of a server?

Answer

You can run the **more /etc/path_to_inst | grep network** command as user **root** to check the NIC type of a server.

A.3.2 System Settings of the Workstation

This topic covers FAQs about workstation system settings.

[A.3.2.1 How to Boot Up the Workstation from the CD-ROM Drive](#)

[A.3.2.2 How to Enable Input Modes on Solaris OS](#)

[A.3.2.3 How to Set the Interface Language of Solaris OS](#)

[A.3.2.4 How to Call the GUI Management Tool in Solaris 10 OS](#)

[A.3.2.5 How to Start the Snapshot Tool When It Is Unavailable](#)

[A.3.2.6 How to Switch to the Multi-user Mode or Single-user Mode](#)

[A.3.2.7 How to Open the Terminal Window on the Desktop in the JDS](#)

[A.3.2.8 How to Operate the CD-ROM](#)

A.3.2.1 How to Boot Up the Workstation from the CD-ROM Drive

Question

How do I boot up the workstation from the CD-ROM drive?

Answer

- 1 At the # prompt, run the following command to display the **OK** prompt (OK>):
init 0
- 2 After the OK prompt is displayed, insert the installation DVD of Solaris OS into the CD-ROM drive.
- 3 Enter **boot cdrom** and press **Enter**.

----End

A.3.2.2 How to Enable Input Modes on Solaris OS

Question

How do I solve the problem that occurs when the switch between the Chinese and English input modes fails on Solaris OS?

Answer

- 1 In most cases, the problem occurs when input modes is disabled. Enable the input modes if they are disabled.
- 2 Run the following commands to enable the input modes:

```
# cd /usr/openwin/bin
# ./htt -nosm
```

NOTE

This operation needs to be performed in an environment supporting GUIs. After the input modes are enabled, the **Htt** flag is displayed in the upper left corner of the screen. Press **Ctrl+Space** to switch between input modes. If the operation is performed on the emulation terminal WinaXe, press **Ctrl+Shift+Space** to switch between input modes.

----End

A.3.2.3 How to Set the Interface Language of Solaris OS

Question

How do I set the interface language of Solaris OS?

Answer

- 1 Power on the workstation, and start Solaris OS.

- 2 Choose **Options > Language**. A dialog box will be displayed prompting you to select a language.
- 3 Select the system language from the list box according to the conditions at your site.
- 4 Click **OK**.

If you want to save the setting of the system language, select **Set selected language as default**.

----End

A.3.2.4 How to Call the GUI Management Tool in Solaris 10 OS

Question

How do I call the GUI management tool in Solaris 10 OS?

Answer

- 1 Log in to Solaris 10 OS through the GUI. Then, run the following command to call the GUI management tool:

```
# smc &
```

----End

A.3.2.5 How to Start the Snapshot Tool When It Is Unavailable

Question

How do I start the snapshot tool when it is unavailable from the shortcut menu? Determine if the snapshot tool is available by right-clicking the desktop. Options related to the snapshot tool will display if they are available. If they are not available, how do I start the snapshot tool?

Answer

- 1 The snapshot tool is attached to Solaris OS. Generally, it is available using the shortcut application. If the snapshot tool is unavailable in the shortcut application, run the following command to start it:

```
#/usr/dt/bin/sdtimage -snapshot
```

----End

A.3.2.6 How to Switch to the Multi-user Mode or Single-user Mode

Question

How do I switch to the multi-user mode or single-user mode?

Answer

- Run the following command to switch to the multi-user mode:

```
ok> boot
```

- Run the following command to switch to the single-user mode:

```
ok> boot -s
```

----End

A.3.2.7 How to Open the Terminal Window on the Desktop in the JDS

Question

How do I open the terminal window on the desktop in the Java Desk System (JDS)?

Answer

- 1 Open the desktop in the JDS.
 1. Enter the user name for login, such as **root**.
 2. Choose **Options > Session > Java Desktop System** to select the JDS.
 3. Click **OK**. Enter the password for the user, such as **root**.
 4. Click **OK** to log in to the desktop in the JDS.
- 2 Right-click on the desktop in the JDS and choose **Open Terminal** from the shortcut menu to open a terminal window.

----End

A.3.2.8 How to Operate the CD-ROM

Question

How do I operate the CD-ROM?

Answer

- 1 If the Sun workstation has a built-in CD-ROM drive, perform the following operation:
The system automatically installs the CD-ROM to the **/cdrom** directory after startup. If there is a CD-ROM in the CD-ROM drive, view the contents of the CD-ROM after accessing the **/cdrom** directory.
- 2 If the Sun workstation has an external CD-ROM drive, perform the following operation:
Power on the CD-ROM drive after the SCSI wire is connected. Then, power on the workstation. The system automatically identifies and installs the CD-ROM to the **/cdrom** directory after startup.
- 3 Use appropriate commands to open the CD-ROM drive.

If there is a CD-ROM in the CD-ROM drive, run appropriate commands to open the CD-ROM drive.

Verify that the CD-ROM is not being used by any program and exit the directory for the CD-ROM. Run the following command as user **root**:

eject

Open the CD-ROM drive and take out the CD-ROM.

**NOTE**

If the system prompts "Device busy" and the CD-ROM cannot be ejected, run the following command as user **root**:

```
# svcadm disable volfs
```

Press the eject button on the drive panel to take out the CD-ROM.

The drive becomes unavailable in this situation. Run the following command:

```
# svcadm enable volfs
```

The CD-ROM drive can then be used.

4 Install or start the system from the CD-ROM.

Insert the CD-ROM to the drive, and then run the following command at the OK prompt on the workstation:

```
OK> boot cdrom
```

By doing this, you can install or start the system from the CD-ROM.

5 Check the SCSI device mounted on the workstation.

Enter the following command at the OK prompt:

```
OK> probe-scsi
```

By doing this, you can check the SCSI device mounted on the workstation. This command is usually used to verify that the CD-ROM drive is correctly mounted.

----End

A.3.3 FTP and Telnet Service Configuration

This topic covers the FAQs about the FTP and Telnet service configuration.

[A.3.3.1 How to Start/Stop the FTP, TFTP, SFTP, and Telnet Services](#)

[A.3.3.2 How to Enable and Disable the FTP/Telnet Authority of user root on Solaris OS](#)

[A.3.3.3 How to Transfer Files by Means of FTP](#)

A.3.3.1 How to Start/Stop the FTP, TFTP, SFTP, and Telnet Services

Question

How do I start/stop the FTP, TFTP, SFTP, and Telnet services?

Answer

Use the following methods to start/stop the FTP, TFTP, SFTP, and Telnet services. You are recommended to restore the original settings afterwards.

- Start the FTP, TFTP, SFTP, and Telnet services as follows:
 - Starting the FTP service
 1. Log in to Solaris OS as user **root**.
 2. Run the following command to start the FTP service:


```
online          22:07:11 svc:/network/tftp/udp6:default
```

3. Run the following command to modify the **inetd** configuration file:
`# vi /etc/inetd.conf`
 Add # to the left of TFTPd.
4. Run the following command to verify that the TFTP service is stopped:
`# svcs -a|grep tftp`
 If there is no response, the TFTP service is stopped.
- Stopping the SFTP service
 1. Log in to Solaris OS as user **root**.
 2. Run the following command to stop the SFTP service:
`# svcadm disable network/ssh`
- Stopping the Telnet service
 1. Log in to Solaris OS as user **root**.
 2. Run the following command to stop the Telnet service:
`# svcadm disable telnet`

A.3.3.2 How to Enable and Disable the FTP/Telnet Authority of user root on Solaris OS

Question

How do I enable and disable the FTP/Telnet authority for user **root** on Solaris OS?

Answer

- 1 Enable or disable the FTP authority for user **root** as follows:
 - Enabling the FTP authority for user **root**
 1. Log in to Solaris OS as user **root**.
 2. Run the following commands to enable the FTP authority for user **root**:
`# svcadm enable ftp`
`# sed "/^root/s///#root/g" /etc/ftpd/ftpusers > /tmp/ftpusers`
`# cp /tmp/ftpusers /etc/ftpd/ftpusers`
 - Disabling the FTP authority for user **root**
 1. Log in to Solaris OS as user **root**.
 2. Run the following commands to enable the FTP authority for user **root**:
`# svcadm disable ftp`
`# sed "/^#root/s///#root/g" /etc/ftpd/ftpusers > /tmp/ftpusers`
`# cp /tmp/ftpusers /etc/ftpd/ftpusers`
- 2 Enable or disable the Telnet authority for user **root** as follows:
 - Enabling the Telnet authority for user **root**
 1. Log in to the Solaris OS as user **root**.
 2. Run the following commands to enable the Telnet authority of user **root**:
`# svcadm enable telnet`
`# sed "/^CONSOLE/s///#CONSOLE/g" /etc/default/login > /tmp/login`
`# cp /tmp/login /etc/default/login`

- Disabling the Telnet authority for user **root**

1. Log in to Solaris OS as user **root**.
2. Run the following commands to disable the Telnet authority of the **root** user:

```
# svcadm disable telnet
# sed "/^#CONSOLE/s//CONSOLE/g" /etc/default/login > /tmp/login
# cp /tmp/login /etc/default/login
```

----End

A.3.3.3 How to Transfer Files by Means of FTP

Question

How do I transfer files by means of FTP?

 NOTE

The available FTP modes are ASCII (default) and binary.

To ensure that files are available after transfer, determine the FTP transfer mode before transferring files. Generally, license files are transferred in ASCII mode whereas binary files such as NMS installation programs and databases **interfaces** files are transferred in binary mode.

Answer

- 1 Run the following command to connect to the server by means of FTP:

ftp *server IP address*

Enter the user name and password of the server.

- 2 Set the FTP transfer mode.

- To use the ASCII mode, run the **ascii** command.
- To use the binary mode, run the **bin** command.

- 3 Go to the path to files to be transferred.

lcd *path of files to be transferred*

- 4 Go to the path where the files are to be transferred.

cd *path to which the files are to be transferred*

- 5 Run the following **put** command to transfer files:

put *names of files to be transferred*

- 6 After the files are transferred, run the **quit** command to break the FTP connection.

----End

A.3.4 Usage and Maintenance of Workstation

This topic covers the FAQs about the usage and maintenance of the workstation.

[A.3.4.1 How to View the Versions and Release Date of the Solaris OS](#)

[A.3.4.2 How to View Hardware Configurations for the Sun Workstation](#)

[A.3.4.3 How to Check Whether the Hard Disk of the Sun Workstation Is Damaged](#)

[A.3.4.4 How to Check the Partition of Solaris OS](#)

[A.3.4.5 How to Check the Remaining Space of a Disk](#)

[A.3.4.6 How to Decompress Files](#)

[A.3.4.7 How to Remotely Log In to the System as User root](#)

[A.3.4.8 How to Access the OS from the Controller](#)

[A.3.4.9 How to Switch Between the Console, OK Prompt, and # Prompt](#)

[A.3.4.10 How to Use the vi Editor](#)

[A.3.4.11 How to Use the Text Editor](#)

[A.3.4.12 How to Query the Process Status](#)

[A.3.4.13 How to Forcibly End a Process](#)

[A.3.4.14 How to Deploy a Solaris Single-Server System If Data Is Stored on Some Hard Disks](#)

A.3.4.1 How to View the Versions and Release Date of the Solaris OS

Question

How do I view the versions and release date of Solaris OS?

Answer

1 Open a terminal window on Solaris OS.

2 Run the following command to view the version information about Solaris OS:

```
# uname -a
```

The Solaris version is Solaris 10 and the core patch version is 141414-07 if the following message is displayed:

```
SunOS NMSServer 5.10 Generic_141414-07 sun4v sparc SUNW,SPARC-Enterprise-T5220
```

3 Run the following command to view the release date of Solaris OS:

```
# more /etc/release
```

A message similar to the following will be displayed:

```
.....
Copyright 2007 Sun Microsystems, Inc. All Rights Reserved.
Use is subject to license terms.
Assembled 16 August 2007
```

----End

A.3.4.2 How to View Hardware Configurations for the Sun Workstation

Question

How do I view hardware configurations for the Sun workstation?

Answer

- 1 Log in to the Sun workstation as the **root** user. Then, run the following commands:

```
# cd /usr/platform/`uname -i`/sbin
```

```
# ./prtdiag
```

A message similar to the following is displayed:

```
System Configuration: Sun Microsystems sun4u Sun Fire V445
System clock frequency: 199 MHZ
Memory size: 8GB
```

```
===== CPUs =====
CPU  Freq      E$      CPU      CPU      Status  Location
----  ----      -
0    1592 MHz  1MB      SUNW,UltraSPARC-IIIi  3.4    on-line  MB/C0/P0
1    1592 MHz  1MB      SUNW,UltraSPARC-IIIi  3.4    on-line  MB/C1/P0
2    1592 MHz  1MB      SUNW,UltraSPARC-IIIi  3.4    on-line  MB/C2/P0
3    1592 MHz  1MB      SUNW,UltraSPARC-IIIi  3.4    on-line  MB/C3/P0
```

```
===== IO Devices =====
Bus    Freq  Slot +  Name +
Type   MHz  Status  Path
-----
pci     199  MB      pci14e4,1668 (network)
        okay  /pci@1e,600000/pci@0/pci@1/pci@0/network@4

pci     199  MB      pci14e4,1668 (network)
        okay  /pci@1e,600000/pci@0/pci@1/pci@0/network@4,1

pci     199  MB/PCI2  SUNW,XVR-100 (display)      SUNW,375-3290
        okay  /pci@1e,600000/pci@0/pci@1/pci@0/pci@8/SUNW,XVR-100@1

pci     199  MB      pci10b9,5229 (ide)
        okay  /pci@1f,700000/pci@0/pci@1/pci@0/ide@1f

pci     199  MB      pci14e4,1668 (network)
        okay  /pci@1f,700000/pci@0/pci@2/pci@0/network@4

pci     199  MB      pci14e4,1668 (network)
        okay  /pci@1f,700000/pci@0/pci@2/pci@0/network@4,1

pciex   199  MB      scsi-pciex1000,58 (scsi-2)  LSI,1068E
        okay  /pci@1e,600000/pci@0/pci@2/scsi@0
```

```
===== Memory Configuration =====
Segment Table:
```

Base Address	Size	Interleave Factor	Contains
0x0	2GB	4	BankIDs 0,1,2,3
0x1000000000	2GB	4	BankIDs 16,17,18,19
0x2000000000	2GB	4	BankIDs 32,33,34,35
0x3000000000	2GB	4	BankIDs 48,49,50,51

Bank Table:

ID	Physical Location ControllerID	GroupID	Size	Interleave Way
0	0	0	512MB	0,1,2,3
1	0	1	512MB	
2	0	1	512MB	
3	0	0	512MB	
16	1	0	512MB	0,1,2,3
17	1	1	512MB	

18	1	1	512MB	
19	1	0	512MB	
32	2	0	512MB	0,1,2,3
33	2	1	512MB	
34	2	1	512MB	
35	2	0	512MB	
48	3	0	512MB	0,1,2,3
49	3	1	512MB	
50	3	1	512MB	
51	3	0	512MB	

Memory Module Groups:

ControllerID	GroupID	Labels	Status
0	0	MB/C0/P0/B0/D0	okay
0	0	MB/C0/P0/B0/D1	okay
0	1	MB/C0/P0/B1/D0	okay
0	1	MB/C0/P0/B1/D1	okay
1	0	MB/C1/P0/B0/D0	okay
1	0	MB/C1/P0/B0/D1	okay
1	1	MB/C1/P0/B1/D0	okay
1	1	MB/C1/P0/B1/D1	okay
2	0	MB/C2/P0/B0/D0	okay
2	0	MB/C2/P0/B0/D1	okay
2	1	MB/C2/P0/B1/D0	okay
2	1	MB/C2/P0/B1/D1	okay
3	0	MB/C3/P0/B0/D0	okay
3	0	MB/C3/P0/B0/D1	okay
3	1	MB/C3/P0/B1/D0	okay
3	1	MB/C3/P0/B1/D1	okay

===== USB Devices =====

Name	Port#
-----	-----
hub	HUB0

Details about the message are as follows:

- The following information indicates a workstation model. In this example, the workstation model is **Sun Fire V445**.

System Configuration: Sun Microsystems sun4u Sun Fire V445
System

- The following information indicates the system clock frequency. In this example, the workstation clock frequency is **199 MHZ**.

System clock frequency: 199 MHZ

- The following information indicates the memory configuration for the workstation. In this example, the memory configuration for the workstation is **8GB**.

Memory size: 8GB

- The following information indicates the CPU configuration for the workstation. In this example, the CPU configuration for the workstation is **4Core**.

===== CPUs =====

CPU	Freq	E\$ Size	CPU Implementation	CPU Mask	Status	Location
---	-----	-----	-----	-----	-----	-----
0	1592 MHz	1MB	SUNW,UltraSPARC-IIIfi	3.4	on-line	MB/C0/P0
1	1592 MHz	1MB	SUNW,UltraSPARC-IIIfi	3.4	on-line	MB/C1/P0
2	1592 MHz	1MB	SUNW,UltraSPARC-IIIfi	3.4	on-line	MB/C2/P0
3	1592 MHz	1MB	SUNW,UltraSPARC-IIIfi	3.4	on-line	MB/C3/P0

 NOTE

Hardware configurations for a workstation vary according to the workstation model.

----End

A.3.4.3 How to Check Whether the Hard Disk of the Sun Workstation Is Damaged

Question

How do I check whether the hard disk of the Sun workstation is damaged?

Answer

- 1 During the operation of the Sun workstation, inappropriate powering-off usually causes damage to the hard disk and even renders the Sybase database unavailable. Run the **iostat -E** command to check whether the hard disk of the OS is damaged.

Log in to the Sun workstation as user **root** and run the following command:

```
# iostat -En
```

A message similar to the following will be displayed:

```
c0t0d0      Soft Errors: 0 Hard Errors: 0 Transport Errors: 0
Vendor: FUJITSU Product: MAY2073RCSUN72G Revision: 0501 Serial No: 0742S0EPT7
Size: 73.40GB <73400057856 bytes>
Media Error: 0 Device Not Ready: 0 No Device: 0 Recoverable: 0
Illegal Request: 0 Predictive Failure Analysis: 0
c0t1d0      Soft Errors: 0 Hard Errors: 0 Transport Errors: 0
Vendor: FUJITSU Product: MAY2073RCSUN72G Revision: 0501 Serial No: 0742S0EPL9
Size: 73.40GB <73400057856 bytes>
Media Error: 0 Device Not Ready: 0 No Device: 0 Recoverable: 0
Illegal Request: 0 Predictive Failure Analysis: 0
c0t2d0      Soft Errors: 0 Hard Errors: 0 Transport Errors: 0
Vendor: FUJITSU Product: MBB2073RCSUN72G Revision: 0505 Serial No: 0805A011C0
Size: 73.40GB <73400057856 bytes>
Media Error: 0 Device Not Ready: 0 No Device: 0 Recoverable: 0
Illegal Request: 0 Predictive Failure Analysis: 0
c0t3d0      Soft Errors: 0 Hard Errors: 0 Transport Errors: 0
Vendor: FUJITSU Product: MBB2073RCSUN72G Revision: 0505 Serial No: 0805A011DH
Size: 73.40GB <73400057856 bytes>
Media Error: 0 Device Not Ready: 0 No Device: 0 Recoverable: 0
Illegal Request: 0 Predictive Failure Analysis: 0
clt0d0      Soft Errors: 1 Hard Errors: 0 Transport Errors: 1
Vendor: TSSTcorp Product: CD/DVDW TS-T632A Revision: SR03 Serial No:
Size: 0.00GB <0 bytes>
Media Error: 0 Device Not Ready: 0 No Device: 0 Recoverable: 0
Illegal Request: 1 Predictive Failure Analysis: 0
c0t3d0      Soft Errors: 0 Hard Errors: 0 Transport Errors: 0
Vendor: FUJITSU Product: MBB2073RCSUN72G Revision: 0505 Serial No: 0805A011DH
Size: 73.40GB <73400057856 bytes>
Media Error: 0 Device Not Ready: 0 No Device: 0 Recoverable: 0
Illegal Request: 0 Predictive Failure Analysis: 0
```

NOTE

The hard disk is damaged if the information to the rights of **Hard Errors** is not **0**. Send the message series files in the **/var/adm** directory to Huawei engineers so that they can apply for a spare part to replace the hard disk on site.

----End

A.3.4.4 How to Check the Partition of Solaris OS

Question

How do I check the partition of Solaris OS?

Answer

- 1 Log in to Solaris OS as user **root**.

2 Run the following command to check all disks of the server:# **format**

The following message will be displayed:

Searching for disks...done

AVAILABLE DISK SELECTIONS:

```

0. c0t0d0 <SUN146G cyl 14087 alt 2 hd 24 sec 848>
   /pci@0,600000/pci@0/pci@8/pci@0/scsi@1/sd@0,0
1. c0t1d0 <SEAGATE-ST914602SSUN146G-0603 cyl 14087 alt 2 hd 24 sec 848>
   /pci@0,600000/pci@0/pci@8/pci@0/scsi@1/sd@1,0
2. clt4d0 <ENGENIO-INF-01-00-0619 cyl 51198 alt 2 hd 128 sec 64>
   /pci@2,600000/SUNW,qlc@0/fp@0,0/ssd@w201600a0b8293a52,0
3. c2t5d0 <ENGENIO-INF-01-00-0619 cyl 51198 alt 2 hd 128 sec 64>
   /pci@2,600000/SUNW,qlc@0,1/fp@0,0/ssd@w202700a0b8293a52,0
Specify disk (enter its number):

```

3 Enter **0** and press **Enter** to view the information about the c1t0d0 disk. The following message will be displayed:

```

selecting c0t0d0
[disk formatted]
/dev/dsk/c0t0d0s1 is in use by dump. Please see dumpadm(1M).

```

FORMAT MENU:

```

disk          - select a disk
type          - select (define) a disk type
partition     - select (define) a partition table
current       - describe the current disk
format        - format and analyze the disk
repair        - repair a defective sector
label         - write label to the disk
analyze       - surface analysis
defect        - defect list management
backup        - search for backup labels
verify        - read and display labels
save          - save new disk/partition definitions
inquiry       - show vendor, product and revision
volname       - set 8-character volume name
!<cmd>        - execute<cmd>, then return
quit
format>

```

4 Enter **p** and press **Enter** to select the partition list. The following message will be displayed:

PARTITION MENU:

```

0 - change `0' partition
1 - change `1' partition
2 - change `2' partition
3 - change `3' partition
4 - change `4' partition
5 - change `5' partition
6 - change `6' partition
7 - change `7' partition
select - select a predefined table
modify - modify a predefined partition table
name    - name the current table
print   - display the current table
label   - write partition map and label to the disk
!<cmd>  - execute<cmd>, then return
quit
partition>

```

5 Enter **p** and press **Enter** to view the partition information of disk c1t0d0, including the raw partition information. The following message will be displayed:


```
Current partition table (original):
Total disk cylinders available: 14087 + 2 (reserved cylinders)

Part      Tag      Flag      Cylinders      Size      Blocks
 0        root      wm         0 - 3091      30.01GB   (3092/0/0)  62928384
 1        swap      wu       3092 - 6389      32.01GB   (3298/0/0)  67120896
 2      backup      wm         0 - 14086     136.71GB   (14087/0/0) 286698624
 3          -        wu         0 - 14086     136.71GB   (14087/0/0) 286698624
 4          -        wu      14083 - 14086      39.75MB   (4/0/0)      81408
 5 unassigned      wm       6390 - 10511     40.00GB   (4122/0/0)  83890944
 6         var      wm     10512 - 13603     30.01GB   (3092/0/0)  62928384
 7 unassigned      wm         0              0         (0/0/0)         0

partition>
```

6 Enter **q** to exit the **clt0d0** disk directory. The following message will be displayed:

```
FORMAT MENU:
disk          - select a disk
type          - select (define) a disk type
partition     - select (define) a partition table
current       - describe the current disk
format        - format and analyze the disk
repair        - repair a defective sector
label         - write label to the disk
analyze       - surface analysis
defect        - defect list management
backup        - search for backup labels
verify        - read and display labels
save          - save new disk/partition definitions
inquiry       - show vendor, product and revision
volname       - set 8-character volume name
!<cmd>        - execute<cmd>, then return
quit
format>
```

7 Enter **q** and exit the **format** command.

8 Repeat Step 2 to Step 7, and select other disks to check the partitions.

----End

A.3.4.5 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.

A.3.4.6 How to Decompress Files

Question

Compressed files are usually in ***.tar**, ***.tar.gz**, or ***.zip** format. How do I decompress these files?

Answer

- 1 To decompress a ***.tar** file, perform the following operation:

The following uses the **abc.tar** file as an example. Run the following command:

```
# tar xvf abc.tar
```

- 2 To decompress a ***.tar.gz** file, perform the following operation:

- The following uses the **abc.tar.gz** file as an example. Run the following commands:

```
# gunzip abc.tar.gz
```

```
# tar xvf abc.tar
```

- The following uses the **solaris10_HuaweiPatch9.0.tar.gz** file as an example. Run the following command:

```
# gzcat solaris10_HuaweiPatch9.0.tar.gz | tar xBpf -
```

- 3 To decompress a ***.zip** file, perform the following operation:

The following uses the **abc.zip** file as an example. Run the following command:

```
# unzip abc.zip
```

----End

A.3.4.7 How to Remotely Log In to the System as User root

Question

Remote login fails after the system is restarted. How do I remotely log in to the system as user **root**?

Answer

- 1 Log in to the server from the controller. Ensure that the server is running.
- 2 Check whether user **root** has rights to log in to the server. Ensure that user **root** has rights to log in to the server by means of FTP.
- 3 Verify the routing information about the server. Ensure that the route is reachable.

----End

A.3.4.8 How to Access the OS from the Controller

Question

How do I access the OS from the controller IP address if login to the OS from the system IP address fails?

Answer

- 1 Log in to the controller.
 - For M4000 servers, log in to the controller in Telnet or SSH mode.

- For T5220 servers, log in to the controller in SSH mode.
- 2 Access the OS.
- For M4000 servers, run the **console -d 0** command to access the OS.
 - For T5220 servers, run the **start /SP/console** command to access the OS.
- End

A.3.4.9 How to Switch Between the Console, OK Prompt, and # Prompt

Question

How do I switch between the console, **OK** prompt, and # prompt?

 NOTE

The switching method varies based on the type of the Sun server used.

Answer

- T5220 Servers
 - Switch from the console to the **OK** prompt.
 1. Log in to the IP address of the system controller in Secure Shell (SSH) mode. Perform the following operations to display the **OK** prompt:

 **NOTE**

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

 - Install the SSH client tool, such as the PuTTY, in the console on Windows. Then, you can log in to the system controller through the tool.
 - Run the **ssh IP address of the system controller** command on the terminal console of another Sun server to log in to the system controller. If a message similar to the following is displayed, enter **yes** to continue:
The authenticity of host '10.71.35.12 (10.71.35.12)' can't be established.
RSA key fingerprint is 0b:23:07:0c:27:72:44:3f:d1:aa:
12:99:ed:dd:c0:5a.
Are you sure you want to continue connecting (yes/no)?
 2. In the command line interface (CLI) that is displayed, enter the user name and password of the system controller. By default, the user name is *root* and the default password is *changeme*.
 3. Enter **set /HOST/bootmode state=reset_nvram script="setenv auto-boot? false"**.

 **NOTE**

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

The following message will be displayed:

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

The following message will be displayed:

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

If the message **start: Target already started** is displayed, the system is running. Perform the following operations:

Enter **stop /SYS**. The following message will be displayed:

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

Enter **y**. The following message will be displayed:

Stopping /SYS

Enter **show /HOST status** repeatedly to check the system status. After a message containing **status = Powered off** is displayed, proceed with the next step.

Enter **start /SYS**. The following message will be displayed:

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

Enter **y** to start the server.

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

The following message will be displayed:

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

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

The following message will be displayed:

Serial console started. To stop, type #.

...

Setting NVRAM parameters to default values.

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

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

- Switch from the **OK** prompt to the **#** prompt.

Run the following command:

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

 NOTE

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

Run the following command to verify that the parameter settings have taken effect:

```
ok printenv
```

Run the following command to enable the system to perform another self-check:

```
ok reset-all
```

The system will display the **OK** prompt. Enter **boot** to display the **#** prompt.

- Switch from the **#** prompt to the console.

Run the following command:

```
# #.
```

 NOTE

Enter **#** and **..**

- Switch from the **#** prompt to the **OK** prompt.

Run the following command:

```
# init 0
```

- M4000 Servers

- Switch from the console to the **OK** prompt.

1. Run the **telnet *IP address of the controller*** command on the console to log in to the controller IP address by means of Telnet.

The following message will be displayed:

Login:

2. Enter the user name, that is, **eis-installer**.

The following message will be displayed:

Password:

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

The following message will be displayed:

XSCF>

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

The following message will be displayed:

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

 NOTE

If **Secure Mode** is **on**, perform the following:

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

The following message will be displayed:

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

2. Enter **y**.

The following message will be displayed:

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

5. Enter **showdomainstatus -a**.

The following message will be displayed:

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

 NOTE

The following message will be displayed:

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

Run the **poweron -d 0** command. Then, run the **showdomainstatus -a** command repeatedly to check the system status until the system displays the status as **running**. Proceed with the next step.

6. Enter **sendbreak -d 0**.
The following message will be displayed:
Send break signal to DomainID 0? [y|n]
 7. Enter **y**.
 8. Enter **console -d 0 -f**.
The following message will be displayed:
Connect to DomainID 0? [y|n]
 9. Enter **y** and press **Enter**.
OK
- Switch from the **OK** prompt to the **#** prompt.
Run the following command:
ok **setenv auto-boot? true**
 **NOTE**
There must be a space between **?** and **true**.
Run the following command to verify that the parameter settings have taken effect:
ok **printenv**
Run the following command to enable the system to perform another self-check:
ok **reset-all**
The system will display the **OK** prompt. Enter **boot** to display the **#** prompt.
 - Switch from the **#** prompt to the console.
Run the following command:
#.
 **NOTE**
Enter **#** and **..**.
 - Switch from the **#** prompt to the **OK** prompt.
Run the following command:
init 0
- V890 Servers
 - Switch from the console to the **OK** prompt.
 1. Run the **telnet IP address of the controller** command on the console to log in to the controller IP address by means of Telnet.
The following message will be displayed:
Login:
 2. Enter the user name **admin** and password. Generally, the default password of the RSC is **admin123**.
 3. Enter **console** to display the **OK** prompt.

 NOTE

In certain conditions, the following message will be displayed:

```
Warning: User < > currently has write permission to this console
and
forcibly removing them will terminate any current write actions
and all work will be lost.
Would you like to continue? [y/n]
```

Enter **y**.

If the V890 server is used for the first time, the system will display the **OK** prompt.

If the V890 server is installed with the operating system (OS), the system will display the **#** prompt. Perform the following operations to display the **OK** prompt:

Enter **~**. to display the **RSC** prompt. (If the ALOM control card is used, enter **#.**)

Run the following command at the **RSC** prompt:

```
rsc> break
```

The following message will be displayed:

```
Are you sure you want to send a break to the system [y/n]?
```

Enter **y**.

```
rsc> console
```

- Switch from the **OK** prompt to the **#** prompt.

Run the following command:

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

 NOTE

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

Run the following command to verify that the parameter settings have taken effect:

```
ok printenv
```

Run the following command to enable the system to perform another self-check:

```
ok reset-all
```

The system will display the **OK** prompt. Enter **boot** to display the **#** prompt.

- Switch from the **#** prompt to the console.

Run the following command:

```
# #.
```

 NOTE

Enter **#** and **..**

- Switch from the **#** prompt to the **OK** prompt.

Run the following command:

```
# init 0
```

- V240, V245, V440, and V445 Servers

- Switch from the console to the **OK** prompt.

1. Run the **telnet IP address of the controller** command on the console to log in to the controller IP address by means of Telnet.

The following message will be displayed:

Login:

2. Enter the user name and password. The default user name and password are **admin**.

3. Enter **console -f** to display the **OK** prompt.

 NOTE

In certain conditions, the following message will be displayed:

```
Warning: User < > currently has write permission to this console
and
forcibly removing them will terminate any current write actions
and all work will be lost.
Would you like to continue? [y/n]
```

Enter **y**.

If the intended server is used for the first time, the system will display the **OK** prompt.

If the server is installed with the OS, the system will display the **#** prompt. Perform the following operations to display the **OK** prompt:

Enter **#**. to display the ALOM prompt. (If the RSC control card is used, enter **~.**)

Run the following command at the ALOM prompt:

```
sc> break
```

The following message will be displayed:

```
Are you sure you want to send a break to the system [y/n]?
```

Enter **y**.

```
sc> console -f
```

- Switch from the **OK** prompt to the **#** prompt.

Run the following command:

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

 NOTE

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

Run the following command to verify that the parameter settings have taken effect:

```
ok printenv
```

Run the following command to enable the system to perform another self-check:

```
ok reset-all
```

The system will display the **OK** prompt. Enter **boot** to display the **#** prompt.

- Switch from the **#** prompt to the console.

Run the following command:

```
# #.
```

 NOTE

Enter **#** and **..**

- Switch from the **#** prompt to the **OK** prompt.

Run the following command:

```
# init 0
```

----End

A.3.4.10 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 A-2](#).

Table A-2 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.

A.3.4.11 How to Use the Text Editor

Question

How do I use the text editor?



NOTE

Use the text editor only through the GUI.

The text editor is recommended because it is easier to use than the vi editor.

Answer

Run the following command to open the text editor:

dtppad *file name*

- If a file with the same filename exists, run the **dtppad** command to open and edit the file.
- If a file with the same filename does not exist, run the **dtppad** command to create and edit a file.

A.3.4.12 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.

A.3.4.13 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.

A.3.4.14 How to Deploy a Solaris Single-Server System If Data Is Stored on Some Hard Disks

Question

A server is equipped with four hard disks, two of which are in use. How to deploy a Solaris single-server system without impacting data on the two hard disks?

Answer

- 1 Remove the two hard disks from the server.
- 2 Use the other two hard disks for U2000 installation and quick system installation.
For details, see the *iManager U2000 Single-Server System Software Installation Guide (Solaris)*.

- 3 Insert the removed hard disks into the server.

If the two hard disks are mounted but the **vfstab** file is not modified, data on the two hard disks can be viewed and used only this time. After the server is restarted, data on the two hard disks cannot be viewed.

- 4 To ensure proper use, mount the two hard disks.

Run the following commands:

```
# mkdir data1  
# mkdir data2  
# mount -F ufs /dev/dsk/c1t2d0s7 /data1  
# mount -F ufs /dev/dsk/c1t3d0s7 /data2
```

- 5 Modify the **vfstab** file to ensure that data on the two hard disks can still be viewed after the server is restarted.

Run the following command:

```
# vi /etc/vfstab
```

Add the following two lines of information to the **vfstab** file:

```
/dev/dsk/clt2d0s7    /dev/rdisk/clt2d0s7    /data1    ufs    2    yes    - /dev/dsk/  
clt3d0s7    /dev/rdisk/clt3d0s7    /data2    ufs    2    yes    -
```

Press **ESC**. Then, press **Shift+;**, enter **wq!**, and press **Enter**.

----End

A.4 Veritas HA System

This topic covers FAQs about the Veritas HA system.

[A.4.1 License Management](#)

This topic describes the FAQs about license management.

[A.4.2 Disk Maintenance](#)

This topic describes the FAQs about disk maintenance.

[A.4.3 System Settings](#)

This topic describes the FAQs about the system settings in the HA system.

A.4.1 License Management

This topic describes the FAQs about license management.

[A.4.1.1 How to Check the Veritas License](#)

[A.4.1.2 How to Update the Veritas License \(Windows\)](#)

A.4.1.1 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-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-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-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

A.4.1.2 How to Update the Veritas License (Windows)

Question

How do I update the Veritas license?

Answer

- 1 Back up all the license files in the **C:\Program Files\Common Files\Veritas Shared\vrtslic\lic** directory.
- 2 In **Control Panel**, click **Add or Remove Programs**. In the **Add or Remove Programs** dialog box, select the Veritas Storage Foundation HA 5.1 for Windows (Server Components) program, and then click **Change**.
- 3 In the dialog box that is displayed, click the **License Management** option button, and then click **Next**.
- 4 Enter the license that is newly applied for, that is, VRTS STORAGE FOUNDATION STANDARD. Then, click **Update**. Click **Finish**.

**NOTE**

- The information about the demo or formal license that is newly applied for is contained in the license file.
 - The licenses that are newly applied for include VRTS STORAGE FOUNDATION STANDARD, VRTS VOLUME REPLICATOR OPTION, and VRTS CLUSTER SERVER HA/DR.
- 5 Repeat the preceding steps, enter the license keys of VRTS VOLUME REPLICATOR OPTION and VRTS CLUSTER SERVER HA/DR.
 - 6 Run the following command to check whether the updated license takes effect:

```
C:\> vxlicrep
```

Check whether the license key of the related component is updated and whether the authentication date of the component is correct.
 - 7 Restart the OS.

----End

A.4.2 Disk Maintenance

This topic describes the FAQs about disk maintenance.

[A.4.2.1 How to Query the Disk Status](#)

[A.4.2.2 How to Query the Status of the Disk Group](#)

[A.4.2.3 How to Query the Status of the Disk Volume \(Solaris & SUSE Linux\)](#)

A.4.2.1 How to Query the Disk Status

Question

How do I query the disk status during the maintenance of the HA system?

Answer

- 1 Run the following command to view the disk status:

vxdisk list

Assume there are two disks. The following message will be displayed on Solaris or SUSE Linux OS:

DEVICE	TYPE	DISK	GROUP	STATUS
clt0d0s2	auto:sliced	disk01	datadg	online
clt1d0s2	auto:sliced	disk02	datadg	online

The following message after mirroring will be displayed on the Windows OS:

Name	MediaName	Diskgroup	DiskStyle	Size (MB)	FreeSpace (MB)
) Status	EnclosureID	P#C#T#L#			
Harddisk0		BasicGroup	MBR	139894	7
Uninitialized	DISKS@u2000	P3C4T0L0			
Harddisk1	Disk1	datadg	MBR	139894	85621
Imported	DISKS@u2000	P3C4T1L0			

- 2 In the Solaris or SUSE Linux OS, check whether the disk status is online. In the Windows OS, check whether the disk status is imported. If not, the disk status is abnormal.

----End

A.4.2.2 How to Query the Status of the Disk Group

Question

How do I query the status of the disk group during the maintenance of the HA system?

Answer

- 1 Run the following command to view the status of the disk group:

vx dg list

A message similar to the following will be displayed on Solaris or SUSE Linux OS:

NAME	STATE	ID
rootdg	enabled	1159119913.12.T5220227183
datadg	enabled	1159119543.10.T5220227183

A message similar to the following will be displayed on Windows OS:

Disk groups are....

Name	:	BasicGroup
Disk Group Type	:	Basic
DiskGroup ID	:	No ID
Status	:	Imported
Name	:	datadg

```

Disk Group Type      : Dynamic (Cluster)
DiskGroup ID         : 5a997293-1286-43e4-83d3-dbbc6bd1d30d
Status               : Imported

```

- 2 On Solaris or SUSE Linux OS, check whether the status of the disk group is enabled. On Windows OS, check whether the status of the disk group is imported. If not, the disk group is abnormal.

On Solaris or SUSE Linux OS, in normal cases, a disk group such as the proceeding one **rootdg** must exist. Otherwise, the disk group is partitioned incorrectly.

----End

A.4.2.3 How to Query the Status of the Disk Volume (Solaris & SUSE Linux)

Question

How do I query the status of the disk volume during the maintenance of the HA system?

Answer

- 1 Run the following command to view the status of the disk volume:

```
# vxprint -l VolumeName
```

For example, run the following command to view the status of the disk volume:

```
# vxprint -l lv_nms_data
```

A message similar to the following will be displayed:

```

Disk group: datadg

Volume:   lv_nms_data
info:     len=62914560
type:     usetype=fsgen
state:    state=ACTIVE kernel=ENABLED cdsrecovery=0/0 (clean)
assoc:    plexes=lv_nms_data-01,lv_nms_data-02,lv_nms_data-03,lv_nms_data-04
          exports=(none)
policies: read=SELECT (round-robin) exceptions=GEN_DET_SPARSE
flags:    closed writecopy writeback
logging:  type=DCM loglen=512 serial=0/0 mapalign=256 (enabled)
apprecov: seqno=0/0
recovery: mode=default
recov_id=0
device:   minor=10002 bdev=309/10002 cdev=309/10002 path=/dev/vx/dsk/datadg/lv_d
          ata
perms:    user=root group=root mode=0666
guid:     {0a1c434c-1dd2-11b2-98fc-392ab8f54da0}

```

In the command, **VolumeName** indicates the name of the disk volume. The name of the current disk volume can be obtained through the **vxprint -v** command.

Table A-3 describes all fields about the status of the disk volume.

Table A-3 Fields about the disk volume status

Field	Description
Disk group	Indicates the disk group to which the disk volume belongs.

Field	Description
Volume	Indicates the name of a disk volume.
Info	Indicates the length of the disk volume.
type	Indicates the type of the disk volume.
state	Indicates the status of the disk volume. In normal cases, the situations are as follows: ● state is ACTIVE. ● kernel is ENABLED.
assoc	Indicates the association relationship of the disk volume. ● rvg indicates the RVG of the disk volume. ● plexes indicates the plexes contained by the disk volume.
policies	Indicates the management policy of the disk volume.
flags	Indicates the flag of the disk volume.
logging	Indicates the log of the disk volume. In normal cases, type is DCM.
apprecov	Indicates the verification parameter of the disk volume.
recovery	Indicates the recovery mode of the disk volume.
device	Indicates the device ID and path of the disk volume.
perms	Indicates the owner and right of the disk volume.
guid	Indicates the sequence of stored data.

----End

A.4.3 System Settings

This topic describes the FAQs about the system settings in the HA system.

[A.4.3.1 What Are the Reasons for Automatic Switching](#)

[A.4.3.2 How to Log in and Exit the VCS \(Veritas Cluster Server\)](#)

[A.4.3.3 How to Query the RVG Status \(Solaris & SUSE Linux\)](#)

[A.4.3.4 How to Query the RVG Status \(Windows\)](#)

[A.4.3.5 How to Query the Rlink Status \(Solaris & SUSE Linux\)](#)

[A.4.3.6 How to Query the Rlink Status \(Windows\)](#)

[A.4.3.7 How to Query the VVR Status \(Solaris & SUSE Linux\)](#)

[A.4.3.8 How to Query the VVR Status \(Windows\)](#)

[A.4.3.9 How to Manually Start the VCS Service \(Solaris & SUSE Linux\)](#)

[A.4.3.10 How to Manually Start the VCS Service \(Windows\)](#)

[A.4.3.11 How to Manually Start the VVR \(Solaris & SUSE Linux\)](#)

[A.4.3.12 How to Manually Stop the VCS Service \(Solaris & SUSE Linux\)](#)

[A.4.3.13 How to Manually Stop the VCS Service \(Windows\)](#)

[A.4.3.14 How to Solve the Problem That the VMDg Node Icon Becomes Grayed out After the High Availability System Is Established \(Windows HA System\)](#)

[A.4.3.15 How to Solve the Problem Where the Communications between the Primary Site and the Secondary Site Are Interrupted After the HA System Is Set Up](#)

[A.4.3.16 How to Rectify the Fault that Certain Menu Items on the VCS Client Are Dimmed](#)

[A.4.3.17 How to Start/Stop the NMS Before Synchronizing the Primary and Secondary Sites](#)

[A.4.3.18 How to Ensure Proper Connection of VVR Ports on Primary and Secondary Sites](#)

[A.4.3.19 How to Ensure Proper File Transfer Between Primary and Secondary Sites](#)

A.4.3.1 What Are the Reasons for Automatic Switching

Question

What are the reasons for automatic switching?

Answer

- 1 The Veritas HA system can implement the automatic switching function. Generally, the automatic switching can be triggered by the following reasons:
 - A certain process with the automatic monitoring mode is faulty and the U2000 System Monitor restarts the process for more than three times. When a certain process of the U2000 is faulty, the U2000 System Monitor restarts the process automatically. If the process fails to be restarted for three times, the VCS determines that the process fails to be started. In this case, the switching of the primary and secondary sites occurs.
 - In the case of the distributed system, the slave server that is in the monitored state and is deployed with instances fails to be connected.
 - The software or hardware of the master server in the active site is faulty.

- 2 When the automatic switching is performed, the following may occur on the client:

The connection to the server is broken. In this case, connect the master server in the secondary site manually.

When the primary site restores to the normal state, on the secondary site, synchronize the data between the primary and secondary sites.

----End

A.4.3.2 How to Log in and Exit the VCS (Veritas Cluster Server)

Question

How do I log in to and exit the VCS?

Answer

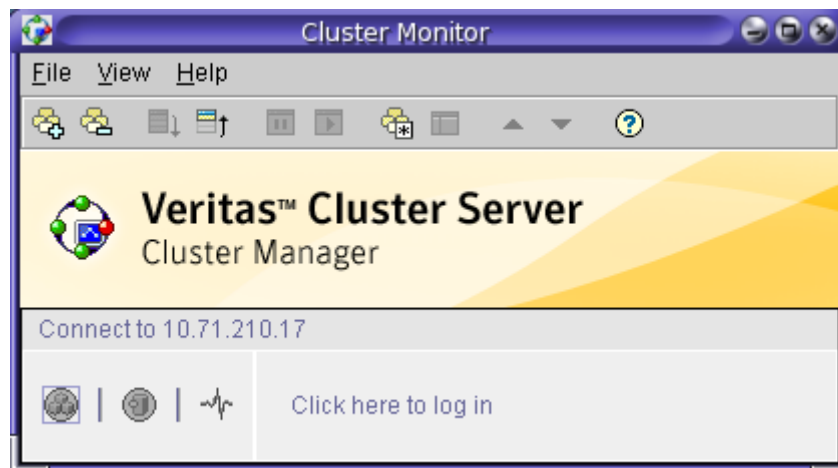
1 Log in to the VCS.

1. Open the Cluster monitor.

In Windows OS, choose **Start > Programs > Symantec > Veritas Cluster Server > Veritas Cluster Manager - Java Console**.

In Solaris or SUSE Linux OS, perform the following operations:

- a. Log in to the OS as user **root**.
- b. Open a terminal window and run the following command:
`# haguic`



 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.

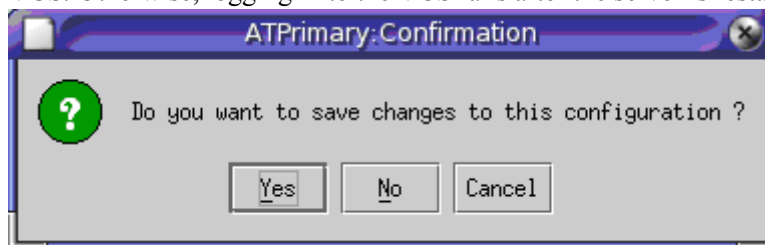
4. Click **OK**.

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

A.4.3.3 How to Query the RVG Status (Solaris & SUSE Linux)

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 A-4 describes the RVG status of the primary site.

Table A-4 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.

Field	Description
info	Indicates the information about the RVG.
state	Indicates the status of the RVG. In normal cases, the situations are as follows: ● state is set to ACTIVE. ● kernel is set to ENABLED.
assoc	Indicates the association information about the RVG. ● datavols indicates the data disk volume that the RVG contains. ● srl indicates the SRLog disk volume that the RVG contains. ● rlinks indicates the RLink that the RVG contains.
att	Indicates the activated Rlink of the RVG.
flags	Indicates the flag of the RVG. In normal cases, the value is closed primary enabled attached .
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 -VI
```

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 A-4](#). Normally, **flags** on the secondary site is **closed secondary enabled attached**.

----End

A.4.3.4 How to Query the RVG Status (Windows)

Question

How do I query the RVG status?

Answer

- 1 Run the following command to view the RVG status of the primary site:

vxprint -Vl

The following message will be displayed:

```

Diskgroup = BasicGroup

Diskgroup = datadg

Rvg      : datarvg
state    : state=ACTIVE kernel=ENABLED
assoc    : datavols=S:
           srl=\Device\HarddiskDmVolumes\datadg\srl
           rlinks=datarlk
att      : rlinks=datarlk
checkpoint :
flags    : primary enabled attached clustered

```

Table A-5 describes the RVG status of the primary site.

Table A-5 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.
state	Indicates the status of the RVG. In normal cases, the situations are as follows: ● state is set to ACTIVE. ● kernel is set to ENABLED.
assoc	Indicates the association information about the RVG. ● datavols indicates the data disk volume that the RVG contains. ● srl indicates the SRLog disk volume that the RVG contains. ● rlinks indicates the Rlink that the RVG contains.
att	Indicates the activated Rlink of the RVG.
flags	Indicates the flag of the RVG. In normal cases, the value is primary enabled attached clustered .

- 2 Run the following command to view the RVG status on the secondary site:

vxprint -Vl

The following message will be displayed:

```

Diskgroup = BasicGroup

Diskgroup = datadg

Rvg      : datarvg
state    : state=ACTIVE kernel=ENABLED
assoc    : datavols=\Device\HarddiskDmVolumes\datadg\lvdata
           srl=\Device\HarddiskDmVolumes\datadg\srl
           rlinks=datarlk

```



```
att      : rlinks=datarlk
checkpoint :
flags    : secondary enabled attached clustered
```

For the description of the RVG status at the secondary site, see [Table A-5](#). Normally, **flags** on the secondary site is **secondary enabled attached clustered**.

----End

A.4.3.5 How to Query the Rlink Status (Solaris & SUSE Linux)

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 <mlinkName>
```

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 A-6](#) describes the Rlink status on the primary site.

Table A-6 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. ● timeout indicates the timeout period. ● rid indicates the ID of the Rlink. ● latency_high_mark indicates the highest delay flag. ● latency_low_mark indicates the lowest delay flag. ● bandwidth_limit indicates the bandwidth limit.	
state	Indicates the status of the Rlink. In normal cases, the situations are as follows: ● state is set to ACTIVE. ● synchronous is set to off. ● latencyprot is set to off. ● srlprot is set to autodem.	
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 A-6](#).

----End

A.4.3.6 How to Query the Rlink Status (Windows)

Question

How do I query the Rlink status?

Answer

- 1 Run the following command at the primary site to query the Rlink status:

vxprint -PI <rlinkName>

For example, run the following command to query the status of **datarlk**:

vxprint -PI datarlk

A message similar to the following will be displayed:

```
Diskgroup = datadg

Rlink      : datarlk
info       : timeout=500 connections=15
            latency_high_mark=10000 latency_low_mark=9950
            bandwidth_limit=none
state      : state=ACTIVE
            synchronous=override latencyprot=off srlprot=autodcm
assoc      : rvg=datarvg
            remote_host=10.71.224.43
            remote_dg=datadg
            remote_rlink=datarlk
            local_host=10.71.224.44
protocol   : TCP/IP
flags      : write attached consistent connected
```

[Table A-7](#) describes the Rlink status on the primary site.

Table A-7 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. ● timeout indicates the timeout period. ● latency_high_mark indicates the highest delay flag. ● latency_low_mark indicates the lowest delay flag. ● bandwidth_limit indicates the bandwidth limit.	
state	Indicates the status of the Rlink. In normal cases, the situations are as follows: ● state is set to ACTIVE. ● synchronous is set to override. ● latencyprot is set to off. ● srlprot is set to autodcm.	
assoc	rvg	Indicates the RVG where the Rlink is located.
	remote_host	Indicates the IP address of the remote host.
	remote_dg	Indicates the remote disk group.
	remote_rlink	Indicates the Rlink name of the remote host.
	local host	Indicates the IP address of the local host.
protocol	Indicates the protocol for synchronizing data.	
flags	Indicates the flag of the Rlink. Normally, the value is write attached consistent connected .	

2 Run the following command on the standby site to query the Rlink status:

vxprint -PI <rlinkName>

For example, run the following command to query the **datarlk** status:

vxprint -PI datarlk

A message similar to the following will be displayed:

```

Diskgroup = datadg

Rlink      : datarlk
info       : timeout=500 connections=15
            latency_high_mark=10000 latency_low_mark=9950
            bandwidth_limit=none
state      : state=ACTIVE
            synchronous=override latencyprot=off srlprot=autodcm
assoc      : rvg=datarvg
            remote_host=10.71.224.44
            remote_dg=datadg
            remote_rlink=datarlk
            local_host=10.71.224.43
protocol   : TCP/IP
flags      : write attached consistent connected

```

For the description of the Rlink status on the secondary site, see [Table A-7](#).

----End

A.4.3.7 How to Query the VVR Status (Solaris & SUSE Linux)

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

A.4.3.8 How to Query the VVR Status (Windows)

Question

How do I query the VVR status when maintaining 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 : RDS
Primary :
    Hostname : 10.71.224.44 <localhost>
    RvgName  : datarvg
    DgName   : datadg
Secondary :
    Hostname : 10.71.224.43
    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:

```
Diskgroup = datadg

Rvg      : datarvg
state    : state=ACTIVE kernel=ENABLED
assoc    : datavols=S:
           srl=\Device\HarddiskDmVolumes\datadg\srl
           rlinks=datarlk
att      : rlinks=datarlk
checkpoint :
flags    : primary enabled attached clustered

Rlink    : datarlk
info     : timeout=500 connections=15
           latency_high_mark=10000 latency_low_mark=9950
           bandwidth_limit=none
state    : state=ACTIVE
           synchronous=override latencyprot=off srlprot=autodcm
assoc    : rvg=datarvg
           remote_host=10.71.224.43
           remote_dg=datadg
           remote_rlink=datarlk
           local_host=10.71.224.44
protocol : TCP/IP
flags    : write attached consistent connected
```

In the preceding information, 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 # **vx dg list** command to query the status of the disk group.
- Run the # **vxprint -l datarvg** command to query the RVG status.
- Run the # **vxprint -l datarlk** command to query the Rlink status.
- Run the # **vxlink -g datadg status datarlk** command on the primary site to query the replication cache status.

Save the response to the preceding commands.

----End

A.4.3.9 How to Manually Start the VCS Service (Solaris & SUSE Linux)

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:

```
# hstart -onenode
```

----End

A.4.3.10 How to Manually Start the VCS Service (Windows)

Question

How do I manually start the VCS service (Windows)?

Answer

- 1 Run the following command to start the VCS process:

```
C : \> hstart
```

----End

A.4.3.11 How to Manually Start the VVR (Solaris & SUSE Linux)

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
```

A.4.3.12 How to Manually Stop the VCS Service (Solaris & SUSE Linux)

Question

How do I manually stop the VCS service (Solaris & SUSE Linux)?

Answer

- 1 Log in to the OS as user **root**.
- 2 Run the following command to stop the VCS service:

```
# hstop -all -force
```


----End

A.4.3.13 How to Manually Stop the VCS Service (Windows)

Question

How do I manually stop the VCS service (Windows)?

Answer

- 1 Run the following command to stop the VCS service:

```
C:\> hstop -all -force
```


----End

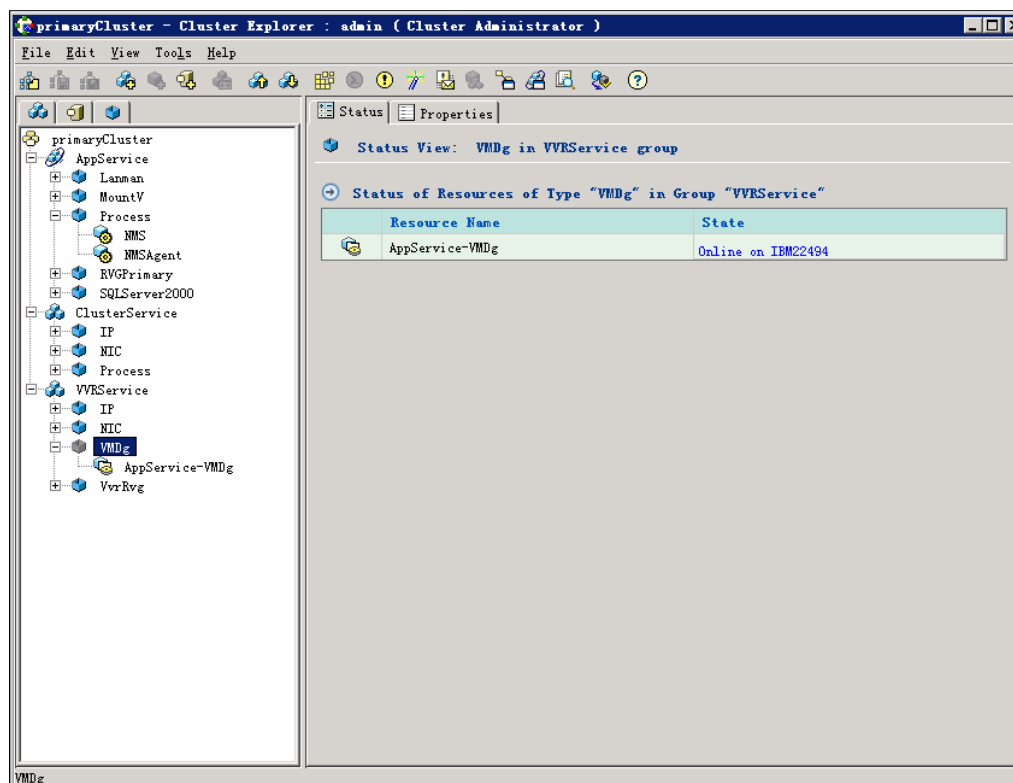
A.4.3.14 How to Solve the Problem That the VMDg Node Icon Becomes Grayed out After the High Availability System Is Established (Windows HA System)

Question

How do I solve the problem that the VMDg node icon becomes grayed out after the high availability system is established (Windows-Veritas)?

Answer

- 1 After establishing the high availability system, log in to the VCS client and view the grayed-out state of the VMDg node icon, as shown in the following figure:



This is the problem of abnormal icon display, but functions are not affected.

----End

A.4.3.15 How to Solve the Problem Where the Communications between the Primary Site and the Secondary Site Are Interrupted After the HA System Is Set Up

Question

After the HA system is set up, the communications between the primary site and secondary site are interrupted. As a result, the active/standby switchover occurs and the replication status between the primary site and the secondary site is abnormal. How do I restore the normal HA system relationship?

Answer

- 1 Check the connection status of the network port or network cables of the primary site. Then, restore the normal communications at the primary site.
- 2 Log in to the VCS client of the primary site. The client displays that the **AppService** resource group is offline. In addition, the client displays errors of the **ClusterService** resource group and **VVRService** resource group.

- 3 Right-click the **ClusterService** resource group and **VVRService** resource group, and then choose **Clear Fault > primaryCluster** from the shortcut menu to clear the errors of the resource groups.
- 4 Right-click the **ClusterService** resource group and **VVRService** resource group respectively, and then choose **Online > Host Name** from the shortcut menu to make the resource groups online.
- 5 At the secondary site, log in to the client of the network management system maintenance suite, and then choose **Deploy > Fore local site be primary**.
- 6 Click **OK**. The normal HA system relationship is restored. All NMS applications are running at the secondary site.

----End

A.4.3.16 How to Rectify the Fault that Certain Menu Items on the VCS Client Are Dimmed

Question

Certain menu items on the VCS client are dimmed. For example, **Switch To > Remote switch**. How do I rectify this fault?

Answer

- 1 Log out of the VCS client.
- 2 Log in to the VCS client again.
- 3 Choose associated menu items on the VCS client.

----End

A.4.3.17 How to Start/Stop the NMS Before Synchronizing the Primary and Secondary Sites

Question

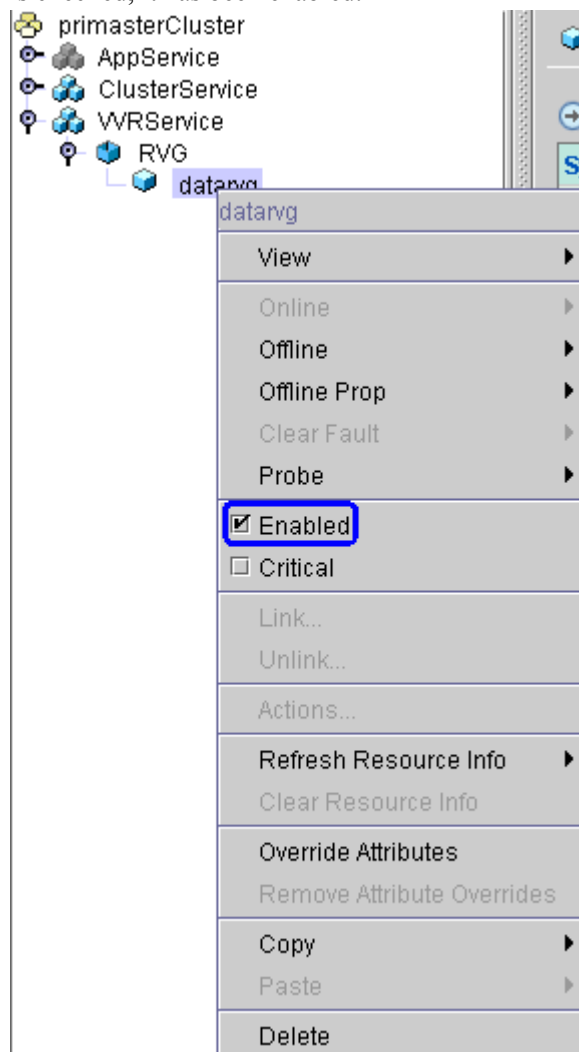
How to start/stop the NMS before synchronizing the primary and secondary sites of a high availability system?

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.

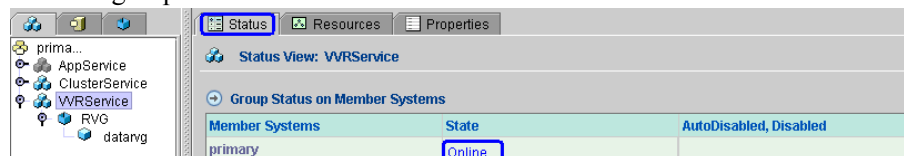
Right-click the datarvg resource and check whether the **Enabled** option is selected. If this option is checked, it has been enabled.



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.



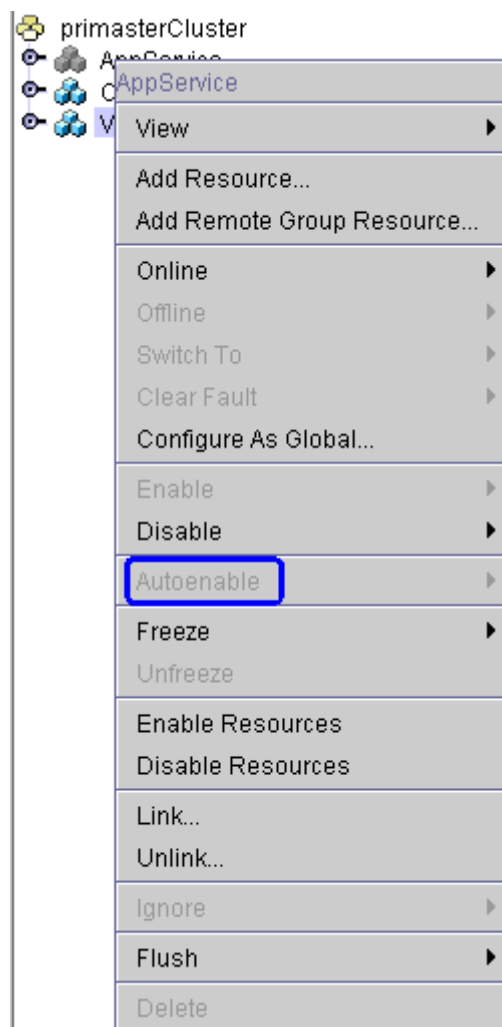
If the VVRService resource group has not been started, do as follows to start it:

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

A.4.3.18 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

A.4.3.19 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

A.5 SQL Server Database

This topic describes the FAQs about the SQL server database.

[A.5.1 How to Change the sa Password of the SQL Server](#)

[A.5.2 How to Expand the master Database](#)

[A.5.3 How to Shut Down the SQL Server Database](#)

[A.5.4 How to Start the SQL Server Database](#)

[A.5.5 How to Solve the Problem That the Password of User sa Is Forgotten](#)

[A.5.6 How to Check Whether the SQL Server Database Can Be Sorted in Binary Mode](#)

[A.5.7 How to Change the Database Sorting Mode to Binary](#)

[A.5.8 How to Check the Name of the SQL Server Database](#)

A.5.1 How to Change the sa Password of the SQL Server

Question

How to change the **sa** password if you forget to set the password during the installation or if you want to change the password?

Answer

- 1 Log in to the NMS maintenance tool client.

1. On the computer where the MSuite client is installed, double-click the **U2000 MSuite** shortcut icon on the desktop. Wait about one minute. The **Login** dialog box is displayed.
 2. Set the related login parameters and click **OK**. The **NMS maintenance suite** window is displayed.
 - IP Address: Indicates the system IP address of the computer where the MSuite server is installed.
 - Port No.: The default port number is **12212**. You do not need to change the default value during login.
 - User Name and Password: Both the default user name and default password are **admin**.
 - 2 On the MSuite client, choose **Deploy > Change Database Administrator Password**. The **Change Database Administrator Password** dialog box is displayed.
 - 3 Enter the old password and new password.
-  **NOTE**
must consist of 6 to 30 characters that can be letters, digits, and underscores (_).
- 4 Click **OK**. The password is changed.

----End

A.5.2 How to Expand the master Database

Question

How to expand the **master** database?

Answer

- 1 In the Enterprise Manager of the SQL server, select the **master** database, right-click, and then choose **Properties**.
- 2 In the dialog box that is displayed, click the **Data Files** tab, modify the database size in the **Space allocated(MB)** area, and then select the **Unrestricted file growth** option button.
- 3 Click the **Transaction Log** tab, modify the database size in the **Space allocated(MB)** area, and then select the **Unrestricted file growth** option button.
- 4 Check whether the modified database size is proper, and click **OK**.
- 5 Restart the database.

----End

A.5.3 How to Shut Down the SQL Server Database

Question

How do I shut down the SQL server database?

 **NOTE**

In normal cases, the SQL server database of the primary site are started but those of the secondary site are not started.

Answer

- 1 In the single-server system, choose **Start > Programs > Microsoft SQL Server > Service Manager**.

The **SQL Server Service Manager** dialog box is displayed.

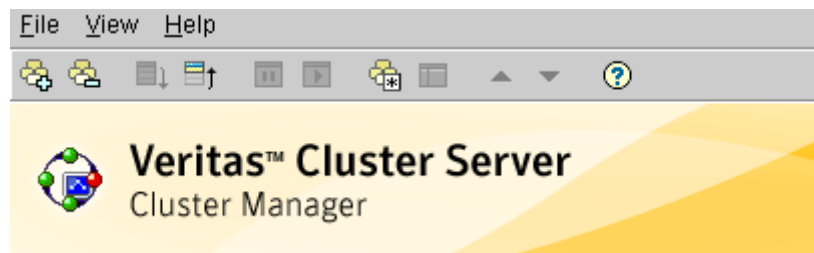
- 2 Click **Stop**.

- 3 Click **Yes**.

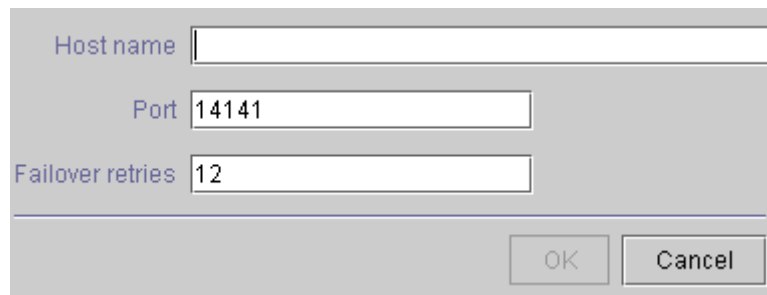
- 4 In the high availability system, log in to the OS as the user who has administrator rights.

- 5 Start the VCS client.

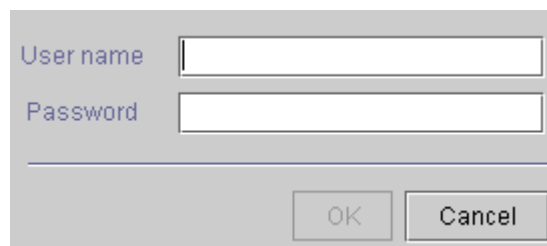
1. Choose **Start > Programs > Symantec > Veritas Cluster Server > Veritas Cluster Manager - Java Console** to start the VCS client.



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



3. Enter the IP address of the system of the primary site. Then, click **OK**.



4. Enter the default user name **admin** and the default password **password** of the VCS client. Then, click **OK**.

- 6 Choose **AppService** from the navigation tree and click the **Resources** tab. Then, right-click **NMSServer** and choose **Offline > host_name** from the shortcut menu. In the dialog box that is displayed, click **Yes**.

- 7 After the **NMSServer** resource is stopped, right-click **AppService-SQLServer2000** and choose **Offline > host_name** from the shortcut menu. In the dialog box that is displayed, click **Yes**.

----End

A.5.4 How to Start the SQL Server Database

Question

How do I start the SQL server database?

NOTE

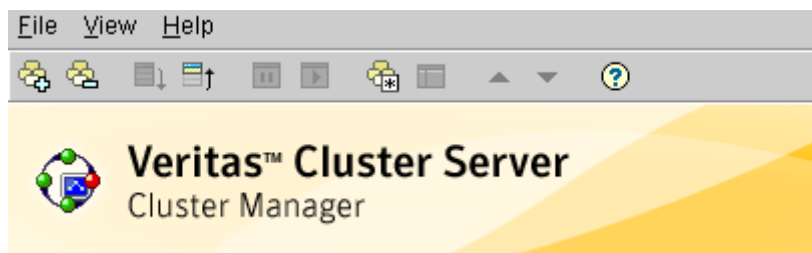
In normal cases, the SQL server database of the primary site are started but those of the secondary site are not started.

Answer

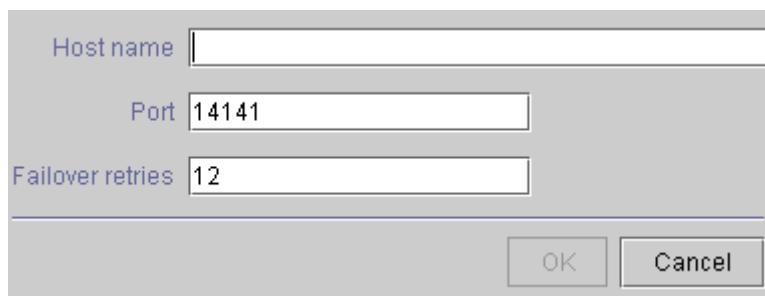
- 1 In the single-server system, choose **Start > Programs > Microsoft SQL Server > Service Manager**.

The **SQL Server Service Manager** dialog box is displayed.

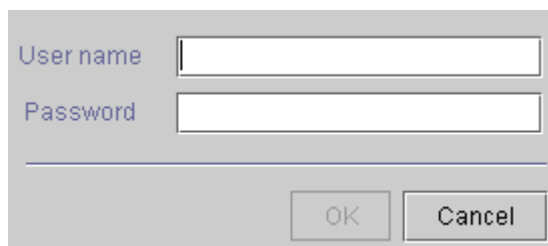
- 2 Click **Start/Continue**.
- 3 In the high availability system, log in to the OS as the user who has administrator rights.
- 4 Start the VCS client.
 1. Choose **Start > Programs > Symantec > Veritas Cluster Server > Veritas Cluster Manager - Java Console** to start the VCS client.



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



3. Enter the IP address of the system of the primary site. Then, click **OK**.



4. Enter the default user name **admin** and the default password **password** of the VCS client. Then, click **OK**.

- 5 Choose **AppService** from the navigation tree and click the **Resources** tab. Then, right-click **AppService-SQLServer2000** and choose **Online** > *host_name* from the shortcut menu. In the dialog box that is displayed, click **Yes**.

----End

A.5.5 How to Solve the Problem That the Password of User sa Is Forgotten

Question

How do I solve the problem that the password of user **sa** of the SQL server database is forgotten?



NOTE

This method is applicable to scenarios where the NMS is not installed. If the NMS is installed and you forget the password of user **sa**, contact Huawei technical support engineers.

Answer

- 1 Choose **start** > **All Programs** > **Microsoft SQL Server** > **Enterprise Manager**.
- 2 In the **SQL Server Enterprise Manager** window, expand **Microsoft SQL Servers** > **SQL Server Group** in **Console Root** on the left, and choose **Security** on a server.
- 3 Click **Login**. Double-click the **sa** item in the right pane, and set the password in the **SQL Server Login Properties-sa** dialog box.

----End

A.5.6 How to Check Whether the SQL Server Database Can Be Sorted in Binary Mode

Question

When you install the SQL Server database, you need to select the binary mode as the sorting mode. How do I check whether the SQL Server database can be sorted in binary mode?

Answer

- 1 Run the following commands at the command prompt:

```
C:\> isql -Usa -Psa password -Sdatabase name
1> sp_helpsort
2> go
```

If the displayed information includes *binary sort*, the database is sorted in binary mode. If the displayed information does not include *binary sort*, the database is not sorted in binary mode.

----End

A.5.7 How to Change the Database Sorting Mode to Binary

Question

How to change the database sorting mode to binary?



NOTE

This operation is applicable to SQL Server 2000 SP4.

Answer

- 1 Choose **Start > Run**. Then, enter **cmd** to open a CLI.
- 2 To change the database sorting mode to binary, run the following commands:

```
C:\> cd C:\HWENGR\engineering\tool\ModifySort
```

```
C:\HWENGR\engineering\tool\ModifySort> ModifySort.bat database name sasa  
password
```

If information similar to the following is displayed, the database sorting mode is changed to binary.

```
Starting deal database sort,please wait.....  
End deal database sort  
Starting deal table sort,please wait.....  
deal DB-Library:'s Tables  
All Finish
```

----End

A.5.8 How to Check the Name of the SQL Server Database

Question

How to check the name of the SQL Server database?

Answer

- 1 Choose **Start > All Programs > Microsoft SQL Server > Client Network Utility**. The **SQL Server Client Network Utility** dialog box is displayed.
- 2 Click the **Alias** tab page to check the database name.

----End

A.6 Sybase Database

This topic covers FAQs about the Sybase database.

[A.6.1 Startup and Shutdown of the Sybase Database](#)

This topic describes the FAQs about the startup and shutdown of the Sybase database.

[A.6.2 Sybase Database Maintenance](#)

This topic describes the FAQs about the Sybase database maintenance.

A.6.1 Startup and Shutdown of the Sybase Database

This topic describes the FAQs about the startup and shutdown of the Sybase database.

[A.6.1.1 How to Disable the Sybase Database Service](#)

[A.6.1.2 How to Start the Sybase Database Service](#)[A.6.1.3 How to Verify That the Sybase Process Is Running](#)

A.6.1.1 How to Disable the Sybase Database Service

Question

How do I disable the Sybase database service?

Answer

- 1 Perform the following operations to disable the Sybase database service in the single-server system:

1. Log in to the OS as user **root**.
2. Run the following commands to disable the Sybase database service:

```
# su - sybase  
$ cd /opt/sybase/OCS*/bin  
$ ./isql -SDBSVR -Usa -Pchangeme
```

```
1> shutdown SYB_BACKUP
```

```
2> go
```

```
1> shutdown
```

```
2> go
```

NOTE

In the `./isql -SDBSVR -Usa -Pchangeme` command, *changeme* is the password of user **sa** of the Sybase database.

3. Run the following command to check whether the Sybase database service is disabled:

```
# ps -ef | grep sybase
```

If the following message is displayed, the Sybase database service has been disabled:

```
root  9629 14603  0 07:46:52 pts/3      0:00 grep sybase
```

- 2 Perform the following operations to disable the Sybase database service at the primary site in the HA system:

1. Log in to the primary site as user **root**.
2. Run the following command to start the VCS client at the primary site:

```
# hagui &
```

3. In the **Cluster Monitor** window, click the server record in the list.
4. In the dialog box that is displayed, enter the user name and the password of the VCS, and click **OK**.

NOTE

The default user of the VCS is **admin** and the default password is **password**.

5. On the VCS client of the primary site, right-click the database node and choose **Offline > PrimaryCluster** from the shortcut menu.
6. In the confirmation dialog box, click **Yes**.
7. Run the following command to check whether the Sybase database service is disabled:

```
# ps -ef | grep sybase
```

If the following message is displayed, the Sybase database service has been disabled:

```
root  9629 14603   0 07:46:52 pts/3      0:00 grep sybase
```

**NOTE**

By default, the Sybase database service at the secondary site is not running.

----End

A.6.1.2 How to Start the Sybase Database Service

Question

How do I start the Sybase database service?

Answer

- 1 Perform the following operations to start the Sybase database service in the single-server system:

1. Open a terminal window on Solaris OS and run the following commands to start the Sybase database service:

```
# su - sybase
$ cd /opt/sybase/ASE*/install
$ ./startserver -f ./RUN_DBSVR &
$ ./startserver -f ./RUN_DBSVR_back &
```

2. Run the following command to check whether the Sybase database service is running:

```
$ ./showserver
```

If the displayed information contains the following message, the Sybase database service is running.

```
UID    PID  PPID   C    STIME TTY          TIME CMD
sybase 4195  4170   0 18:42:26 ?           70:35 /opt/sybase/ASE-15_0/bin/
dataserver -ONLINE:1,0,0x6505fd2a, 10000000000, 0x18fc
sybase 4563  4559   0 18:42:50 ?           0:00 /opt/sybase/ASE-15_0/bin/
backupserver -SDBSVR_back -e/opt/sybase/ASE-15_0/install
sybase 4170  4168   0 18:42:00 ?           546:12 /opt/sybase/ASE-15_0/bin/
dataserver -sDBSVR -d/opt/sybase/data/lv_master -e/opt
```

- 2 Perform the following operations to start the Sybase database service in the HA system:

1. Run the following command to start the VCS client:

```
# hagui &
```
2. Choose **File > New Cluster** from the main menu. In the window that is displayed, enter the IP address of the server and click **OK**.
3. Enter the default user name **admin** and the default password **password** of the VCS client. Click **OK**.
4. Expand the **AppService** node in the navigation tree, and expand the **SybaseBk** node. Right-click **BackupServer** and choose **Online > host_name** from the shortcut menu.
5. In the dialog box that is displayed, click **Yes**.

Wait until **BackupServer** and **DatabaseServer** on the **Resources** tab page are available, which indicates that the Sybase database service is running.

----End

A.6.1.3 How to Verify That the Sybase Process Is Running

Question

How do I verify that the Sybase process is running?

Answer

- 1 In the single-server system, open a terminal window on Solaris OS.

- 2 Run the following commands to check the Sybase process status:

```
# su - sybase
$ cd /opt/sybase/ASE*/install
$ ./showserver
```

If the displayed information contains the following message, the Sybase database service is running.

```
UID   PID  PPID   C    STIME TTY          TIME CMD
sybase 4195  4170   0   18:42:26 ?           70:35 /opt/sybase/ASE-15_0/bin/
dataserver -ONLINE:1,0,0x6505fd2a, 10000000000, 0x18fc
sybase 4563  4559   0   18:42:50 ?           0:00 /opt/sybase/ASE-15_0/bin/
backupserver -SDBSVR_back -e/opt/sybase/ASE-15_0/install
sybase 4170  4168   0   18:42:00 ?           546:12 /opt/sybase/ASE-15_0/bin/
dataserver -sDBSVR -d/opt/sybase/data/lv_master -e/opt
```

- 3 Perform the following operations to start the Sybase database service in the HA system:

1. Run the following command to start the VCS client:
hagui &
2. Choose **File > New Cluster** from the main menu. In the window that is displayed, enter the IP address of the server and click **OK**.
3. Enter the default user name **admin** and the default password **password** of the VCS client. Click **OK**.
4. Expand the **AppService** node in the navigation tree, and expand the **SybaseBk** node. Right-click **BackupServer** and choose **Online > host_name** from the shortcut menu.
5. In the dialog box that is displayed, click **Yes**.

Wait until **BackupServer** and **DatabaseServer** on the **Resources** tab page are available, which indicates that the Sybase database service is running.

----End

A.6.2 Sybase Database Maintenance

This topic describes the FAQs about the Sybase database maintenance.

[A.6.2.1 How to Verify That the Sybase Database Has Been Installed](#)

[A.6.2.2 How to Check the Sybase Database Version](#)

[A.6.2.3 How to View the Server Name of the Sybase Database](#)

- [A.6.2.4 How to Change the Password of User sa for the Sybase Database](#)
- [A.6.2.5 How to Clear the Password of the Sybase Database](#)
- [A.6.2.6 How to View the Bit Number of the Sybase Database](#)
- [A.6.2.7 How to View the Details of the Sybase Database](#)
- [A.6.2.8 How to View Data Tables](#)
- [A.6.2.9 How to Query a Database Table if Only Part of the Table Name Is Remembered](#)
- [A.6.2.10 How to Identify Database Errors Caused by Unexpected Powering-Off of the Workstation](#)
- [A.6.2.11 How to Expand Space for the master Database](#)
- [A.6.2.12 How to Set Up More User Connections to a Database](#)
- [A.6.2.13 How to Check for Database Errors Using the dbcc Tool](#)
- [A.6.2.14 How to Set the Network Transport Parameters of Databases](#)
- [A.6.2.15 How to Delete a Suspect Database](#)
- [A.6.2.16 How to Delete a Damaged User Database](#)
- [A.6.2.17 How to Delete a Database from the Sybase Database?](#)
- [A.6.2.18 How to View the Deadlock Information in the Database](#)

A.6.2.1 How to Verify That the Sybase Database Has Been Installed

Question

How do I verify that the Sybase database has been installed?

Answer



NOTE

- The Sybase database will be automatically installed when the U2000 is installed if the Sybase database does not exist on the system.
- If the Sybase database exists on the system, a dialog box will be displayed asking you whether or not you want to reuse the Sybase database. There is no need to reinstall the Sybase database if it is reused (saves time, but not recommended).
- Consult with the computer administrator to see if the Sybase database has been installed.
- Verify that the installation directory and file of the Sybase database exist. A sample directory is **/opt/sybase**.
- Verify that the version of the Sybase database is correct. For details, see [A.6.2.2 How to Check the Sybase Database Version](#).
- Verify that the Sybase database is running. For details, see [A.6.1.3 How to Verify That the Sybase Process Is Running](#). For details about how to start the Sybase database, see [A.6.1.2 How to Start the Sybase Database Service](#).

----End

A.6.2.2 How to Check the Sybase Database Version

Question

How do I perform the required check on the Sybase database version to see if it is correct after the Sybase database is installed?

Answer

- 1 Switch to user **sybase**, and connect to the Sybase database. Run the following commands:

```
# su - sybase
```

```
$ cd /opt/sybase/OCS*/bin
```

```
$ ./isql -SDBSVR -Usa -Pchangeme
```

 **NOTE**

In the `./isql -SDBSVR -Usa -Pchangeme` command, *changeme* is the password of user **sa** of the Sybase database.

- 2 Run the following commands to check the Sybase database version:

```
1> use master
```

```
2> go
```

```
1> select @@version
```

```
2> go
```

 **NOTE**

There must be a space between **select** and **@** in the **select @@version** command.

A message similar to the following will be displayed:

```
Adaptive Server Enterprise/15.0.3/EBF 16548 ESD#1/P/Sun_svr4/OS 5.8/ase1503/268
0/64-bit/FBO/Thu Mar 5 09:39:28 2009
(1 row affected)
```

The preceding message indicates that Sybase database version is SYBASE 15.0.3.

----End

A.6.2.3 How to View the Server Name of the Sybase Database

Question

How do I view the server name of the Sybase database?

Answer

- 1 Log in to the OS as user **sybase**.
- 2 Run the following command to view the server name of the Sybase database:


```
$ more /opt/sybase/interfaces
```

A message similar to the following will be displayed:

```
DBSVR
      master tcp ether 10.71.225.89 4100
      query tcp ether 10.71.225.89 4100
      master tcp ether 10.71.225.89 4100
      query tcp ether 10.71.225.89 4100
      master tcp ether 127.0.0.1 4100
      query tcp ether 127.0.0.1 4100

DBSVR_back
      master tcp ether 10.71.225.89 4200
      query tcp ether 10.71.225.89 4200
      master tcp ether 10.71.225.89 4200
      query tcp ether 10.71.225.89 4200
      master tcp ether 127.0.0.1 4200
      query tcp ether 127.0.0.1 4200
```

 NOTE

Run the following commands to change the server name of the Sybase database to **DBSVR**:

```
$ cd /opt/HWENGR/upgrade/scripts/solaris
$ ./_modifyInterfaces.sh old_main_DBServer_name DBSVR
$ ./_modifyCfgFile.sh old_main_DBServer_name DBSVR
$ ./_modifyLogFile.sh old_main_DBServer_name DBSVR
$ ./_modifyRunFile.sh old_main_DBServer_name DBSVR
```

In the preceding commands, **old_main_DBServer_name** indicates the name of the server to be reused.

----End

A.6.2.4 How to Change the Password of User sa for the Sybase Database

Question

How do I change the password of user **sa** for the Sybase database?

Answer

- 1 Shut down the NMS server and client.

Log in to the single system as user **nmsuser** and run the following commands to end the U2000 processes:

```
$ cd /opt/U2000/server/bin
$ ./stopnms.sh
```

Log in to the primary site and run the following command to start the VCS client in the Veritas HA system:

```
# hagui &
```

In the **Cluster Monitor** window, click a server record in the information list.

In the login dialog box that is displayed, enter the user name and password of the VCS. Click **OK** to log in to the VCS client. The default user name and password of the VCS are **admin** and **password**.

Right-click **NMSServer** and choose **Offline > Host name** from the shortcut menu.

In the confirmation dialog box, click **Yes**.

 NOTE

Ensure that the database is running.

- 2 Log in to the network management maintenance suite (MSuite) client.
 1. On the computer where the MSuite client is installed, double-click the **U2000 MSuite** shortcut icon on the desktop. Wait about one minute. The **Login** dialog box is displayed.
 2. Set the login parameters and click **OK**. The **NMS maintenance suite** window will be displayed.
 - IP Address: Indicates the system IP address of the computer where the MSuite server is installed.
 - Port No.: The default port ID is **12212**. There is no need to change the default value during login.
 - User Name and Password: The default user name and password are **admin**.
 - 3 On the MSuite client, choose **Deploy > Change Database Administrator Password**. The **Change Database Administrator Password** dialog box is displayed.
 - 4 Enter the old password and new password.
- 5 Click **OK**. The password is changed.

 NOTE

A password must be 6-30 characters long and consists of letters or digits. Special characters are not allowed.

----End

A.6.2.5 How to Clear the Password of the Sybase Database

Question

How do I clear the password of the Sybase database?

Answer

- 1 Run the following commands to set the minimum password length to 0:

```
1> sp_configure 'minimum password length',0
2> go
```
 - 2 Run the following commands to clear the original password:

```
1> sp_password 'original password',null
2> go
```
- End

A.6.2.6 How to View the Bit Number of the Sybase Database

Question

How do I view the bit number of the Sybase database?

Answer

- 1 Run the following commands to view the bit number of the Sybase database:

```
# cd /opt/sybase/OCS*/bin
# ./isql -SDBSVR -Usa -Pchangeme
1>select @@version
2>go
```

NOTE

- In the `./isql -SDBSVR -Usa -Pchangeme` command, *changeme* is the password of user **sa** of the Sybase database.
- There must be a space between **select** and **@** in the `select @@version` command.

The following message will be displayed:

```
Adaptive Server Enterprise/12.5.3/EBF 13325 ESD#5/P/Sun_svr4/OS 5.8/ase1253/193
9/64-bit/FBO/Tue Dec 6 09:13:20 2005
```

64-bit indicates the bit number of the Sybase database.

----End

A.6.2.7 How to View the Details of the Sybase Database

Question

How do I view the details about the Sybase database during routine maintenance?

Answer

- 1 Run the following commands to view the details of all databases:

```
# cd /opt/sybase/OCS*/bin
# ./isql -SDBSVR -Usa -Pchangeme
1>sp_helpdb
2>go
```

NOTE

In the `./isql -SDBSVR -Usa -Pchangeme` command, *changeme* is the password of user **sa** of the Sybase database.

The information about the Sybase database will be displayed, including the name, size, owner, and status.

- 2 Run the following commands to view the details of a specific database:

```
1>sp_helpdb database_name
```

```
2>go
```

 **NOTE**

In the **sp_helpdb database_name** command, *database_name* is the name of the Sybase database.

Database space used can also be viewed.

----End

A.6.2.8 How to View Data Tables

Question

How do I view the details of data tables of the Sybase database during routine maintenance?

Answer

 **NOTE**

The following uses Sybase 12.5 as an example. For Sybase 12.0, replace **12_5** with **12_0** in the commands.

1. Run the following commands to view all data tables of the database.

```
# cd /opt/sybase/OCS*/bin
```

```
# ./isql -SDBSVR -Usa -P<sa password>
```

```
1>use <dbname>
```

```
2>go
```

```
1>sp_help
```

```
2>go
```

The data of all data tables in the specified database will be displayed, including name, owner, and type.

2. Run the following commands to view the details of a specific data table:

```
1>sp_help <tablename>
```

```
2>go
```

The structure data of the data table is displayed. This operation must be performed on the current database. Otherwise, the system prompts that the data table is not found.

A.6.2.9 How to Query a Database Table if Only Part of the Table Name Is Remembered

Question

How do I query a database table if I cannot remember the complete name of a database table?

Answer

- 1 Assume that **abc** is included in a database table name. Run the following SQL commands to query the database table after opening the database view:

```
1> select name from sysobjects where name like "%abc%"
```

```
2> go
```

All database table names containing **abc** will be displayed in a list.

----End

A.6.2.10 How to Identify Database Errors Caused by Unexpected Powering-Off of the Workstation

Question

How do I identify database errors caused by unexpected powering-off of the workstation?

Answer

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

2 Run the following commands to identify the database error:

```
# ps -ef | grep dataserver
```

NOTE

- If `/opt/sybase/ASE*/bin/dataserver` is displayed, the database server is running. In this case, skip the step for manually starting the database server, and check whether the database server malfunctions based on startup information.
- When only a line of `grep dataserver` is displayed, the database server is not running. In this case, run the following commands to start the database server manually:

```
# su - sybase
```

```
$ cd /opt/sybase/ASE*/install
```

```
$ ./startserver -f ./RUN_DBSVR
```

```
$ ./startserver -f ./RUN_DBSVR_back
```

3 Run the following commands to check whether the database server malfunctions by viewing the *Database server name.log* file:

```
$ cd /opt/sybase/ASE*/install
```

```
$ tail -100 DBSVR.log
```

NOTE

- Run the `tail -100 DBSVR.log` command to view the latest 100 records in the log file. You can adjust the number of records to be displayed.
- Check whether `error` or other error symbols are contained in the file. For example, error 926, a common error, is displayed:

```
Error: 926, Severity: 14, State: 1 00:00000:00001:2002/05/31  
09:26:26.65 server Database 'FaultDB' cannot be opened.
```

If the preceding message is displayed, the database server FaultDB is faulty.

4 Run the following commands to check whether the database connection is available if the preceding errors are not displayed:

```
$ cd /opt/sybase/OCS*/bin
```

```
$ ./isql -SDBSVR -Usa -P<sa password>
```

 NOTE

<sa password> is the password of user **sa** of the Sybase database.

The 1> prompt is displayed. If the 1> prompt is not displayed, verify that the database server is running and the password of user **sa** is correct.

Run the following commands to check whether the database is offline:

1>**sp_helpdb**

2>**go**

If the system does not prompt any error, the U2000 database works properly. In this case, start the U2000 again.

 NOTE

- If the NMS of Chinese edition is installed, illegible characters may be displayed when you log in to the system by using the remote terminal login tool (CLI-based). Then, set the encoding scheme of the remote terminal login tool to **UTF-8**.
- If the remote terminal login tool does not support the function of setting the encoding scheme, log in to the system through the GUI.

- 5 If the system prompts an error, check for database errors according to the error code and rectify the error. The following uses the FaultDB database as an example to describe how to rectify error 926.

Run the following commands:

1>**sp_configure "allow updates", 1**

2>**go**

1>**update sysdatabases set status =-32768 where name="FaultDB"**

2>**go**

1>**shutdown with nowait**

2>**go**

Restart the Sybase database service and register with the Sybase database as user **sa**.

1>**update sysdatabases set status=0 where name="FaultDB"**

2>**go**

1>**sp_configure "allow updates", 0**

2>**go**

1>**shutdown with nowait**

2>**go**

Check whether the U2000 database works properly. If the database error persists, contact Huawei technical support engineers.

----End

A.6.2.11 How to Expand Space for the master Database

Question

How do I expand space for the master database when it is full?

Answer

- 1 Run the **sp_helpdevice** command to check the space of the master database.
- 2 Run the following commands to increase space for the master database if the available space of the database device is sufficient:

```
# cd /opt/sybase/OCS*/bin  
# ./isql -SDBSVR -Usa -P<sa password>  
1>alter database master on master=18  
2>go
```
- 3 Run the following commands to back up the master database if the available space of the database device is insufficient:

```
# ./isql -SDBSVR -Usa -P<sa password>  
1>dump database master to '/opt/sybase/master.dump'  
2>go
```
- 4 Run the following commands to clear logs in the master database:

```
# clear master log  
1>dump tran master with truncate_only  
2>go
```
- 5 Run the following commands to restart the master database:

```
1>shutdown SYB_BACKUP  
2>go  
1>shutdown  
2>go  
----End
```

A.6.2.12 How to Set Up More User Connections to a Database

Question

How do I set up more user connections to a database?

Answer

- 1 Run the following commands to add the following content at the end of the **/etc/system** file:

```
# vi /etc/system
```

```
set rlim_fd_max = 4096 (set the maximum number of process file descriptors)
```

```
set rlim_fd_cur = 2048 (set the current number of process file descriptors)
```

- 2 Restart the system and run the following command to verify that the modification has taken effect:

```
$ sysdef | grep "file descriptors"
```

The following message will be displayed. The first hexadecimal number indicates the current value and the one indicates the maximum value.

```
0x00000000000000800:0x0000000000001000    file descriptors
```

- 3 Run the following commands to set the maximum number of user connections:

```
1>sp_configure 'number of user connections ',1024
```

```
2>go
```

```
----End
```

A.6.2.13 How to Check for Database Errors Using the dbcc Tool

Question

How do I check for database errors using the dbcc tool?

Answer

- 1 Log in to the OS of the primary site as user **root**.
- 2 Run the following commands to view the database error information:

```
# cd /opt/sybase/OCS*/bin
```

```
# ./isql -SDBSVR -Usa -P<sa password>
```

```
1>dbcc checkdb(database name)
```

```
2>go
```

 **NOTE**

In the **./isql -SDBSVR -Usa -P<sa password>** command, *<sa password>* indicates the password of user **sa**.

The system will display information about all database tables and database errors. The following uses **FaultDB** as an example.

```
1>dbcc checkdb(FaultDB)
```

```
2>go
```

A message similar to the following will be displayed:


```
Checking FaultDB
Checking sysobjects
The total number of data pages in this table is 6.
Table has 104 data rows.
ii
```

DBCC execution completed. If DBCC printed error messages, contact a user with System Administrator (sa) role.

- 3 Run the following commands to view the information about the database table error:

```
1>use (database name)
```

```
2>go
```

```
1>dbcc checktable(table name)
```

```
2>go
```

The system will display the check results and the error information about the database table.

- 4 Run the following commands to restore the database index:

```
1>dbcc reindex(table name)
```

```
2>go
```

All indexes of the database are automatically recreated.

- 5 Run the **quit** command to exit the **isql** program.

 NOTE

By default, the database service at the secondary site is not running.

----End

A.6.2.14 How to Set the Network Transport Parameters of Databases

Question

How do I set the network transport parameters of databases?

Answer

- 1 In Solaris 10, the network transmission parameters of databases are set incorrectly if you set **Transport type** to **tli tcp** when installing Sybase 12.5 manually or after you change the database transmission type to **tli tcp** in the **/opt/sybase/interfaces** file.

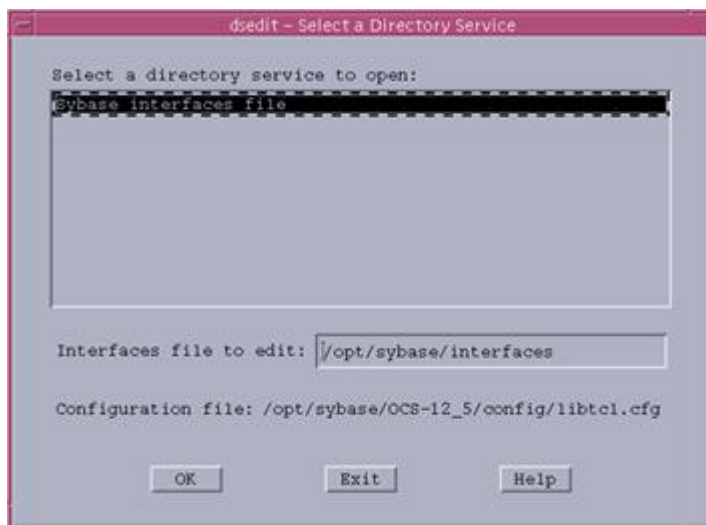
In Solaris10, set **Transport type** to **tcp** while installing Sybase12.5. Perform the following operations to correct parameter values if the parameters are set incorrectly.

- 2 Log in to the server as user **root**. Open the terminal window and run the following commands:

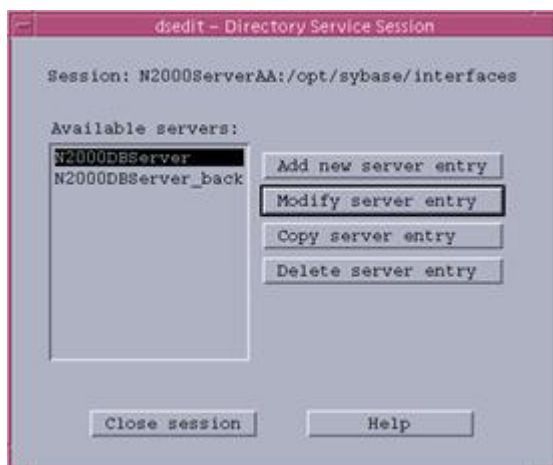
```
# ./opt/sybase/SYBASE.sh
```

```
# dsedit
```

- 3 In the dialog box as shown in [Figure A-2](#), click **OK**.

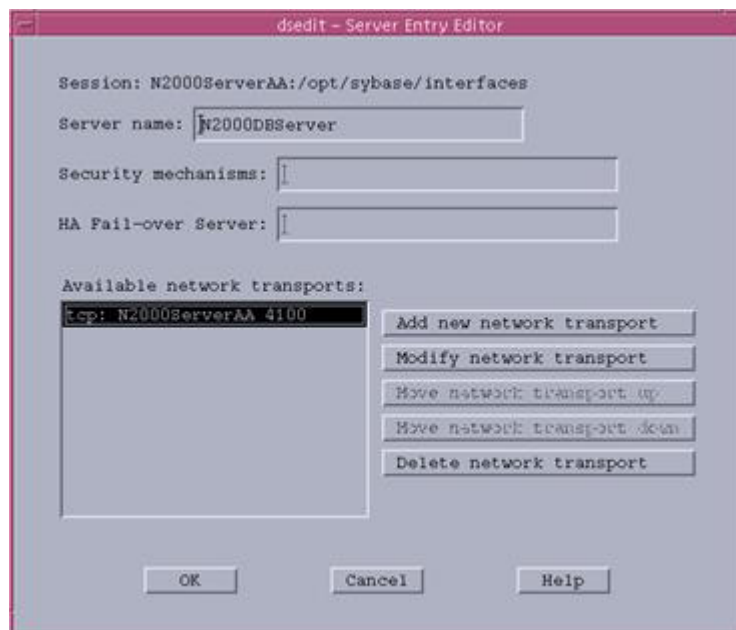
Figure A-2 Selecting the service path

- 4 In the dialog box as shown in [Figure A-3](#), select **DBSVR** and click **Modify Server entry**.

Figure A-3 Selecting the database service

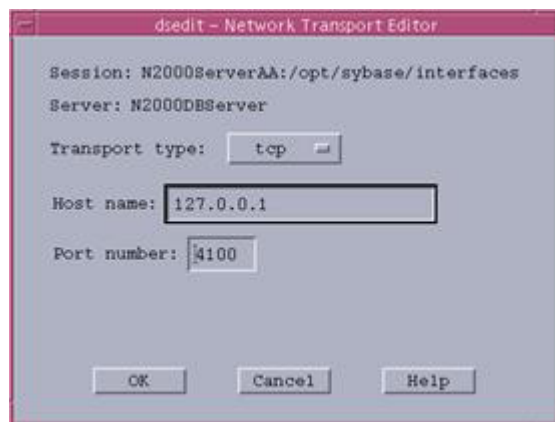
- 5 In the dialog box as shown in [Figure A-4](#), select available network transport settings, and click **Modify network transport**.

Figure A-4 Selecting available network transport settings



- 6 In the dialog box as shown in [Figure A-5](#), select **tcp** from the **Transport type** drop-down list.

Figure A-5 Modifying the transport type



- 7 Click **OK** in turn. The dialog box as shown in [Figure A-3](#) is displayed.
- 8 Repeat Step 4 to Step 6 and set **Transport type** of the **DBSVR_back** database to **tcp**.
- 9 Save the settings and close all the windows.
- 10 Restart the Sybase database to make the settings take effect.

NOTE

Before the operation, run the **ps -ef|grep sybase** command to check whether the Sybase service is running. If the Sybase service is running, stop it and restart it. If the Sybase service is not running, restart it.

----End

A.6.2.15 How to Delete a Suspect Database

Question

How do I delete a suspect database?

Answer

- 1 A suspect database cannot be deleted by the **drop database DBname** command. Run the **dbcc dbrepair(DBname, dropdb)** command in the **isql** command mode to delete the database. Replace **DBname** with the name of the actual suspect database. If the suspect database still cannot be deleted, change the database status to **320** and run the **dbcc dbrepair(DBname, dropdb)** command.

For example, if you cannot delete the suspect database iMapAlarmDB by running the **dbcc dbrepair(iMapAlarmDB, dropdb)** command, perform the following steps.

- 2 Change the status of the iMapAlarmDB database to **320**. Log in to the database as user **sa** and run the following commands:

```
1>sp_configure 'allow update', 1
```

```
2>go
```

```
1>update master..sysdatabases set status = -32768 where name = iMapAlarmDB '
```

```
2>go
```

```
1>shutdown
```

```
2>go
```

- 3 Restart the database server, log in to the system as a superuser, and run the following commands:

```
# su - sybase
```

```
$ cd /opt/sybase/ASE*/install
```

```
$ ./opt/sybase/SYBASE.sh
```

```
$ ./startserver -f ./RUN_DBSVR
```

```
$ ./startserver -f ./RUN_DBSVR_back &
```

- 4 Log in to the database as a superuser and run the following commands:

```
1>sp_configure 'allow update', 1
```

```
2>go
```

```
1>update master..sysdatabases set status = 320 where name = ' iMapAlarmDB '
```

```
2>go
```

```
1>select * from master..sysdatabases where name=" iMapAlarmDB "
```

```
2>go
```

The following message will be displayed:

```
name dbid suid status version logptr
crdate dumptrdate status2
audflags deftabaud defvwaud defpraud def_remote_type
def_remote_loc
status3 status4
-----
iMapAlarmDB 7 3 320 1 52602
02/01/14 02/02/07 48
0 0 0 0 NULL
NULL 0 0
(1 row affected)
```

- 5 Run the following commands to shut down the database:

```
1>shutdown
```

```
2>go
```

- 6 Restart the database server, log in to the system as user **root**, and run the following commands:

```
# su - sybase
```

```
$ cd /opt/sybase/ASE*/install
```

```
$ ./opt/sybase/SYBASE.sh
```

```
$ ./startserver -f ./RUN_DBSVR
```

```
$ ./startserver -f ./RUN_DBSVR_back &
```

 **NOTE**

Restart the database after changing the database status.

----End

A.6.2.16 How to Delete a Damaged User Database

Question

How do I delete a damaged database that cannot be deleted by the **drop database** command?

Answer

- 1 In the **isql** command mode, register with the SQL server as user **sa**.
- 2 Run the following commands to allow for modifying the system tables:

```
1>sp_configure "allow updates",1
2>go
```
- 3 Run the following commands to set the to-be-deleted user database to the suspect state.

```
1>use master
```

```
2>go
```

```
1>begin tran
```

```
2>go
```

```
1>update sysdatabases set status=256
```

```
2>where name="pubs2"
```

```
3>go
```

If 1 row affected is displayed, run the following commands:

```
1>commit
```

```
2>go
```

If 1 row affected is not displayed, run the following commands:

```
1>rollback
```

```
2>go
```

4 Restart the database server and register as user **sa** by running the **isql** command.

5 Run the following commands to delete the database:

```
1>dbcc dbrepair(pubs2,dropdb)
```

```
2>go
```

6 Run the following commands to allow for modifying the system tables:

```
1>sp_configure "allow updates",0
```

```
2>go
```

----End

A.6.2.17 How to Delete a Database from the Sybase Database?

Question

How do I delete a database from the Sybase database?

Answer

1 Run the following commands to gain access to the database:

```
# cd /opt/sybase/OCS*/bin
```

```
# ./isql -SDBSVR -Usa -P<sa password>
```

 NOTE

In the preceding command, `-SDBSVR` indicates that the database instance name is **DBSVR**.

If the password of user **sa** is changed, run the following command to gain access to the database:

```
# ./isql -SDBSVR -Usa -Pxxxx
```

In the preceding command, **XXXX** indicates the new password of user **sa**.

- 2 Run the following `isql` command:

```
1> drop database database name
```

For example:

```
1> drop database VpnDB
```

Run the following command to exit the **isql** program:

```
1> quit
```

- 3 In the `/opt/Sybase/data` directory, delete the `([database name]+data).dat` file and the `([database name]+log).dat` file, such as the **VpnDBdata.dat** file and the **VpnDBlog.dat** file.

----End

A.6.2.18 How to View the Deadlock Information in the Database

Question

How do I view the deadlock information in the Sybase database when errors occur?

Answer

- 1 Log in to the database server as user **root**.

- 2 Run the following commands:

```
# cd /opt/sybase/OCS*/bin
```

```
# ./isql -SDBSVR -Usa -P<sa password>
```

```
1>sp_lock
```

```
2>go
```

fid	spid	loid	locktype	table_id	page
	row	dbname	class		
	context				

	0	10	20 Sh_intent	464004684	0
		0 master	Non Cursor Lock		

```
(1 row affected)  
(return status = 0)
```

 NOTE

In the preceding information, `Non Cursor Lock` indicates that no deadlock occurs. The database name is `master`; the process ID of the locked table is `spid=10`; the locked table ID is `table_id=464004684`.

For further information, perform the following operations:

Run the following commands:

```
1>dbcc traceon(3604)
```

```
2>go
```

After the **dbcc** command is executed, contact the system administrator if any error information is displayed.

```
1>use master
```

```
2>go
```

```
1>select object_name(464004684)
```

```
2>go
```

```
-----  
spt_values
```

```
(1 row affected)
```

```
1>dbcc sqltext(10)
```

```
2>go
```

After the **dbcc** command is executed, contact the system administrator if any error information is displayed.

 NOTE

The previous commands are used to view the sessions of `table_id=464004684` and `spid=10`.

----End

A.7 Oracle Database

This topic describes the FAQs about the Oracle database.

[A.7.1 How to Check Whether the Oracle Database Has Been Installed](#)

[A.7.2 How to Check the Version of the Oracle Database](#)

[A.7.3 How to Check the Name of the Oracle Database](#)

[A.7.4 How to Start the Oracle Database in the High Availability System](#)

[A.7.5 How Can I Start the Oracle Database \(Single-Server System\)?](#)

[A.7.6 How to Shut Down the Oracle Database \(High Availability System\)](#)

[A.7.7 How Can I Stop the Oracle Database \(Single-Server System\)?](#)

[A.7.8 How Can I Check Whether the Oracle Database Is Started?](#)

[A.7.9 How Can I Change the Password of an Oracle Database User?](#)

[A.7.10 How Can I Check Whether the Oracle Listener Is Started?](#)

A.7.1 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 [A.7.8 How Can I Check Whether the Oracle Database Is Started?](#). For details about how to start the Oracle database, see [A.7.5 How Can I Start the Oracle Database \(Single-Server System\)?](#) [A.7.4 How to Start the Oracle Database in the High Availability System](#).

----End

A.7.2 How to Check the Version of the Oracle Database

Question

How to check the version of the Oracle database?

Answer

See [A.7.8 How Can I Check Whether the Oracle Database Is Started?](#).

A.7.3 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

A.7.4 How to Start the Oracle Database in the High Availability System

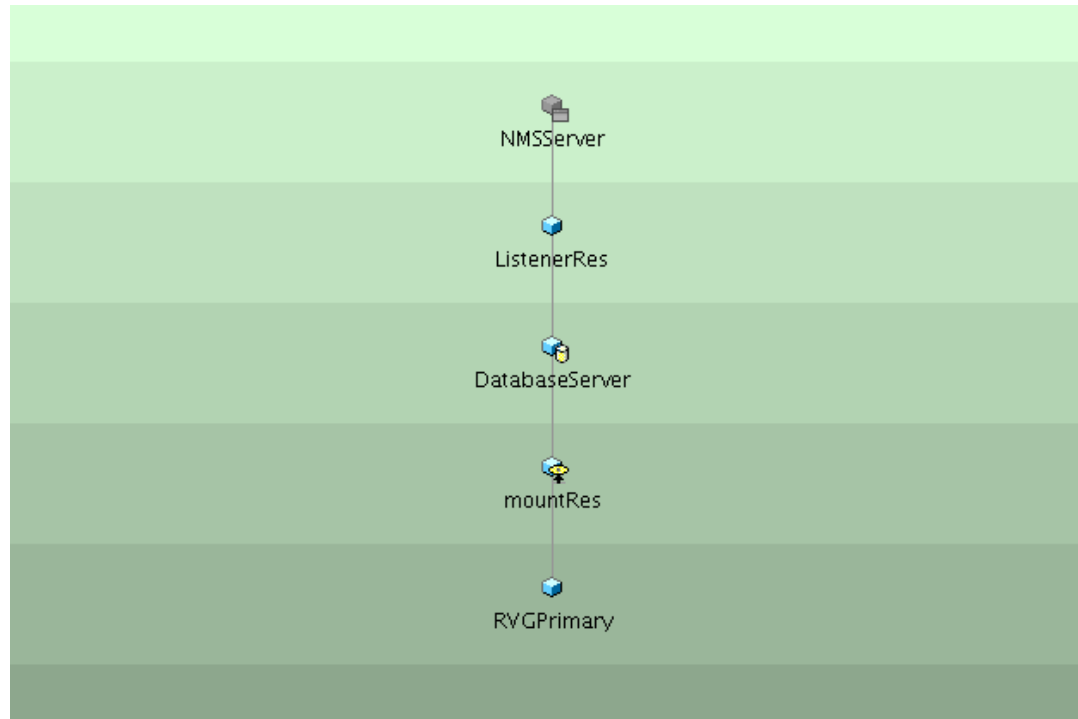
Question

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:

```
# hacli &
```
- 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

A.7.5 How Can I Start the Oracle Database (Single-Server System)?

Question

How Can I Start the Oracle Database?

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 Run the **startup** command to start the Oracle database.

```
> startup
```

The following is a display sample:

```
ORACLE instance started.
```

```
Total System Global Area 1610612736 bytes
Fixed Size                  2046264 bytes
Variable Size               385877704 bytes
Database Buffers            1207959552 bytes
Redo Buffers                 14729216 bytes
Database mounted.
Database opened.
```

ORACLE instance started, Database mounted, and Database opened indicate that the Oracle DB is started properly.

----End

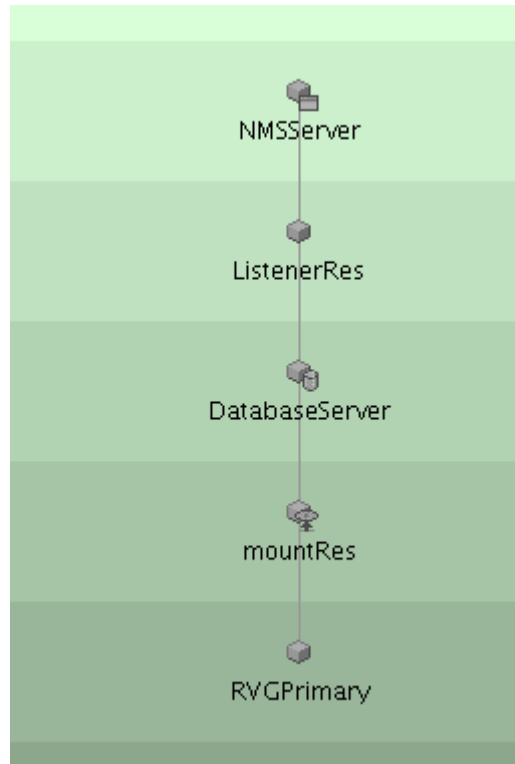
A.7.6 How to Shut Down the Oracle Database (High Availability System)

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

A.7.7 How Can I Stop the Oracle Database (Single-Server System)?

Question

How Can I Shut Down the Oracle Database?

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 Run the **shutdown** command to shut down the Oracle database.

```
> shutdown immediate
```

The following is a display sample:

```
Database closed.  
Database dismounted.  
ORACLE instance shut down.
```

Database closed indicates that the Oracle database is closed successfully. **Database dismounted** indicates that the database is dismounted successfully. **ORACLE instance shut down** indicates that the database instances are closed successfully.

----End

A.7.8 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 single system, see [A.7.5 How Can I Start the Oracle Database \(Single-Server System\)?](#) to start the Oracle database. for HA system, see [A.7.4 How to Start the Oracle Database in the High Availability System](#) to start the Oracle database.

----End

A.7.9 How Can I Change the Password of an Oracle Database User?

Question

How to Change the Password of an Oracle Database User?

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 Run the following command to modify the password of the database user **system**:

```
> alter user system identified by "testpwd";
```

system is the user name to be changed; **testpwd** is the customized password of the **system** user.

If **User altered** is displayed, it indicates that modification is successful; otherwise, find out the cause for failure according to the prompt.

----End

A.7.10 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

A.8 MSuite

This topic covers FAQs about the MSuite.

[A.8.1 How to Verify That The Process of the MSuite Server Is Started](#)

[A.8.2 How to Start the Process of the MSuite Server](#)

[A.8.3 How to End Processes on the MSuite Server](#)

A.8.4 How to Start the MSuite Client

A.8.1 How to Verify That The Process of the MSuite Server Is Started

Question

Login to the MSuite client is allowed only when the process of the MSuite server is running. How do I verify that process of the MSuite server is running?

Answer

- In Windows OS, check whether the **msdaemon.exe** and **msserver.exe** processes are started in the **Task Manager** window. If you can find the two processes in the process list, the MSuite server is running.
- In Solaris or SUSE Linux OS, run the following command as user **root** to verify that the MSuite server is running:

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

The MSuite server is running if **/opt/HWNMSJRE/jre_sol/bin/java -server** is displayed.

A.8.2 How to Start the Process of the MSuite Server

Question

Generally, the process of the MSuite server is started with the OS startup. How do I start the process of the MSuite server?

Answer

- In Windows OS, check whether the **msdaemon.exe** and **msserver.exe** processes are started in the **Task Manager** window. If you can find the two processes in the process list, the MSuite server is running. If the two processes do not exist in the process list, the MSuite server is not running. In this case, perform the following operations to start the MSuite server:

Go to the **C:\HWENGR\engineering** path, and double-click the **startserver.bat** file.

- In Solaris or SUSE Linux OS, run the following command as user **root** to verify that the MSuite server is running:

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

The MSuite server is running if **/opt/HWNMSJRE/jre_sol/bin/java -server** is displayed. Run the following commands to start the MSuite server if it is not running:

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

----End

A.8.3 How to End Processes on the MSuite Server

Question

How do I end processes on the MSuite server?

Answer

- In Windows OS, go to the **C:\HWENGR\engineering** path, double-click the **stopserver.bat** file, and end the MSuite server process.
- On Solaris or SUSE Linux OS, run the following commands as the **root** user:

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

A.8.4 How to Start the MSuite Client

Question

How do I start the MSuite client?

Answer

1. On a computer installed with the MSuite client, double-click the **U2000 NMS Maintenance Suite** shortcut icon on the desktop and then wait about one minute. The **Login** dialog box is displayed.

NOTE

- In Solaris OS, log in to the Java desktop system as user **nmsuser**. Otherwise, the **U2000 NMS Maintenance Suite** shortcut icon is not displayed on the desktop. To start the MSuite client by running commands, run the following commands as user **nmsuser**:

```
cd /opt/U2000/engineering  
./startclient.sh
```
 - In SUSE Linux OS, log in to GUI-based desktop system as user **root**. Otherwise, the **U2000 NMS Maintenance Suite** shortcut icon is not displayed on the desktop. To start the MSuite client by running commands, you need to run the following command as the **nmsuser** user:

```
cd /opt/U2000/engineering  
./startclient.sh
```
2. Set the login parameters.
 - IP Address:
 - To log in to the local MSuite server, use the default IP address **127.0.0.1**.
 - To log in to the remote MSuite server, enter the IP address of the computer where the MSuite server is installed. If multiple IP addresses are configured for the computer, use the NMS application IP address.
 - Port No.: The default port ID is **12212**. There is no need to change the default value during login but ensure that the port is not occupied.
 - User Name: The default user name is **admin**.
 - Password: The default password is **admin**.
 3. Click **Login**.

NOTE

- When you log in to the MSuite client, a progress bar is displayed showing the progress of querying components and instances. Wait until the operation is complete.
- The MSuite works in single-user mode. Specifically, only one MSuite client can log in to the MSuite at one time.

A.9 U2000 System

This topic covers FAQs about the U2000 system.

- [A.9.1 How to Verify That the U2000 Is Installed](#)
- [A.9.2 How to Change the System Time and Time Zone of the Single-Server System on Windows](#)
- [A.9.3 How to Change the System Time and Time Zone of the Single-Server System \(Solaris\)](#)
- [A.9.4 How to Change the System Time and Time Zone of the Single-Server System \(SUSE Linux-Distributed\)](#)
- [A.9.5 How to Change the System Time and Time Zone of the High Availability System on Windows](#)
- [A.9.6 How to Change the System Time and Time Zone of the High Availability System \(Solaris\)](#)
- [A.9.7 How to Change the System Time and Time Zone of the High Availability System \(SUSE Linux-Distributed\)](#)
- [A.9.8 How to Change the IP Address of the Single-Server System on Windows](#)
- [A.9.9 How to Change the Host Name of the Single-Server System on Windows](#)
- [A.9.10 How to Change the IP Address and Host Name for the Single-Server System \(Solaris\)](#)
- [A.9.11 How to Change the IP Address and Host Name of the Single-Server System \(SUSE Linux-Distributed\)](#)
- [A.9.12 How to Modify the Server IP Address of High Availability System \(Windows\)](#)
- [A.9.13 How to Change the Host Name of the High Availability System \(Windows\)](#)
- [A.9.14 How to Change the IP Address and Host name for the High Availability System \(Solaris\)](#)
- [A.9.15 How to Change the IP Address and Host Name of the High Availability System \(SUSE Linux-Distributed\)](#)
- [A.9.16 How to Verify That the Processes of the U2000 Single-Server System Are Running on Windows](#)
- [A.9.17 How to Start the Processes of the U2000 Single-Server System on Windows](#)
- [A.9.18 How to End the Processes of the U2000 Single-Server System on Windows](#)
- [A.9.19 How to Verify That the Processes of the U2000 Single-Server System Are Running on Solaris](#)
- [A.9.20 How to Start the Processes of the U2000 Single-Server System on Solaris](#)
- [A.9.21 How to End the Processes of the U2000 Single-Server System on Solaris](#)
- [A.9.22 How to Verify That the Processes of the U2000 Single-Server System \(SUSE Linux-Distributed\) Are Running](#)
- [A.9.23 How to Start the Processes of the U2000 Single-Server System \(SUSE Linux-Distributed\)](#)
- [A.9.24 How to End the Processes of the U2000 Single-Server System \(SUSE Linux-Distributed\)](#)
- [A.9.25 How to Check Whether the U2000 Processes of the High Availability System \(Windows\) Are Started](#)
- [A.9.26 How to Start the U2000 Processes of the High Availability System \(Windows\)](#)
- [A.9.27 How to End the U2000 Processes of the High Availability System \(Windows\)](#)

- [A.9.28 How to Check Whether the U2000 Processes of the High Availability System \(Solaris\) Are Started](#)
- [A.9.29 How to Start the U2000 Processes of the High Availability System \(Solaris\)](#)
- [A.9.30 How to End the U2000 Processes of the High Availability System \(Solaris\)](#)
- [A.9.31 How to Check Whether the U2000 Processes of the High Availability System \(SUSE Linux-Distributed\) Are Started](#)
- [A.9.32 How to Start the U2000 Processes of the High Availability System \(SUSE Linux-Distributed\)](#)
- [A.9.33 How to End the U2000 Processes of the High Availability System \(SUSE Linux-Distributed\)](#)
- [A.9.34 What Factors Affect the Response Speed of the NMS](#)
- [A.9.35 How to Resolve the Problem Wherein Illegible Characters Occur in the NMS Window](#)
- [A.9.36 How to Configure the ipmap.cfg Mapping File](#)
- [A.9.37 How to Determine Which Types of Software Are Preinstalled](#)
- [A.9.38 How to Check Whether the daem Process Is Started](#)
- [A.9.39 How to Start the daem Process](#)
- [A.9.40 How to End the daem Process](#)
- [A.9.41 How to Rectify the Application GUI Startup Failure Caused by User Switching](#)
- [A.9.42 How to Rectify the U2000 Startup Failure After the IP Address or Host Name of the Single-Server System \(Solaris\) Is Changed Manually](#)
- [A.9.43 How to Rectify the U2000 Startup Failure Because the IP Address or Host Name of the Single-Server System \(SUSE Linux-Distributed\) Is Changed Manually](#)
- [A.9.44 How to View the U2000 and Sybase Database Installation Paths](#)
- [A.9.45 How to View Network Configurations for the Primary Site or Secondary Site Installed with a HA System](#)
- [A.9.46 How to Rectify the Mouse Detection Failure and Open the GUI After the T5220 Is Connected to the KVM](#)
- [A.9.47 How to Check Downloaded Software Packages by Using MD5 Software](#)
- [A.9.48 How to Rectify the Failure to Connect to the Sybase Database During U2000 Installation](#)
- [A.9.49 Reinstalling the U2000 on or Migrating the U2000 to Another Computer](#)
- [A.9.50 How to Set the Communication Mode on the U2000 server for the Single-Server System \(Windows\)](#)
- [A.9.51 How to Set the Communication Mode on the U2000 server for the Single-Server System \(Solaris\)](#)
- [A.9.52 How to Configure the Communication Mode for a Linux-based U2000 Server?](#)
- [A.9.53 How to Set the Communication Mode on the U2000 Server for the High Availability System \(Windows\)](#)

[A.9.54 How to Set the Communication Mode of the Server in a High Availability System \(Solaris\)?](#)

[A.9.55 How to Set the Communication Mode of the Server in a High Availability System \(SUSE Linux-Distributed\)](#)

A.9.1 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 a user with administrator rights.
2. Check whether the icons of the U2000 client and U2000 System Monitor exist on the desktop. If they exist, it indicates that the U2000 has been installed.

 NOTE

Sometimes, the shortcut icons do not exist on the desktop because they are deleted by mistake. In this case, check whether the U2000 is installed by choosing **Start > All Programs**. If the U2000 item exists after you choose **Start > All Programs**, it indicates that the U2000 is installed.

1. Log in to the OS as user **nmsuser**.
2. Check whether the icons of the U2000 client and U2000 System Monitor exist on the desktop. If they exist, it indicates that the U2000 has been installed.
3. If login to the desktop fails, run the following commands to view the **/opt/U2000** directory: If this directory exists and is not empty, it indicates that the U2000 is installed.

```
$ cd /opt/U2000
```

```
$ ls
```

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
```

A.9.2 How to Change the System Time and Time Zone of the Single-Server System on Windows

Question

How do I change the system time and time zone of the single-server system on Windows?



CAUTION

When the U2000 services are running, do not change the system time.

Answer

- 1 Stop the U2000 processes and the SQL Server database.
- 2 Open the **Control Panel** window. Then, double-click the **Date and Time** icon.
- 3 In the dialog box that is displayed, click the **Time & Data** tab to set the current system date and time. Click the **Time Zone** tab and select the required time zone from the related drop-down list.
- 4 Click **OK**.
- 5 Restart the OS.

----End

A.9.3 How to Change the System Time and Time Zone of the Single-Server System (Solaris)

Question

How do I change the system time and time zone of the single-server system (Solaris)?

Answer

- 1 Log in to the OS of the server as user **nmsuser**.
- 2 Open a terminal window and run the following commands to end U2000 processes.

```
$ cd /opt/U2000/server/bin
$ ./stopnms.sh
```

- 3 Run the following commands to end database processes.

```
# su - sybase

$ cd /opt/sybase/OCS*/bin

$ ./isql -SDBSVR -Usa -Pchangeme
```

```
1> shutdown SYB_BACKUP
```

```
2> go
```

```
1> shutdown
```

```
2> go
```

 **NOTE**

In the `./isql -SDBSVR -Usa -Pchangeme` command, *changeme* is the password of user **sa** of the Sybase database.

- 4 After the processes are ended, [log in to the MSuite client](#).
- 5 On the MSuite client, choose **Deploy > Modify time zone**. The **Modify the system time zone** dialog box is displayed.
- 6 Set the time zone and system time according to the local time zone and standard time.

- 7 Click **OK**.
- 8 After changing the system time and time zone, restart the OS for the settings to take effect. Restart the OS by following prompts. The commands for restarting the OS are as follows:

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

----End

A.9.4 How to Change the System Time and Time Zone of the Single-Server System (SUSE Linux-Distributed)

Question

How do I change the system time and time zone of the SUSE Linux single-server system?

Answer

- 1 Log in to the OS of the master server as user **root**.
- 2 Open a terminal window and run the following commands to end U2000 processes.

```
# cd /opt/U2000/server/bin
# ./stopnms.sh
```
- 3 Run the following commands to end database processes.

```
> su - oracle
password:oracle_user_password
> sqlplus / as sysdba
SQL> shutdown immediate
SQL> exit
> exit
```
- 4 Log in to the slave server as user **root**. Open a terminal window and run the following command to end the **daem** process of the slave server:

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



CAUTION

If multiple slave servers are installed, perform this step on every slave server.

- 5 After the **daem** process is ended, **log in to the MSuite client**.



NOTE

The IP address entered during login is the system IP address of the master server.

- 6 On the MSuite client, choose **Deploy > Modify time zone**. The **Modify the system time zone** dialog box is displayed.
- 7 Set the time zone and system time according to the local time zone and standard time.
- 8 Click **OK**.
- 9 After changing the system time and time zone, restart the OS for the settings to take effect. Restart the OSs of the master server and all slave servers by following prompts. The commands for restarting the OSs are as follows:

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

----End

A.9.5 How to Change the System Time and Time Zone of the High Availability System on Windows

Question

How do I change the system time and time zone of the high availability system on Windows?

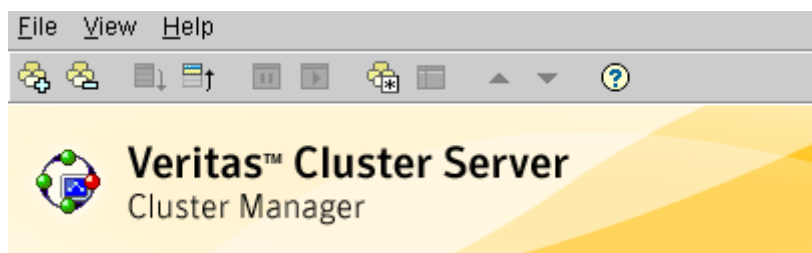


CAUTION

When the U2000 services are running, do not change the system time.

Answer

- 1 Stop the U2000 processes and the SQL Server database.
 1. Choose **Start > Programs > Symantec > Veritas Cluster Server > Veritas Cluster Manager - Java Console** to start the VCS client.



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

3. Enter the IP address of the system of the primary site. Then, click **OK**.

4. Enter the default user name **admin** and the default password **password** of the VCS client. Then, click **OK**.
 5. Right-click **AppService** in the navigation tree and choose **Offline** > *host_name* from the shortcut menu.
 6. In the dialog box that is displayed, click **Yes**.
- 2 Open the **Control Panel** window. Then, double-click the **Date and Time** icon.
 - 3 In the dialog box that is displayed, click the **Time & Data** tab to set the current system date and time. Click the **Time Zone** tab and select the required time zone from the related drop-down list.
 - 4 Click **OK**.
 - 5 Restart the OS.

----End

A.9.6 How to Change the System Time and Time Zone of the High Availability System (Solaris)

Question

How do I change the system time and time zone of the High Availability System (Solaris)?

Answer

- 1 Log in to the primary site as user **root**. Open a terminal window and run the following command to shut down the high availability system:

```
# hagrps -offline AppService -sys host_name_of_active_site
```

For example, if the host name of the primary site is **Primaster**, run the # **hagrps -offline AppService -sys Primaster** command.

- 2 [Log in to the MSuite client.](#)



NOTE

The IP address entered during login is the system IP address of the primary site.

- 3 On the MSuite client, choose **Deploy** > **Modify time zone**. The **Modify the system time zone** dialog box is displayed.
- 4 Set the time zone and system time according to the local time zone and standard time.
- 5 Click **OK**.
- 6 After changing the system time and time zone, restart the OS for the settings to take effect. Restart the OS by following prompts. The commands for restarting the OS are as follows:

```
# cd /opt/VRTSvcs/bin
# hastop -all -force
# sync;sync;sync;sync
# shutdown -y -g0 -i6
```

- 7 [Log in to the MSuite client.](#)



NOTE

The IP address entered during login is the system IP address of the secondary site.

- 8 Set the time zone and system time according to the local time zone and standard time.
- 9 Set the time zone and system time according to the local time zone and standard time.
- 10 Click **OK**.
- 11 After changing the system time and time zone, restart the OS for the settings to take effect. Restart the OS by following prompts. The commands for restarting the OS are as follows:

```
# cd /opt/VRTSvcs/bin
# hstop -all -force
# sync;sync;sync;sync
# shutdown -y -g0 -i6
```


----End

A.9.7 How to Change the System Time and Time Zone of the High Availability System (SUSE Linux-Distributed)

Question

How do I change the system time and time zone of the High Availability System (SUSE Linux-Distributed)?

Answer

- 1 Log in to the master server of the active site as user **root**. Open a terminal window and run the following command to shut down the high availability system:

```
# hgrp -offline AppService -sys host name of master server of active site
```


For example, if the host name of the master server of the active site is **Primaster**, run the **#hgrp -offline AppService -sys Primaster** command.
- 2 Log in to the slave server as user **root**. Open a terminal window and run the following command to end the **daem** process of the slave server:

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



CAUTION

If multiple slave servers are installed, perform this step on every slave server of the primary and secondary sites.

- 3 **Log in to the MSuite client.**



NOTE

The IP address entered during login is the system IP address of the master server of the primary site.

- 4 On the MSuite client, choose **Deploy > Modify time zone**. The **Modify the system time zone** dialog box is displayed.
- 5 Set the time zone and system time according to the local time zone and standard time.
- 6 Click **OK**.
- 7 After changing the system time and time zone, restart the OS for the settings to take effect. Restart the OS by following prompts. The commands for restarting the OS are as follows:

```
# cd /opt/VRTSvcs/bin
# hstop -all -force
# sync;sync;sync;sync
# shutdown -r now
```

**CAUTION**

You need to perform this step on the master server of the primary site and all slave servers.

8 Log in to the MSuite client.**NOTE**

The IP address entered during login is the system IP address of the master server of the secondary site.

- 9 Set the time zone and system time according to the local time zone and standard time.
- 10 Set the time zone and system time according to the local time zone and standard time.
- 11 Click **OK**.
- 12 After changing the system time and time zone, restart the OS for the settings to take effect. Restart the OS by following prompts. The commands for restarting the OS are as follows:

```
# cd /opt/VRTSvcs/bin
# hstop -all -force
# sync;sync;sync;sync
# shutdown -r now
```

**CAUTION**

You need to perform this step on the master server of the secondary site and all slave servers.

----End

A.9.8 How to Change the IP Address of the Single-Server System on Windows

Question

How do I to change the server IP address when the networking plan is changed?

**CAUTION**

If the server IP address or host name is changed, the previously backed up data cannot be used for restoration. In such a case, you need to back up the data again.

Do not change an IP address and a host name at the same time. Otherwise, the U2000 fails to be started.

Changing an IP address includes the following major steps:

1. Shut down the U2000 server and client, and ensure that the database is running.
2. Shut down the U2000 MSuite server.
3. Change the IP address of the U2000 server.
4. Start the U2000 MSuite server.
5. Log in to the U2000 MSuite client and synchronize IP address changes in configuration files. If the IP address changes are not synchronized, the U2000 fails to start properly.
6. Restart the OS.

Answer

- 1 Shut down the NMS server and client.

In the directory of the NMS software after the installation, for example, the **D:\U2000\server\bin** directory, run the **stopnms.bat** file to end the NMS processes.

NOTE

Ensure that the database is started.

- 2 End the server process of the MSuite.

In the **C:\HWENGR\engineering** directory, double-click the **stopserver.bat** file to end the server process of the MSuite.

- 3 In the classic start menu mode, choose **Start > Settings > Network Connections**.

- 4 In the **Network Connections** dialog box that is displayed, right-click the network connection to be configured and choose **Properties** from the shortcut menu.

- 5 On the **General** tab page (for the local connection) or **Network** tab page (for all other connections), select **Internet Protocol (TCP/IP)**. Then, click **Properties**.

- 6 In the **Internet Protocol (TCP/IP) Properties** dialog box that is displayed, enter the new IP address, subnet mask, and default gateway address, and perform the related modification. Click **OK**.

- 7 Start the server process of the MSuite.

In the **C:\HWENGR\engineering** directory, double-click the **startserver.bat** file to start the server process of the MSuite.

- 8 Log in to the MSuite client.

1. On the computer where the MSuite client is installed, double-click the **U2000 MSuite** shortcut icon on the desktop. Wait about one minute. The **Login** dialog box is displayed.
2. Set the related login parameters and click **OK**. The **NMS maintenance suite** window is displayed.
 - IP Address: Indicates the system IP address of the computer where the MSuite server is installed.
 - Port No.: The default port number is **12212**. You do not need to change the default value during login.
 - User Name and Password: Both the default user name and default password are **admin**.

NOTE

A dialog box may be displayed during the process of logging in to the MSuite client. Click **OK** according to the prompt.

- 9 On the **Server** tab page, right-click the server to be configured and choose **Synchronize the network configuration** from the shortcut menu. Click **OK**.
- 10 Restart the OS.

**NOTE**

If NBIs and instances are deployed and the xFtp monitor is configured before the IP address is changed, you must configure NBIs on the MSuite client and re-configure the xFtp monitor on the U2000 client after changing the IP address.

- For details about how to configure NBIs, see the related NBI user guide.
- For details about how to configure the xFtp monitor, see the U2000 Help.

----End

A.9.9 How to Change the Host Name of the Single-Server System on Windows

Question

How do I change the host name of the single-server system on Windows?

**CAUTION**

If the server IP address or host name is changed, the previously backed up data cannot be used for restoration. In such a case, you need to back up the data again.

Do not change an IP address and a host name at the same time. Otherwise, the U2000 fails to be started.

Changing the host name includes the following major steps:

1. Shut down the U2000 server and client.
2. Change the host name of the U2000 server.
3. Restart the OS.
4. Log in to the U2000 MSuite client and synchronize host name changes in configuration files. If the host name changes are not synchronized, the U2000 fails to start properly.

Answer

- 1 Log in to the OS as a user with administrator rights.
- 2 Shut down the NMS server and client.

In the directory of the NMS software after the installation, for example, the **D:\U2000\server\bin** directory, run the **stopnms.bat** file to end the NMS processes.

- 3 Perform the following operations to change the host name of the server:
 1. On the desktop, right-click the **My Computer** icon and choose **Properties** from the shortcut menu.
 2. In the dialog box that is displayed, click the **Computer Name** tab, and then click **Change**.

3. In the dialog box that is displayed, change the computer name, and then click **OK**.
4. Restart the OS.
- 4 Log in to the MSuite client.
 1. On the computer where the MSuite client is installed, double-click the **U2000 MSuite** shortcut icon on the desktop. Wait about one minute. The **Login** dialog box is displayed.
 2. Set the related login parameters and click **OK**. The **NMS maintenance suite** window is displayed.
 - IP Address: Indicates the system IP address of the computer where the MSuite server is installed.
 - Port No.: The default port number is **12212**. You do not need to change the default value during login.
 - User Name and Password: Both the default user name and default password are **admin**.



NOTE

A dialog box may be displayed during the process of logging in to the MSuite client. Click **OK** according to the prompt.

- 5 On the **Server** tab page, right-click the server to be configured and choose **Synchronize the network configuration** from the shortcut menu. Click **OK**.

----End

A.9.10 How to Change the IP Address and Host Name for the Single-Server System (Solaris)

Question

How to change the IP address and host name for the single-server system (Solaris)?

Answer

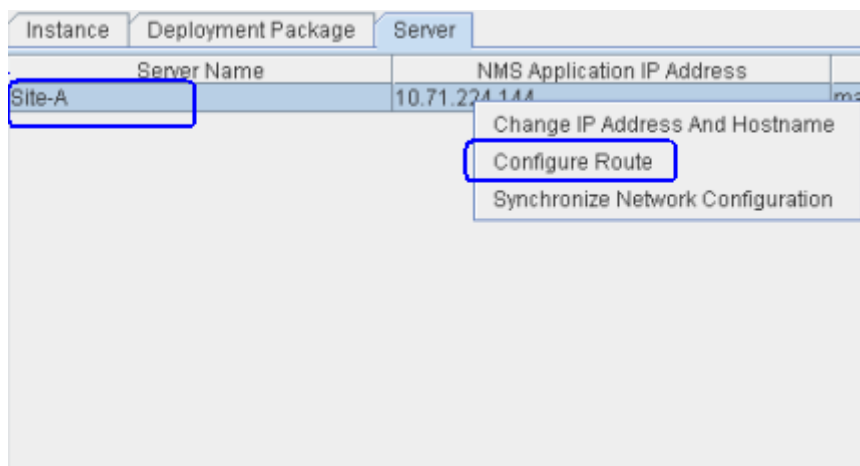


NOTE

To change the IP address and host name for the single-server system (Solaris), do as follows:

1. Stop U2000 server processes.
 2. Use the MSuite to change the IP address and host. If a route is changed, reconfigure the route.
 3. Restart the OS to make the modifications take effect.
- 1 Log in to the OS of the server as user **nmsuser**.
- 2 Open a terminal window and run the following commands to end U2000 processes.

```
$ cd /opt/U2000/server/bin
$ ./stopnms.sh
```
- 3 After the processes are ended, **log in to the MSuite client**.
- 4 On the MSuite client, click the **Server** tab.
- 5 If the route changes, do as follows to add a route. If the route does not change, you do not need to change the IP address or host name. Instead, skip this step.
 1. Right-click the server name and choose **Configure Route** from the shortcut menu.



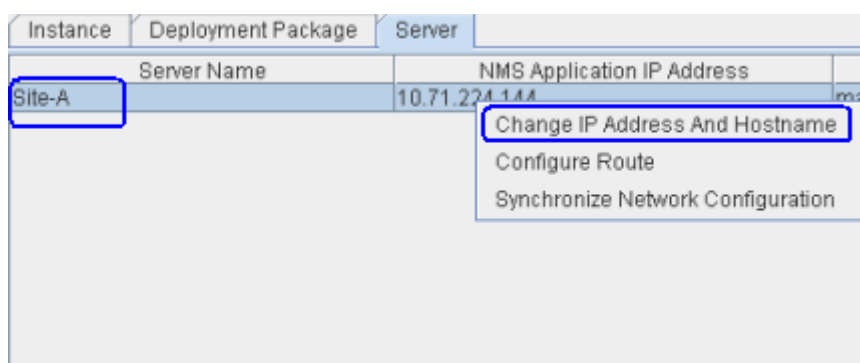
2. In the dialog box that is displayed, click **Add** or **Delete** according to actual route conditions to re-configure the route.

Destination	Subnet Mask	Route
0.0.0.0	0.0.0.0	10.71.224.1
10.71.224.0	255.255.254.0	10.71.224.144
127.0.0.1	255.255.255.255	127.0.0.1

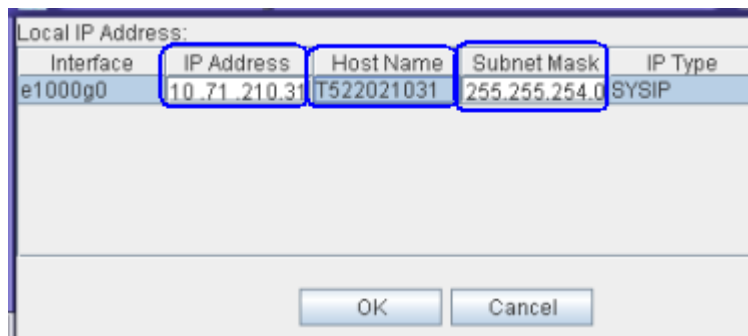
3. Click **OK**.

6 Do as follows to change the host name and IP address.

1. Right-click the server name and choose **Change IP Address And Hostname** from the shortcut menu.



2. In the **Change IP Address And Hostname** dialog box, enter the new host name, IP address, and subnet mask.



3. Click **OK**. The progress bar is displayed. Wait patiently.
 4. After the configuration is complete, the **Message** dialog box is displayed, asking you to restart the OS and back up the database in time. click **OK**.
- 7 Restart the OS for the settings to take effect.

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

NOTE

If NBIs and instances are deployed and the xFtp monitor is configured before the host name and IP address are changed, you must configure NBIs on the MSuite client and re-configure the xFtp monitor on the U2000 client after changing the IP address and host name.

- For details about how to configure NBIs, see the related NBI user guide.
- For details about how to configure the xFtp monitor, see the U2000 Help.

----End

A.9.11 How to Change the IP Address and Host Name of the Single-Server System (SUSE Linux-Distributed)

Question

How to change the IP address and host name of the Single-Server System (SUSE Linux-Distributed)?

Answer

NOTE

To change the IP address and host name for the single-server system (Solaris), do as follows:

1. Stop U2000 server processes.
 2. Use the MSuite to change the IP address and host. If a route is changed, reconfigure the route.
 3. Restart the OS to make the modifications take effect.
- 1 Log in to the OS of the master server as user **root**.
 - 2 Open a terminal window and run the following commands to end U2000 processes.


```
# cd /opt/U2000/server/bin
# ./stopnms.sh
```
 - 3 Log in to the slave server as user **root**. Open a terminal window and run the following command to end the **daem** process of the slave server:


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

**CAUTION**

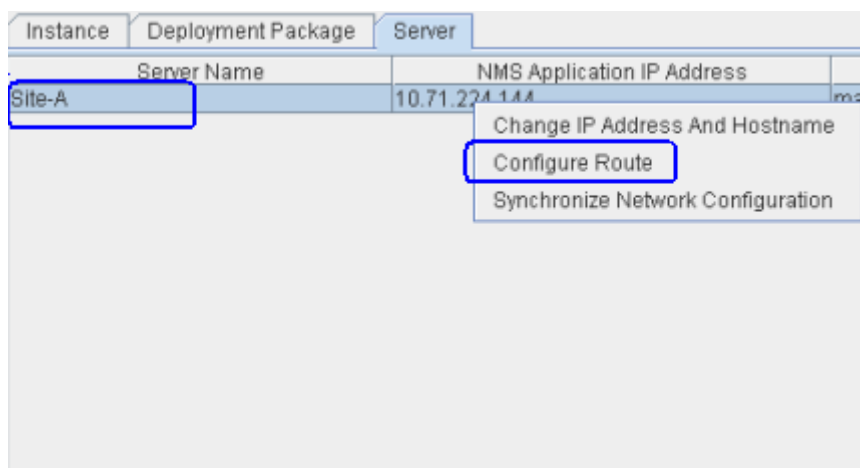
If multiple slave servers are installed, perform this step on every slave server.

- 4 After the **daem** process is ended, **log in to the MSuite client**.

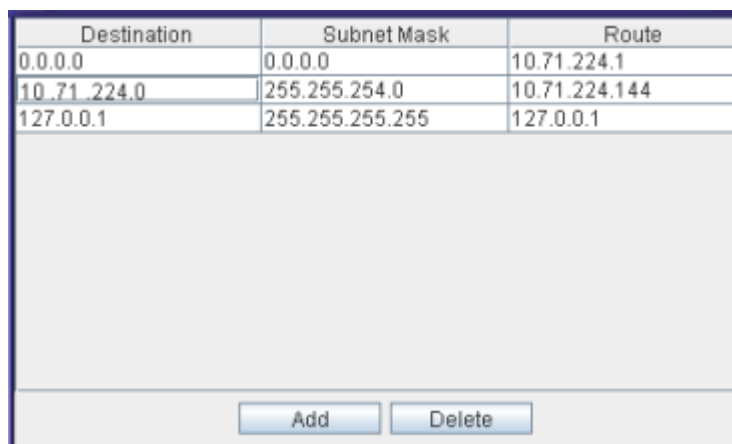
**NOTE**

The IP address entered during login is the system IP address of the master server.

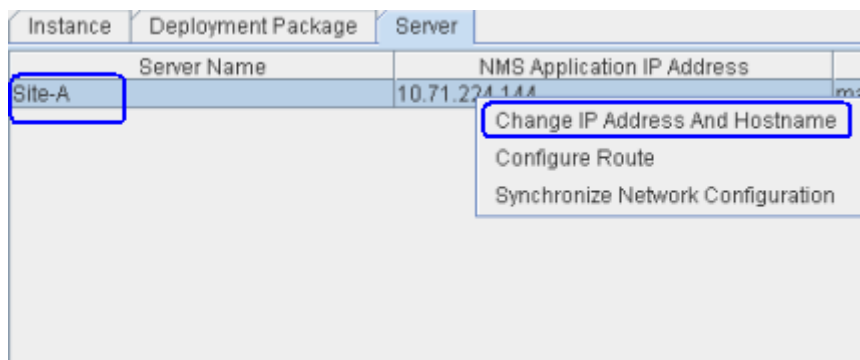
- 5 On the MSuite client, click the **Server** tab.
- 6 If the route changes, do as follows to add a route. If the route does not change, you do not need to change the IP address or host name. Instead, skip this step.
1. Right-click the server name and choose **Configure Route** from the shortcut menu.



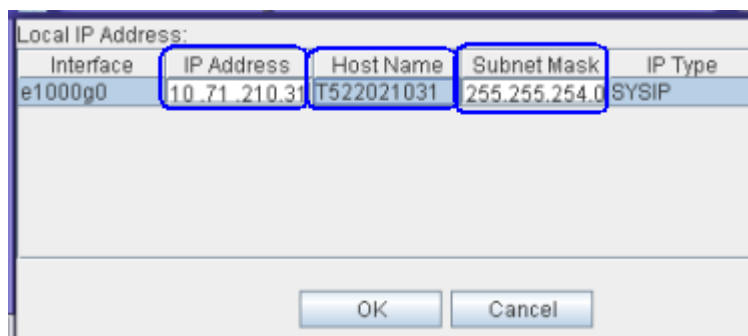
2. In the dialog box that is displayed, click **Add** or **Delete** according to actual route conditions to re-configure the route.



3. Click **OK**.
- 7 Do as follows to change the host name and IP address.
1. Right-click the server name and choose **Change IP Address And Hostname** from the shortcut menu.



2. In the **Change IP Address And Hostname** dialog box, enter the new host name, IP address, and subnet mask.



3. Click **OK**. The progress bar is displayed. Wait patiently.
 4. After the configuration is complete, the **Message** dialog box is displayed, asking you to restart the OS and back up the database in time. click **OK**.
- 8 Restart the OS of the server whose host name and IP address are changed for the settings to take effect.

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

NOTE

1. If NAT networking was used, you must re-configure the **ipmap.cfg** file after the OS is restarted. For details, see [A.9.36 How to Configure the ipmap.cfg Mapping File](#).
2. If NBIs and instances are deployed and the xFtp monitor is configured before the host name and IP address are changed, you must configure NBIs on the MSuite client and re-configure the xFtp monitor on the U2000 client after changing the IP address and host name.
 - For details about how to configure NBIs, see the related NBI user guide.
 - For details about how to configure the xFtp monitor, see the U2000 Help.

----End

A.9.12 How to Modify the Server IP Address of High Availability System (Windows)

Question

How do I to change the server IP address when the networking plan is changed?

**CAUTION**

If the server IP address or host name is changed, the previously backed up data cannot be used for restoration. In such a case, you need to back up the data again.

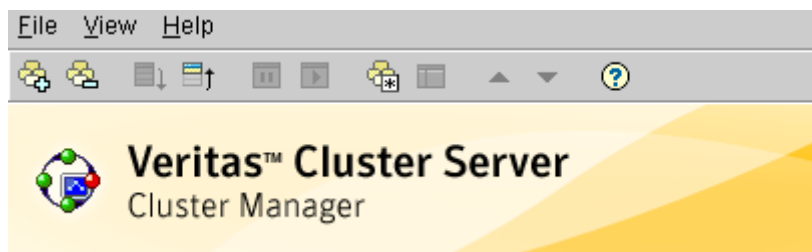
Do not change an IP address and a host name at the same time. Otherwise, the U2000 fails to be started.

Changing an IP address includes the following major steps:

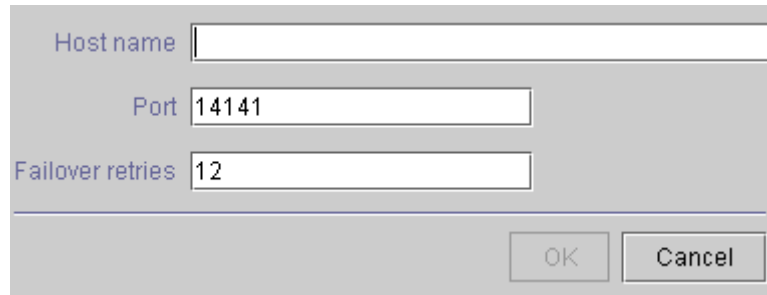
1. Separate the primary and secondary sites.
2. Shut down the U2000 server and client, and ensure that the database is running.
3. Shut down the U2000 MSuite server.
4. Change the IP address of the U2000 server.
5. Change the system IP address that is set in the VCS.
6. Start the U2000 MSuite server.
7. Log in to the U2000 MSuite client and synchronize IP address changes in configuration files. If the IP address changes are not synchronized, the U2000 fails to start properly.
8. Restart the OS.
9. Import the datadg disk group.
10. Synchronize the primary and secondary sites and reestablish their high availability relationship.

Answer

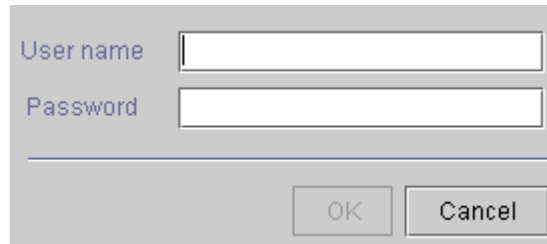
- 1 Log in to the NMS maintenance tool client. Choose **Deploy > Separate the primary and secondary sites**. The **Separate the primary and secondary sites** dialog box is displayed.
- 2 Click **OK**. The progress bar is displayed indicating the status of separating the primary and secondary sites. Wait until the dialog box is displayed indicating that the separation is complete.
- 3 Click **OK**.
- 4 On the primary site, perform the following operations to end the U2000 processes:
 1. Choose **Start > Programs > Symantec > Veritas Cluster Server > Veritas Cluster Manager - Java Console** to start the VCS client.



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



3. Enter the IP address of the system of the primary site. Then, click **OK**.



4. Enter the default user name **admin** and the default password **password** of the VCS client. Then, click **OK**.
5. Right-click **AppService** in the navigation tree and choose **Offline** > **host_name** from the shortcut menu.
6. In the dialog box that is displayed, click **Yes**.
- 5 Perform the following operations on the primary site to start the database:
 1. In the navigation tree, right-click **AppService-SQLServer2000**, and then choose **Online** > **host_name** from the shortcut menu.
 2. In the dialog box that is displayed, click **Yes**.
- 6 **Optional:** If the IP address is required to be changed on the secondary site, perform the preceding operations to start the database on the secondary site.
- 7 End the server process of the MSuite.

In the **C:\HWENGR\engineering** directory, double-click the **stopserver.bat** file to end the server process of the MSuite.
- 8 In the classic start menu mode, choose **Start** > **Settings** > **Network Connections**.
- 9 In the **Network Connections** dialog box that is displayed, right-click the network connection to be configured and choose **Properties** from the shortcut menu.
- 10 On the **General** tab page (for the local connection) or **Network** tab page (for all other connections), select **Internet Protocol (TCP/IP)**. Then, click **Properties**.
- 11 In the **Internet Protocol (TCP/IP) Properties** dialog box that is displayed, enter the new IP address, subnet mask, and default gateway address, and perform the related modification. Click **OK**.
- 12 Modify the system IP address in the VCS. Open the CLI and run the following commands:

```
C: \> haconf -makerw
```

```
C: \> haclus -modify ClusterAddress system IP address of the primary site
```

**NOTE**

When running the preceding commands on the secondary site, enter the system IP address of the secondary site.

C : \> **haconf -dump -makero**

- 13** Start the server process of the MSuite.

In the **C:\HWENGR\engineering** directory, double-click the **startserver.bat** file to start the server process of the MSuite.

- 14** Log in to the MSuite client.

1. On the computer where the MSuite client is installed, double-click the **U2000 MSuite** shortcut icon on the desktop. Wait about one minute. The **Login** dialog box is displayed.
2. Set the related login parameters and click **OK**. The **NMS maintenance suite** window is displayed.
 - **IP Address**: Indicates the system IP address of the computer where the MSuite server is installed.
 - **Port No.**: The default port number is **12212**. You do not need to change the default value during login.
 - **User Name and Password**: Both the default user name and default password are **admin**.

**NOTE**

A dialog box may be displayed during the process of logging in to the MSuite client. Click **OK** according to the prompt.

- 15** On the **Server** tab page, right-click the server to be configured and choose **Synchronize the network configuration** from the shortcut menu. Click **OK**.

- 16** Restart the OS.

- 17** After the OS is restarted, run the following command to import the disk group **datadg**:

C : \> **vx dg -g datadg -s import**

- 18** Choose **Deploy > Synchronize the primary and secondary sites** on the primary site. The **Synchronize the primary and secondary sites** dialog box is displayed.

- 19** Enter the IP address of the remote server.

**NOTE**

Here, **Remote IP** refers to the IP address of the secondary site.

- 20** Click **OK**. A progress bar is displayed indicating the synchronization progress between the primary and secondary sites. Wait approximately 20 minutes until a dialog box is displayed indicating that the synchronization is completed.

- 21** Click **OK**. The synchronization between the primary and secondary sites is complete.

----End

Postrequisite

 NOTE

If NBIs and instances are deployed and the xFtp monitor is configured before the IP address is changed, you must configure NBIs on the MSuite client and re-configure the xFtp monitor on the U2000 client after changing the IP address.

- For details about how to configure NBIs, see the related NBI user guide.
- For details about how to configure the xFtp monitor, see the U2000 Help.

A.9.13 How to Change the Host Name of the High Availability System (Windows)

Question

How do I change the host name of the high availability system (Windows)?



CAUTION

If the server IP address or host name is changed, the previously backed up data cannot be used for restoration. In such a case, you need to back up the data again.

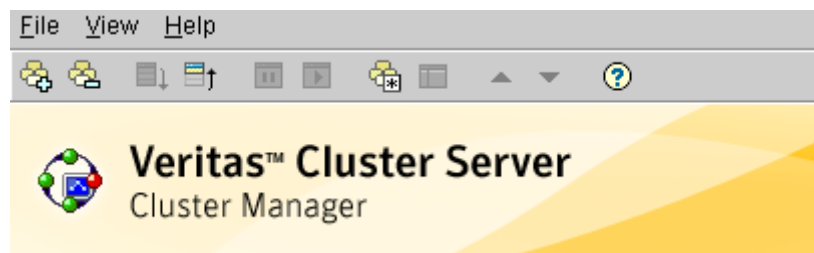
Do not change an IP address and a host name at the same time. Otherwise, the U2000 fails to be started.

Changing the host name includes the following major steps:

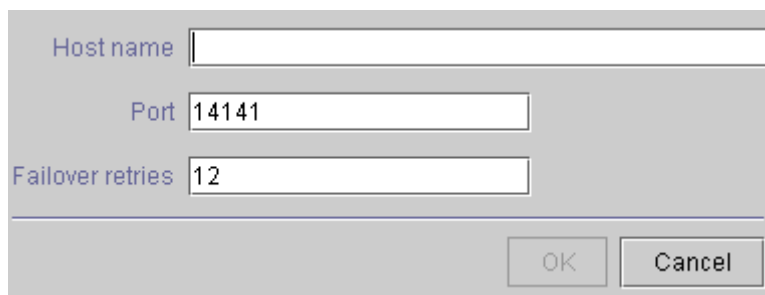
1. Shut down the U2000 server and client.
2. Stop the VCS service and communication.
3. Change the host name changes in configuration files.
4. Change the host name of the U2000 server.
5. Restart the OS.
6. Log in to the U2000 MSuite client and synchronize host name changes in configuration files. If the host name changes are not synchronized, the U2000 fails to start properly.

Answer

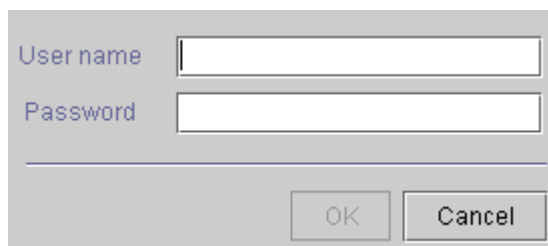
- 1 Log in to the OS as a user with administrator rights.
- 2 At the primary site, perform the following operations to end the U2000 processes:
 1. Choose **Start > Programs > Symantec > Veritas Cluster Server > Veritas Cluster Manager - Java Console** to start the VCS client.



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



3. Enter the IP address of the system of the primary site. Then, click **OK**.



4. Enter the default user name **admin** and the default password **password** of the VCS client. Then, click **OK**.
 5. Right-click **AppService** in the navigation tree and choose **Offline** > **host_name** from the shortcut menu.
 6. In the dialog box that is displayed, click **Yes**.
- 3 To stop the VCS service, run the following command on the server whose host name is to be changed:
- ```
C : \> hastop -all -force
```
- 4 To stop the VCS communication, run the following command on the server whose host name is to be changed:
- ```
C : \> net stop llt
```
- Enter **y** and press Enter at prompt.
- 5 Navigate to the **C:\Program Files\Veritas\comms\llt** path. Then, change the host name in the **llthosts.txt** file to a new one. You need to perform this step on the server whose host name is to be changed.
 - 6 Navigate to the **C:\Program Files\Veritas\comms\llt** path. Then, change the host name in the **llttab.txt** file to a new one. You need to perform this step on the server whose host name is to be changed.
 - 7 Navigate to the **C:\Program Files\Veritas\Cluster Server\conf** path. Then, change the host name in the **sysname** file to the new host name. You need to perform this step on the server whose host name is to be changed.
 - 8 Navigate to the **C:\Program Files\Veritas\cluster server\conf\config** path. Then, change the host name in the **main.cf** file to the new host name. You need to perform this step on the server whose host name is to be changed.
 - 9 Perform the following operations to change the host name of the server:
 1. On the desktop, right-click the **My Computer** icon and choose **Properties** from the shortcut menu.

2. In the dialog box that is displayed, click the **Computer Name** tab, and then click **Change**.
 3. In the dialog box that is displayed, change the computer name, and then click **OK**.
 4. Restart the OS.
- 10** Log in to the MSuite client.
1. On the computer where the MSuite client is installed, double-click the **U2000 MSuite** shortcut icon on the desktop. Wait about one minute. The **Login** dialog box is displayed.
 2. Set the related login parameters and click **OK**. The **NMS maintenance suite** window is displayed.
 - **IP Address:** Indicates the system IP address of the computer where the MSuite server is installed.
 - **Port No.:** The default port number is **12212**. You do not need to change the default value during login.
 - **User Name and Password:** Both the default user name and default password are **admin**.
-  **NOTE**
A dialog box may be displayed during the process of logging in to the MSuite client. Click **OK** according to the prompt.
- 11** On the **Server** tab page, right-click the server to be configured and choose **Synchronize the network configuration** from the shortcut menu. Click **OK**.
- 12** **Optional:** If the host name of the Veritas high availability system on the secondary site also needs to be changed, perform primary/secondary site switchover and then repeat the preceding steps to change the host name of the Veritas high availability system on the secondary site.
- End

A.9.14 How to Change the IP Address and Host name for the High Availability System (Solaris)

Question

How do I change the IP address and host name for the High Availability System (Solaris)?

Answer

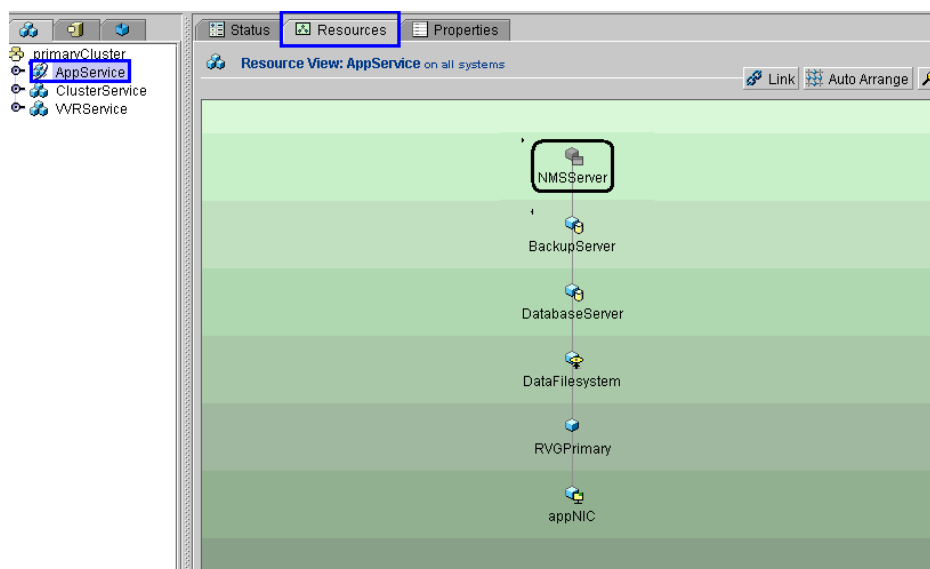
NOTE

To change the IP address and host name for the single-server system (Solaris), do as follows:

1. Use the MSuite to separate the primary site from the secondary site.
2. Log in to a VCS client and ensure that the **NMSServer** resource is in **offline** state and other resources are in **online** state on the primary site.
3. Use the MSuite to change the IP address and host name for the primary site. If a route is changed, reconfigure the route.
4. Restart the OS to make the modifications take effect.
5. Log in to a VCS client and ensure that the **NMSServer** resource is in **offline** state and other resources are in **online** state on the secondary site.
6. Use the MSuite to change the IP address and host name for the secondary site. If a route is changed, reconfigure the route.
7. Restart the OS to make the modifications take effect.
8. Use the MSuite to reconnect the primary and secondary sites.

- 1 **Log in to the MSuite of primary site.**
- 2 Separate the primary site from the secondary site. For details, see [D.6.2 Deleting the HA Relationship Between the Primary and Secondary Sites](#).
- 3 Log in to the VCS clients of the primary site. For details, see [A.4.3.2 How to Log in and Exit the VCS \(Veritas Cluster Server\)](#).
- 4 On the VCS client, choose **AppService > Resources** and ensure that the **NMSServer** resource of the primary site is in the **offline** state and other resources are in the **online** state.

Figure A-6 High Availability System (Solaris) resources



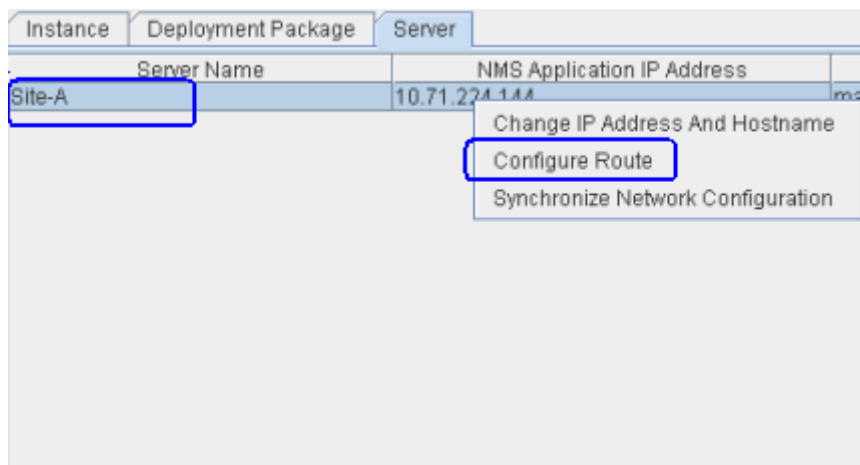
 NOTE

- Resources whose icons are grayed out are in the **offline** state. For example, the **NMSServer** resource in the preceding figure. Resources whose resource icons are not grayed out are in the **online** state. For example, the **BackupServer** resource in the preceding figure.
- Check the status of all resources and ensure that the **NMSServer** resource is in the **offline** state and other resources are in the **online** state.
- To make a resource online, right-click the resource and choose **online > hostname** from the shortcut menu. In the **Question** dialog box, click **Yes**.
- To make a resource offline, right-click the resource and choose **offline > hostname** from the shortcut menu. In the **Question** dialog box, click **Yes**.

5 On the MSuite client, click the **Server** tab.

6 If the route changes, do as follows to add a route. If the route does not change, you do not need to change the IP address or host name. Instead, skip this step.

- Right-click the server name and choose **Configure Route** from the shortcut menu.



- In the dialog box that is displayed, click **Add** or **Delete** according to actual route conditions to re-configure the route.

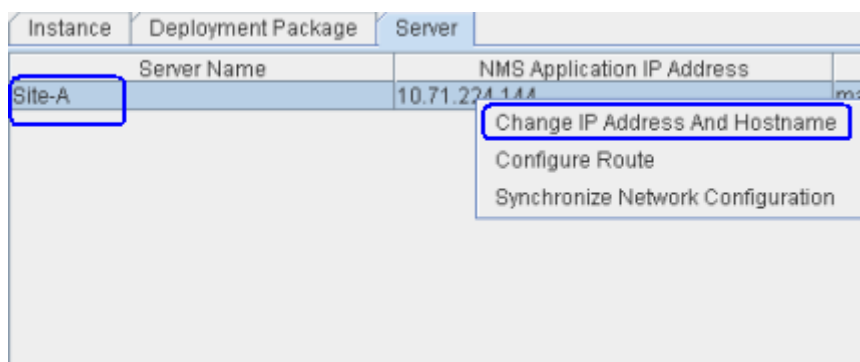
Destination	Subnet Mask	Route
0.0.0.0	0.0.0.0	10.71.224.1
10.71.224.0	255.255.254.0	10.71.224.144
127.0.0.1	255.255.255.255	127.0.0.1

Buttons: Add, Delete

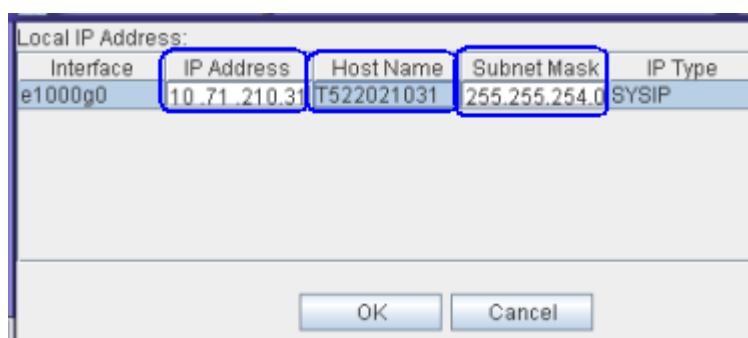
- Click **OK**.

7 Do as follows to change the host name and IP address.

- Right-click the server name and choose **Change IP Address And Hostname** from the shortcut menu.



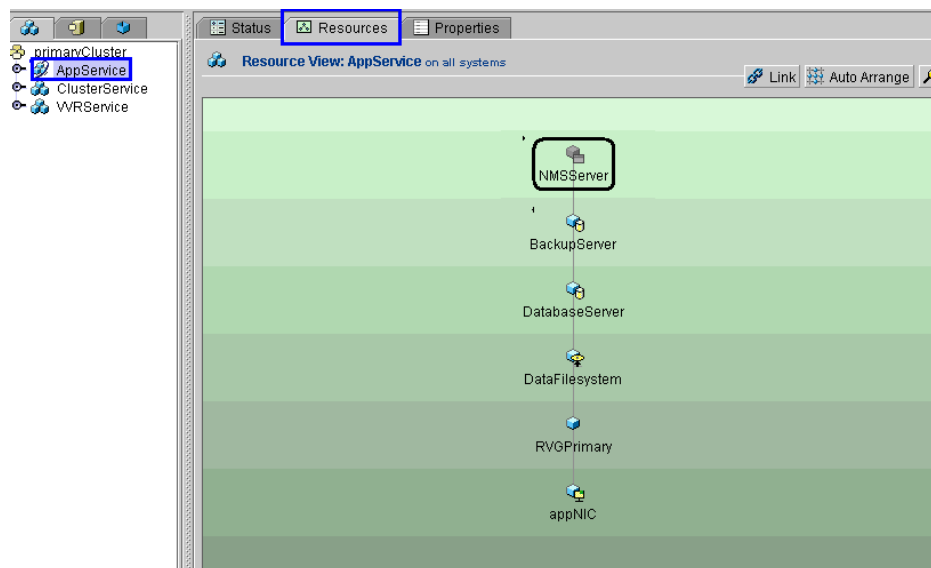
2. In the **Change IP Address And Hostname** dialog box, enter the new host name, IP address, and subnet mask.



3. Click **OK**. The progress bar is displayed. Wait patiently.
4. After the configuration is complete, the **Message** dialog box is displayed, asking you to restart the OS and back up the database in time. click **OK**.
- 8 Restart the OS of the server whose host name and IP address are changed for the settings to take effect.


```
# cd /opt/VRTSvcs/bin
# hstop -all -force
# sync;sync;sync;sync
# shutdown -y -g0 -i6
```
- 9 Log in to the VCS clients of the secondary site. For details, see [A.4.3.2 How to Log in and Exit the VCS \(Veritas Cluster Server\)](#).
- 10 On the VCS client, choose **AppService > Resources** and ensure that the **NMSServer** resource of the secondary site is in the **offline** state and other resources are in the **online** state.

Figure A-7 High Availability System (Solaris) resources



NOTE

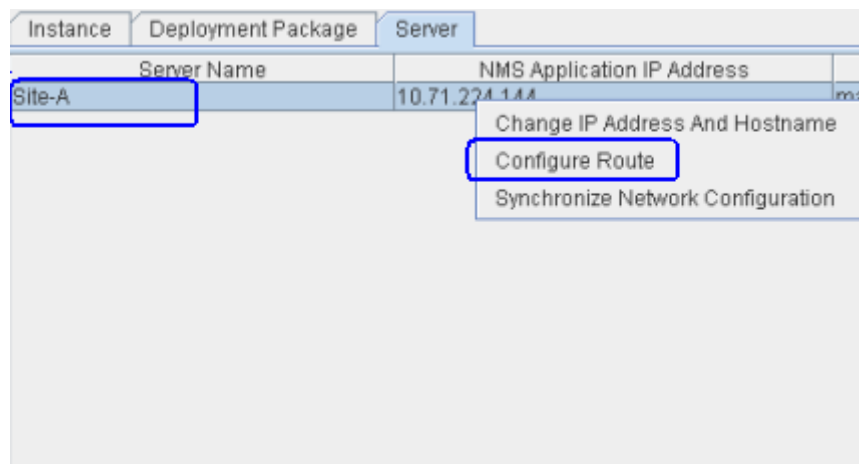
- Resources whose icons are grayed out are in the **offline** state. For example, the **NMSServer** resource in the preceding figure. Resources whose resource icons are not grayed out are in the **online** state. For example, the **BackupServer** resource in the preceding figure.
- Check the status of all resources and ensure that the **NMSServer** resource is in the **offline** state and other resources are in the **online** state.
- To make a resource online, right-click the resource and choose **online > hostname** from the shortcut menu. In the **Question** dialog box, click **Yes**.
- To make a resource offline, right-click the resource and choose **offline > hostname** from the shortcut menu. In the **Question** dialog box, click **Yes**.

11 Log in to the MSuite of secondary site.

12 On the MSuite client, click the **Server** tab.

13 If the route changes, do as follows to add a route. If the route does not change, you do not need to change the IP address or host name. Instead, skip this step.

- Right-click the server name and choose **Configure Route** from the shortcut menu.



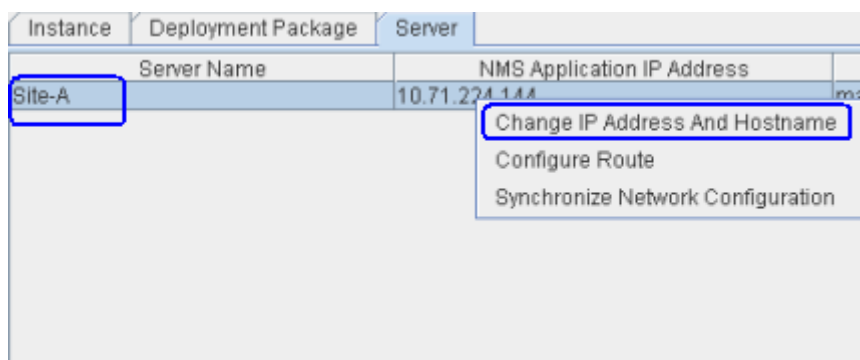
2. In the dialog box that is displayed, click **Add** or **Delete** according to actual route conditions to re-configure the route.

Destination	Subnet Mask	Route
0.0.0.0	0.0.0.0	10.71.224.1
10.71.224.0	255.255.254.0	10.71.224.144
127.0.0.1	255.255.255.255	127.0.0.1

3. Click **OK**.

14 Do as follows to change the host name and IP address.

1. Right-click the server name and choose **Change IP Address And Hostname** from the shortcut menu.



2. In the **Change IP Address And Hostname** dialog box, enter the new host name, IP address, and subnet mask.

Local IP Address:				
Interface	IP Address	Host Name	Subnet Mask	IP Type
e1000g0	10.71.210.31	T522021031	255.255.254.0	SYSIP

3. Click **OK**. The progress bar is displayed. Wait patiently.
 4. After the configuration is complete, the **Message** dialog box is displayed, asking you to restart the OS and back up the database in time. click **OK**.
- 15** Restart the OS of the server whose host name and IP address are changed for the settings to take effect.

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

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

- 16 Log in to the OS of the primary site as the **root** user.
- 17 Connect the primary and secondary sites. For details, see [D.6.1 Establishing the HA Relationship Between the Primary and Secondary Sites](#).

 NOTE

If NBIs and instances are deployed and the xFtp monitor is configured before the host name and IP address are changed, you must configure NBIs on the MSuite client and re-configure the xFtp monitor on the U2000 client after changing the IP address and host name.

- For details about how to configure NBIs, see the related NBI user guide.
- For details about how to configure the xFtp monitor, see the U2000 Help.

----End

A.9.15 How to Change the IP Address and Host Name of the High Availability System (SUSE Linux-Distributed)

Question

How do I change the IP address and host name of the High Availability System (SUSE Linux-Distributed)?

Answer

 NOTE

To change the IP address and host name for the single-server system (Solaris), do as follows:

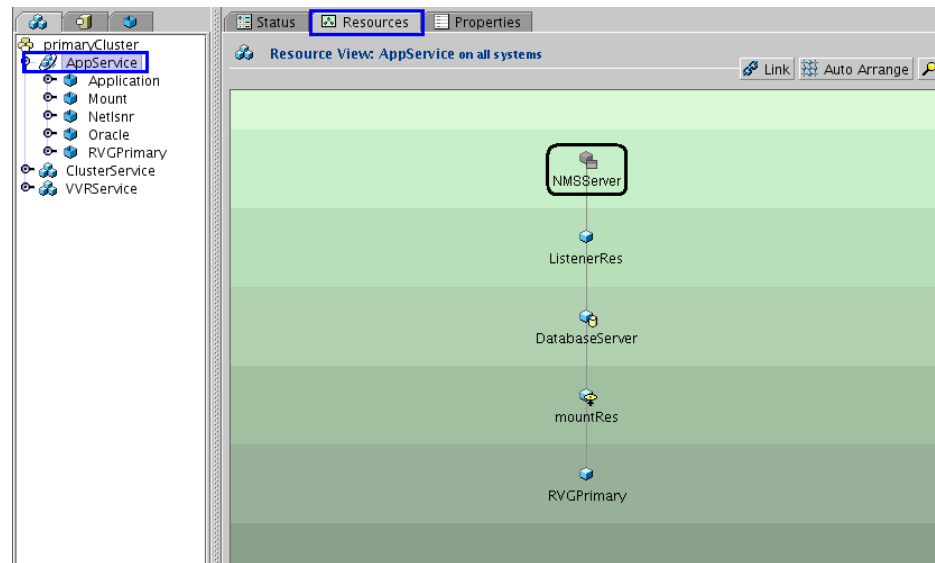
1. Use the MSuite to separate the primary site from the secondary site.
2. Log in to a VCS client and ensure that the **NMSServer** resource is in **offline** state and other resources are in **online** state on the primary site.
3. Use the MSuite to change the IP address and host name for the primary site. If a route is changed, reconfigure the route.
4. Restart the OS to make the modifications take effect.
5. Log in to a VCS client and ensure that the **NMSServer** resource is in **offline** state and other resources are in **online** state on the secondary site.
6. Use the MSuite to change the IP address and host name for the secondary site. If a route is changed, reconfigure the route.
7. Restart the OS to make the modifications take effect.
8. Use the MSuite to reconnect the primary and secondary sites.

- 1 [Log in to the MSuite client of the master server the primary site](#)

 NOTE

The IP address entered during login is the system IP address of the master server of the primary site.

- 2 Separate the primary site from the secondary site. For details, see [D.6.2 Deleting the HA Relationship Between the Primary and Secondary Sites](#).
- 3 Log in to the VCS clients of the primary site. For details, see [A.4.3.2 How to Log in and Exit the VCS \(Veritas Cluster Server\)](#).
- 4 On the VCS client, choose **AppService > Resources** and ensure that the **NMSServer** resource of the primary site is in the **offline** state and other resources are in the **online** state.

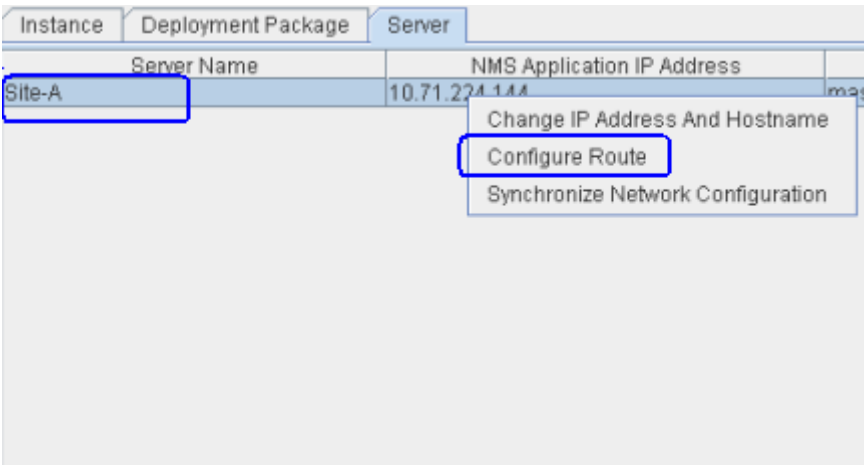
Figure A-8 High Availability System (SUSE Linux-Distributed) resources**NOTE**

- Resources whose icons are grayed out are in the **offline** state. For example, the **NMSServer** resource in the preceding figure. Resources whose resource icons are not grayed out are in the **online** state. For example, the **BackupServer** resource in the preceding figure.
 - Check the status of all resources and ensure that the **NMSServer** resource is in the **offline** state and other resources are in the **online** state.
 - To make a resource online, right-click the resource and choose **online > hostname** from the shortcut menu. In the **Question** dialog box, click **Yes**.
 - To make a resource offline, right-click the resource and choose **offline > hostname** from the shortcut menu. In the **Question** dialog box, click **Yes**.
- 5 Log in to the slave server as user **root**. Open a terminal window and run the following command to end the **daem** process of the slave server:
- ```
/etc/init.d/u2kdaem stop
```

**CAUTION**

There must be a space between the dot (.) and **svc\_profile.sh**.

- 6 On the MSuite client, click the **Server** tab.
- 7 If the route changes, do as follows to add a route. If the route does not change, you do not need to change the IP address or host name. Instead, skip this step.
1. Right-click the server name and choose **Configure Route** from the shortcut menu.



2. In the dialog box that is displayed, click **Add** or **Delete** according to actual route conditions to re-configure the route.

| Destination | Subnet Mask     | Route         |
|-------------|-----------------|---------------|
| 0.0.0.0     | 0.0.0.0         | 10.71.224.1   |
| 10.71.224.0 | 255.255.254.0   | 10.71.224.144 |
| 127.0.0.1   | 255.255.255.255 | 127.0.0.1     |

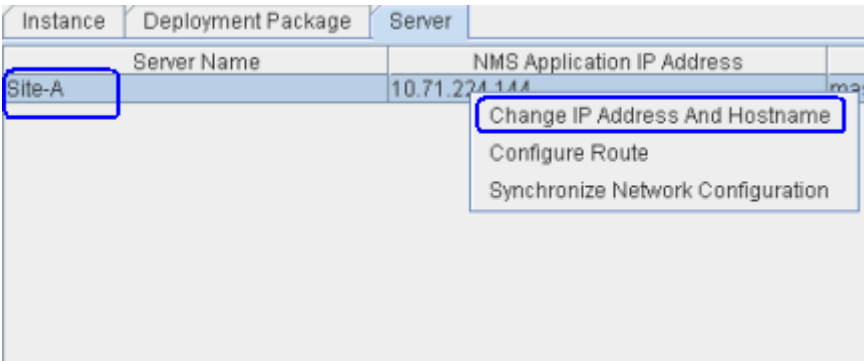
Add

Delete

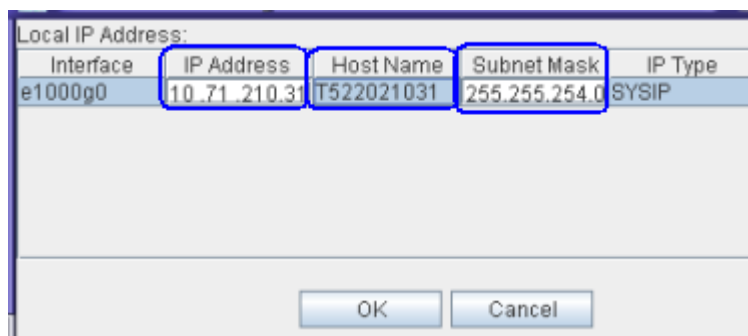
3. Click **OK**.

8 Do as follows to change the host name and IP address.

1. Right-click the server name and choose **Change IP Address And Hostname** from the shortcut menu.



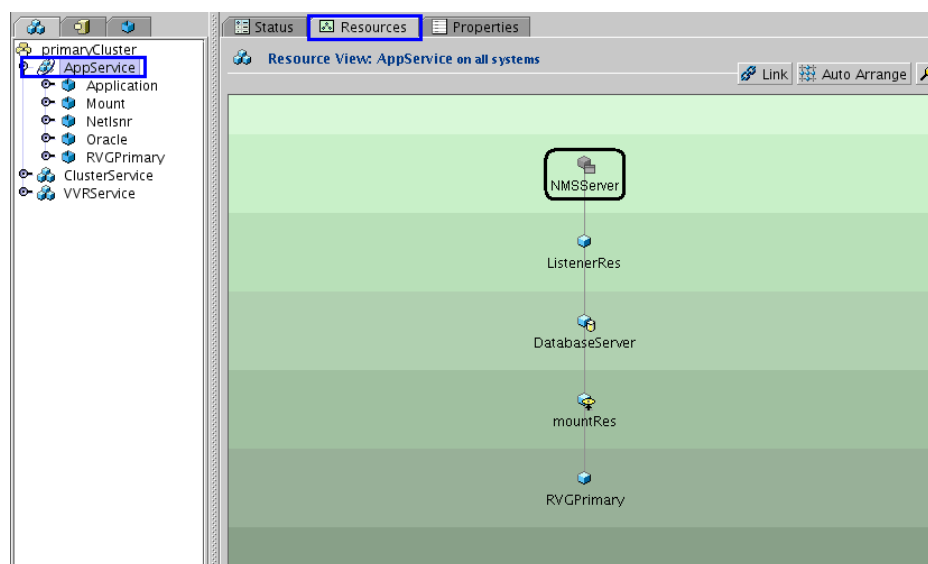
2. In the **Change IP Address And Hostname** dialog box, enter the new host name, IP address, and subnet mask.



3. Click **OK**. The progress bar is displayed. Wait patiently.
4. After the configuration is complete, the **Message** dialog box is displayed, asking you to restart the OS and back up the database in time. click **OK**.
- 9 Restart the OS of the server whose host name and IP address are changed for the settings to take effect.
 

```
cd /opt/VRTSvcs/bin
hstop -all -force
sync;sync;sync;sync
shutdown -r now
```
- 10 Log in to the VCS clients of the secondary site. For details, see [A.4.3.2 How to Log in and Exit the VCS \(Veritas Cluster Server\)](#).
- 11 On the VCS client, choose **AppService > Resources** and ensure that the **NMSServer** resource of the secondary site is in the **offline** state and other resources are in the **online** state.

**Figure A-9** High Availability System (SUSE Linux-Distributed) resources





 **NOTE**

- Resources whose icons are grayed out are in the **offline** state. For example, the **NMSServer** resource in the preceding figure. Resources whose resource icons are not grayed out are in the **online** state. For example, the **BackupServer** resource in the preceding figure.
- Check the status of all resources and ensure that the **NMSServer** resource is in the **offline** state and other resources are in the **online** state.
- To make a resource online, right-click the resource and choose **online > hostname** from the shortcut menu. In the **Question** dialog box, click **Yes**.
- To make a resource offline, right-click the resource and choose **offline > hostname** from the shortcut menu. In the **Question** dialog box, click **Yes**.

- 12** Log in to the slave server as user **root**. Open a terminal window and run the following command to end the **daem** process of the slave server:

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



**CAUTION**

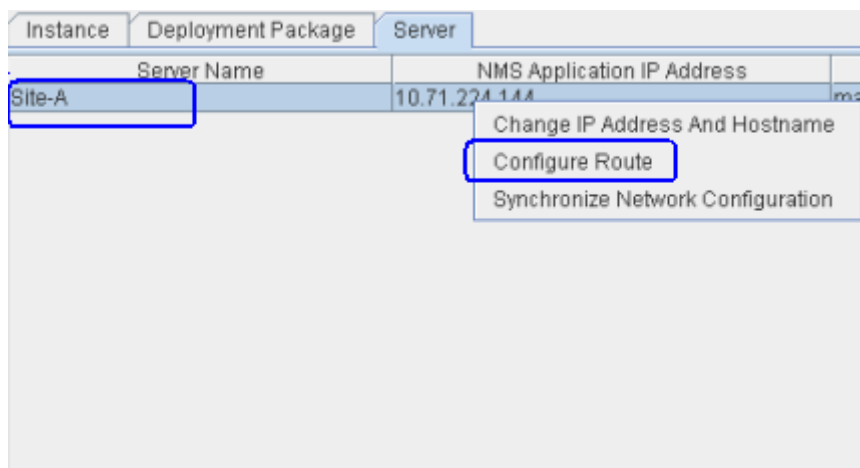
There must be a space between the dot (.) and **svc\_profile.sh**.

- 13** [Log in to the MSuite client of the master server the secondary site.](#)

 **NOTE**

The IP address entered during login is the system IP address of the master server of the primary site.

- 14** On the MSuite client, click the **Server** tab.
- 15** If the route changes, do as follows to add a route. If the route does not change, you do not need to change the IP address or host name. Instead, skip this step.
- Right-click the server name and choose **Configure Route** from the shortcut menu.



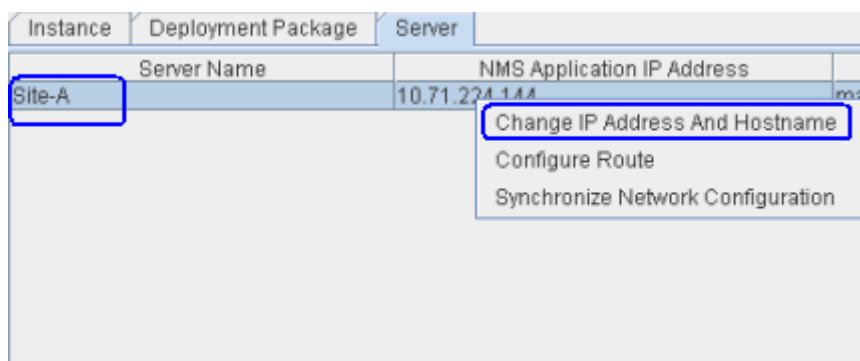
- In the dialog box that is displayed, click **Add** or **Delete** according to actual route conditions to re-configure the route.

| Destination | Subnet Mask     | Route         |
|-------------|-----------------|---------------|
| 0.0.0.0     | 0.0.0.0         | 10.71.224.1   |
| 10.71.224.0 | 255.255.254.0   | 10.71.224.144 |
| 127.0.0.1   | 255.255.255.255 | 127.0.0.1     |

3. Click **OK**.

**16** Do as follows to change the host name and IP address.

1. Right-click the server name and choose **Change IP Address And Hostname** from the shortcut menu.



2. In the **Change IP Address And Hostname** dialog box, enter the new host name, IP address, and subnet mask.

Local IP Address:

| Interface | IP Address   | Host Name  | Subnet Mask   | IP Type |
|-----------|--------------|------------|---------------|---------|
| e1000g0   | 10.71.210.31 | T522021031 | 255.255.254.0 | SYSIP   |

3. Click **OK**. The progress bar is displayed. Wait patiently.
4. After the configuration is complete, the **Message** dialog box is displayed, asking you to restart the OS and back up the database in time. click **OK**.

**17** Restart the OS of the server whose host name and IP address are changed for the settings to take effect.

```
cd /opt/VRTSvcs/bin
hastop -all -force
sync;sync;sync;sync
shutdown -r now
```

18 Log in to the OS of the master server of primary site as **root** user.

19 [Log in to the MSuite client of the master server the primary site](#)



**NOTE**

The IP address entered during login is the system IP address of the master server of the primary site.

20 Connect the primary and secondary sites. For details, see [D.6.1 Establishing the HA Relationship Between the Primary and Secondary Sites](#).



**NOTE**

1. If NAT networking was used, you must re-configure the **ipmap.cfg** file after the OS is restarted. For details, see [A.9.36 How to Configure the ipmap.cfg Mapping File](#).
2. If NBIs and instances are deployed and the xFtp monitor is configured before the host name and IP address are changed, you must configure NBIs on the MSuite client and re-configure the xFtp monitor on the U2000 client after changing the IP address and host name.
  - For details about how to configure NBIs, see the related NBI user guide.
  - For details about how to configure the xFtp monitor, see the U2000 Help.

----End

## A.9.16 How to Verify That the Processes of the U2000 Single-Server System Are Running on Windows

### Question

How do I verify that the processes of the U2000 single-server system are running on Windows?

### Answer

- 1 Log in to the OS as a user with **administrator** rights. The system automatically starts the database and U2000 service.
- 2 Choose **Start > Programs > Network Management System > U2000 System Monitor** or double-click the associated shortcut icon on the desktop to start the System Monitor.
- 3 In the **Login** dialog box, enter a user name and password to access the System Monitor window. The user name is **admin** and the initial password is blank by default. When you log in to the System Monitor for the first time, you must change the initial password.
- 4 Check whether U2000 processes can be properly started. The processes whose startup mode is **manual** must be started manually.

----End

## A.9.17 How to Start the Processes of the U2000 Single-Server System on Windows

### Question

How do I start the processes of the U2000 single-server system (Windows)?

## Answer

- 1 Log in to the OS as a user with **administrator** rights. The system automatically starts the database and U2000 service.
- 2 If the database does not automatically start along with the OS, run the following command to manually start it.

Choose **Start > Programs > Microsoft SQL Server > Enterprise Manager**, and click **Start/Continue** to start the database. If the database has started, skip this step.

- 3 Manually start the U2000 processes.

You can run the **startnms.bat** file in the U2000 installation directory **\server\bin**.

----End

## A.9.18 How to End the Processes of the U2000 Single-Server System on Windows

### Question

How do I end the processes of the U2000 single-server system on Windows?



### CAUTION

You can stop all the services of the NMS, including the system monitoring process.

If you use the **Stop All NMS Services** function of the System Monitor, the system monitoring process is not ended. Do not use this method if perform operations for shutting down the NMS that are associated with the database.

---

## Answer

- 1 Exit all the U2000 clients.
- 2 End the NMS processes.

In the directory of the NMS software after the installation, for example, the **D:\U2000\server\bin** directory, run the **stopnms.bat** file to end the NMS processes.

----End

## A.9.19 How to Verify That the Processes of the U2000 Single-Server System Are Running on Solaris

### Question

How do I verify that the processes of the U2000 single-server system are running on Solaris?

## Answer

- 1 Log in to the server as user **nmsuser**.
- 2 Check the U2000 processes.

Run the following command to check whether the U2000 is running:

```
$ daem_ps
```

Information similar to the following is displayed:

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

### NOTE

The U2000 is running if the displayed information contains **imap\_sysmonitor -cmd start**.

----End

## A.9.20 How to Start the Processes of the U2000 Single-Server System on Solaris

### Question

How do I start the processes of the U2000 single-server system on Solaris?

### Answer

- 1 Log in to the server as user **nmsuser**.
- 2 Ensure that the U2000 is running.

Run the following command to check whether the U2000 is running:

```
$ daem_ps
```

Information similar to the following is displayed:

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

### NOTE

The U2000 is running if the displayed information contains **imap\_sysmonitor -cmd start**.

Run the following command to start the U2000 if it is not running:

```
$ cd /opt/U2000/server/bin
$./startnms.sh
```

----End

## A.9.21 How to End the Processes of the U2000 Single-Server System on Solaris

### Question

How do I end the processes of the U2000 single-server system on Solaris?

### Answer

- 1 Log in to the server as user **nmsuser**.
- 2 Ensure that the U2000 is not running:

To check the running status of the U2000 process, run the following command:

```
$ daem_ps
```

Information similar to the following is displayed:

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



#### NOTE

The U2000 is running if the displayed information contains **imap\_sysmonitor -cmd start**.

Run the following commands to stop U2000 if it is running:

```
$ cd /opt/U2000/server/bin
$./stopnms.sh
```

----End

## A.9.22 How to Verify That the Processes of the U2000 Single-Server System (SUSE Linux-Distributed) Are Running

### Question

How do I verify that processes of the U2000 single-server system (SUSE Linux-distributed) are running?

### Answer

- 1 Log in to the master server as user **nmsuser**.
- 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/imapmr
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

## A.9.23 How to Start the Processes of the U2000 Single-Server System (SUSE Linux-Distributed)

### Question

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

### Answer

- 1 Log in to the master server as user **root**.
- 2 On the master server, start U2000 server processes.

1. To check whether U2000 server processes have been 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 27069 1 0 10:31:39 ? 1:39 imapmr
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**

The U2000 is running if the displayed information contains **imap\_sysmonitor -cmd start**.

2. If the U2000 processes are not started, run the following command to start U2000 processes:

```
cd /opt/U2000/server/bin
./startnms.sh
```

----End

## A.9.24 How to End the Processes of the U2000 Single-Server System (SUSE Linux-Distributed)

### Question

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

## Answer

- 1 Log in to the master server as user **root**.
- 2 Run the following commands to stop the U2000:

```
cd /opt/U2000/server/bin
./stopnms.sh
```

----End

## A.9.25 How to Check Whether the U2000 Processes of the High Availability System (Windows) Are Started

### Question

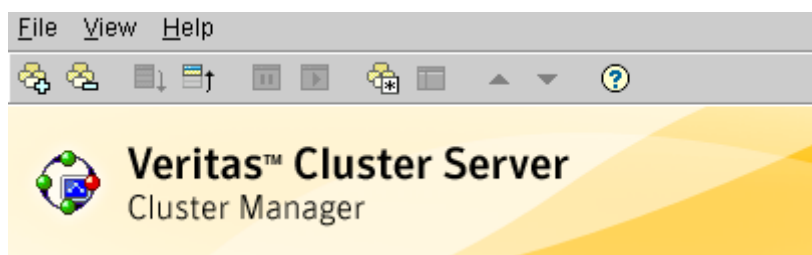
How to check whether the U2000 processes of the high availability system (Windows) are started?

#### NOTE

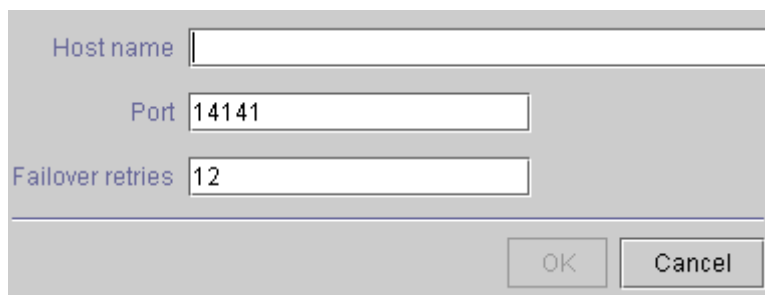
In normal cases, the U2000 processes of the primary site are started but those of the secondary site are not started.

## Answer

- 1 Log in to the OS as a user with administrator rights.
- 2 Start the VCS client.
  1. Choose **Start > Programs > Symantec > Veritas Cluster Server > Veritas Cluster Manager - Java Console** to start the VCS client.

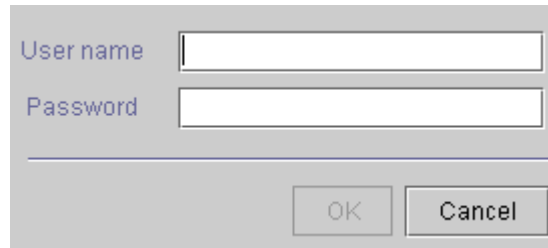


2. Choose **File > New Cluster**. A dialog box is displayed, as shown in the following figure.



3. Enter the IP address of the system of the primary site. Then, click **OK**.





4. Enter the default user name **admin** and the default password **password** of the VCS client. Then, click **OK**.
- 3 Select the **AppService** resource group from the navigation tree and check whether resources on the **Resource** tab page are started.

----End

## A.9.26 How to Start the U2000 Processes of the High Availability System (Windows)

### Question

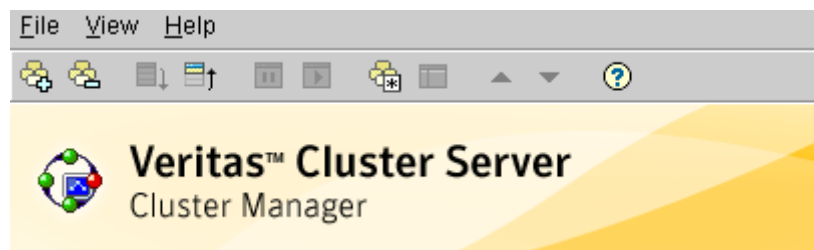
How to start the U2000 processes of the high availability system (Windows)?

#### NOTE

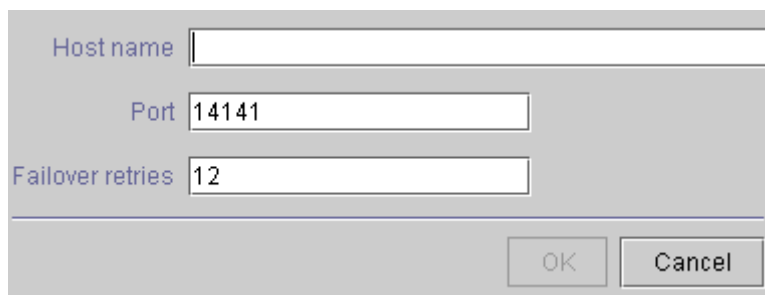
In normal cases, the U2000 processes of the primary site are started but those of the secondary site are not started.

### Answer

- 1 Log in to the OS as a user with **administrator** rights. The system automatically starts the database and U2000 service.
- 2 If the database and U2000 processes do not automatically start along with the OS, run the following command to manually start them:
  1. Choose **Start > Programs > Symantec > Veritas Cluster Server > Veritas Cluster Manager - Java Console** to start the VCS client.

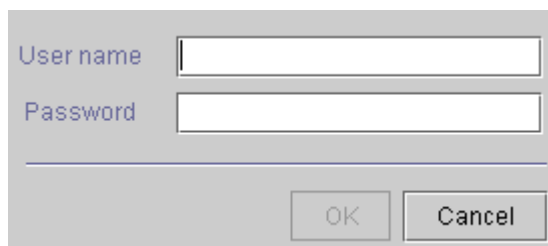


2. Choose **File > New Cluster**. A dialog box is displayed, as shown in the following figure.



A dialog box with a light gray background. It contains three input fields: 'Host name' (empty), 'Port' (containing '14141'), and 'Failover retries' (containing '12'). At the bottom right are 'OK' and 'Cancel' buttons.

3. Enter the IP address of the system of the primary site. Then, click **OK**.



A dialog box with a light gray background. It contains two input fields: 'User name' (empty) and 'Password' (empty). At the bottom right are 'OK' and 'Cancel' buttons.

4. Enter the default user name **admin** and the default password **password** of 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**.

----End

## A.9.27 How to End the U2000 Processes of the High Availability System (Windows)

### Question

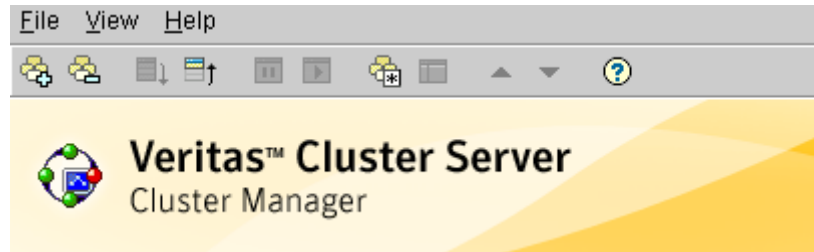
How do I end the U2000 processes of the high availability system (Windows)?

#### NOTE

In normal cases, the U2000 processes of the primary site are started but those of the secondary site are not started.

### Answer

- 1 Log in to the OS as a user with administrator rights.
- 2 End the U2000 processes of the Veritas high availability system.
  1. Choose **Start** > **Programs** > **Symantec** > **Veritas Cluster Server** > **Veritas Cluster Manager - Java Console** to start the VCS client.



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

3. Enter the IP address of the system of the primary site. Then, click **OK**.

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

----End

## A.9.28 How to Check Whether the U2000 Processes of the High Availability System (Solaris) Are Started

### Question

How to check whether the U2000 processes of the high availability system (Solaris) are started?

### Answer

- 1 Log in to the OS of the active site as the **nmsuser** user.
- 2 Check the U2000 processes.

Run the following command to check whether the U2000 is running:

```
$ daem_ps
```

Information similar to the following is displayed:

```

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

```

**NOTE**

The U2000 is running if the displayed information contains **imap\_sysmonitor -cmd start**.

----End

## A.9.29 How to Start the U2000 Processes of the High Availability System (Solaris)

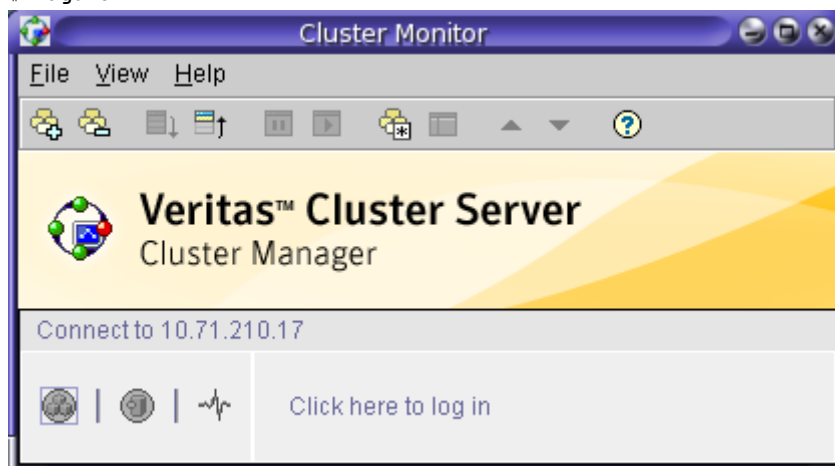
### Question

How do I start the U2000 processes of the high availability system (Solaris)?

### Answer

- 1 Log in to the OS of the primary site as user **root**.
- 2 Log in to the VCS.
  1. Open a terminal window, run the following command:

```
haGUI &
```

**NOTE**

If the login window fails to be displayed and the terminal displays a message indicating that the current status is "STALE\_ADMIN\_WAIT", run the **# hasys -force host name of node** command.

2. Click **Connect to Cluster name**.

**NOTE**

If you are logging in to the VCS for the first time, you need to create a new Cluster.

- a. Click **File > New Cluster**.
- b. Enter the IP address of application network.
- c. Click **OK**.
3. Enter *User Name* and *Password*.

 **NOTE**

The default user name of the VCS is **admin** and the password is **password**. For system security, modify the password and remember the new password.

- 3 In the **Cluster Explorer** window, right-click the **AppService** resource group in the navigation tree and choose **Online > primary** from the shortcut menu to start the Sybase process and U2000 server process.

 **TIP**

Click the **Resources** tab to view the start status of each resource.

Normally, on the **Status** tab page, **Online** is displayed for **State** in the **Group Status on Member Systems** area on the active site, and **Online on primary** is displayed for **Status** in the **Resource Status** area.

 **NOTE**

- In actual configuration, use the actual host name.
- If a fault has occurred during start of the AppService process, right-click **AppService** and choose **clear fault** from the shortcut menu to clear the fault. Then, choose **Online > host\_name** to start the AppService process.

- 4 In the dialog box that is displayed, click **Yes**.

----End

## A.9.30 How to End the U2000 Processes of the High Availability System (Solaris)

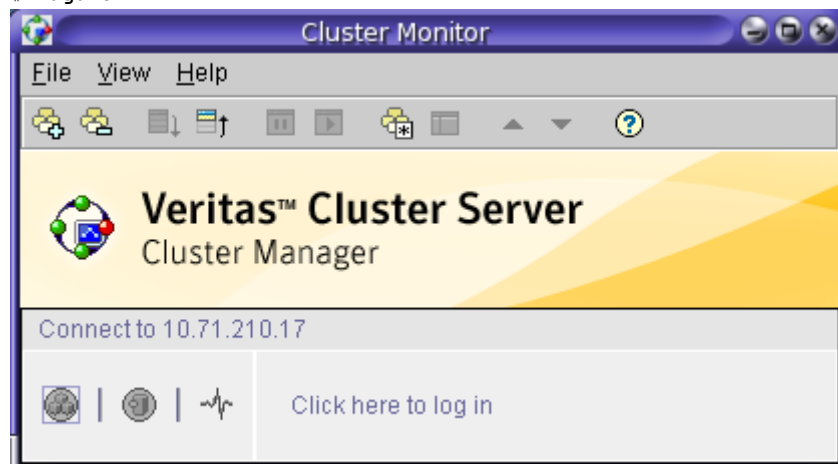
### Question

How do I end the U2000 processes of the high availability system (Solaris)?

### Answer

- 1 Log in to the OS of the active site as the **root** user.
- 2 Log in to the VCS.
  1. Open a terminal window, run the following command:

```
haguic
```



 **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

## A.9.31 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/imapmr
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

## A.9.32 How to Start the U2000 Processes of the High Availability System (SUSE Linux-Distributed)

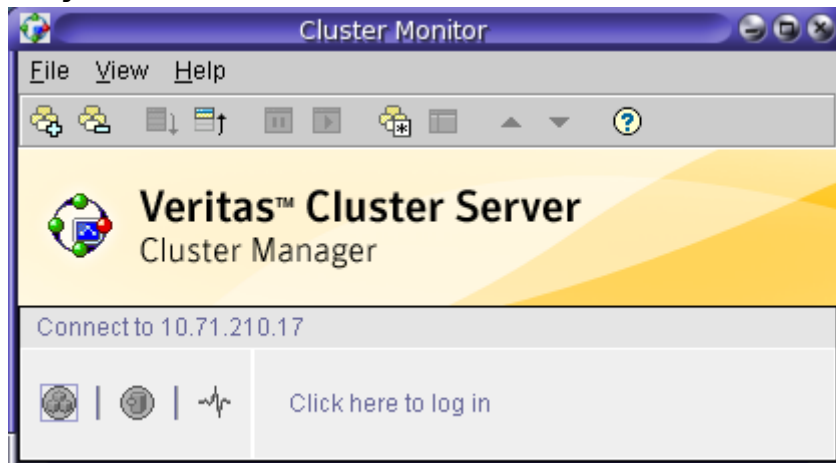
### Question

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:

```
hagu i &
```



 **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

## A.9.33 How to End the U2000 Processes of the High Availability System (SUSE Linux-Distributed)

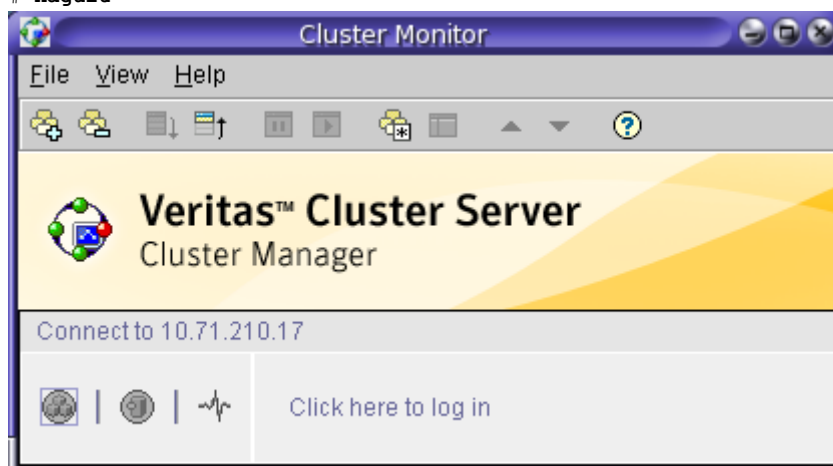
### Question

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:

```
haguic
```

 **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

## A.9.34 What Factors Affect the Response Speed of the NMS

### Question

What factors affect the response speed of the NMS?

### Answer

- 1 Number of gateway NEs and number of NEs managed by a gateway NE.
- 2 Status of the communication between the NMS and gateway NEs.
- 3 Scale of ECC subnetworks.
- 4 Hardware configurations of the U2000 server.
- 5 Management capability of the U2000 server.

----End

## A.9.35 How to Resolve the Problem Wherein Illegible Characters Occur in the NMS Window

### Question

How do I resolve the problem that illegible characters occur in the NMS window?

### Answer

- 1 The possible causes are as follows:
  - Illegible characters may occur when multiple NMSs of different languages manage the same NE.
  - If the character set is modified by means of commands on the NE side, illegible characters may occur when you query the information about the NE on the NMS.

- If the character set is configured after the NE is upgraded, illegible characters may occur when you query the information about the NE on the NMS.

In any of the preceding cases, the problem can be resolved after you restore the original character set.

----End

## A.9.36 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 A-8** 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

## A.9.37 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

In the single-server system: The U2000 is installed based on the bill of material (BOM).

- If the U2000 license BOM is available, the U2000 needs to be installed according to the license BOM. Technical support engineers should change the IP address, install the license on the U2000, and then use the U2000.
- If the U2000 license BOM is unavailable, only the OS needs to be installed.

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.

## A.9.38 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 imapmr
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

## A.9.39 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

## A.9.40 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

## A.9.41 How to Rectify the Application GUI Startup Failure Caused by User Switching

### Question

After a user logs in to the graphical desktop system as user **root** and runs the **su - nmsuser** command to switch to user **nmsuser**, applications such as the NMS maintenance suite client, U2000 client, and U2000 System Monitor client fail to start. How do I rectify this fault?

### Answer

- 1 Use either of the following methods to rectify the fault.
  - Method 1: Log out of the graphical desktop system and then log in as user **nmsuser**. Then, start an application in the desktop system.
  - Method 2: Perform the following operations in the current window:
    1. Run the following command to switch back to user **root**:  

```
$ exit
```

 **NOTE**  
The command prompt for user **root** is **#**. If **#** is not displayed after you run the **exit** command, run the **exit** command again.
    2. Run the following command to check the **DISPLAY** variable of user **root**. Then, record the value of the **DISPLAY** variable.  

```
echo $DISPLAY
```
    3. Run the following commands to switch to user **nmsuser** and set the **DISPLAY** variable.  

```
xhost +
su - nmsuser
$ export DISPLAY=DISPLAY value
```

 **NOTE**  
In the preceding command, **DISPLAY value** is the recorded value of the **DISPLAY** variable.
    4. Run the appropriate command to start the application.

----End

## A.9.42 How to Rectify the U2000 Startup Failure After the IP Address or Host Name of the Single-Server System (Solaris) Is Changed Manually

### Question

If the IP address or host name of the Single-Server System (Solaris) is changed not by following steps described in [A.9.10 How to Change the IP Address and Host Name for the Single-Server System \(Solaris\)](#) but in manual mode, the U2000 fails to start. How do I rectify this fault?

### Answer

- 1 Log in to the OS as user **root**.
- 2 Change the IP address recorded in the Sybase database.

Run the **vi** command to modify the **interfaces** configuration file and change the IP address to the new IP address.

```
su - sybase
$ vi /opt/sybase/interfaces
```

### 3 Restart the Sybase database.

1. To stop the database service manually, run the following commands:

```
$ cd /opt/sybase/OCS*/bin
$./isql -SDBSVR -Usa -P<sa password>
```

#### NOTE

<sa password> is the password of user **sa** of the Sybase database.

```
1> shutdown SYB_BACKUP
2> go
1> shutdown
2> go
```

2. To start the Sybase database, run the following commands:

```
$ cd /opt/sybase/ASE*/install
$./startserver -f ./RUN_DBSVR &
$./startserver -f ./RUN_DBSVR_back &
```

Run the following command to check whether the Sybase database is started:

```
$./showserver
```

If the displayed message contains `/opt/sybase/ASE-15_0/install/RUN_DBSVR` and `/opt/sybase/ASE-15_0/install/RUN_DBSVR_back`, the database is already started.

### 4 Synchronize network configurations by using the MSuite.

1. Log in to the MSuite client.
2. On the MSuite client, click the **Server** tab.
3. Right-click the server whose network configurations need to be synchronized and choose **Synchronize Network Configuration** from the shortcut menu. A dialog box is displayed for you to confirm the operation.
4. Click **OK**. A progress bar showing the synchronization progress is displayed.
5. When the system displays the message "Synchronize network configuration success", click **OK**.

----End

## A.9.43 How to Rectify the U2000 Startup Failure Because the IP Address or Host Name of the Single-Server System (SUSE Linux-Distributed) Is Changed Manually

### Question

If the IP address or host name of the Single-Server System (SUSE Linux-Distributed) is changed not by following steps described in [A.9.11 How to Change the IP Address and Host Name of the Single-Server System \(SUSE Linux-Distributed\)](#) but in manual mode, the U2000 fails to start. How do I rectify this fault?

## Answer

- 1 To check and record the host name, run the following command:

```
hostname
```

- 2 To check whether the IP address or host name recorded in the **listener.ora** file in the **/opt/oracle/oradb/home/network/admin** path is changed, run the following command:

```
more /opt/oracle/oradb/home/network/admin/listener.ora
```

The following message will be displayed:

```
LISTENER =
 (DESCRIPTION_LIST =
 (DESCRIPTION =
 (ADDRESS = (PROTOCOL = IPC) (KEY = EXTPROC1521))
 (ADDRESS = (PROTOCOL = TCP) (HOST = Masterserver) (PORT = 1521))
)
)
```

### NOTE

- If the host name recorded in "HOST = **Masterserver**" is different from the current host name, run the **vi** command to change the host name in the **listener.ora** file to the current host name.
- If the host name recorded in "HOST = **Masterserver**" is the same as the current host name, proceed to next step.

- 3 To check whether the IP address or host name recorded in the **tnsnames.ora** file in the **/opt/oracle/oradb/home/network/admin** path is changed, run the following command:

```
more /opt/oracle/oradb/home/network/admin/tnsnames.ora
```

The following message will be displayed:

```
U2KDB =
 (DESCRIPTION =
 (ADDRESS = (PROTOCOL = TCP) (HOST = Masterserver) (PORT = 1521))
 (CONNECT_DATA =
 (SERVER = DEDICATED)
 (SERVICE_NAME = U2KDB)
)
)
```

### NOTE

- If the host name recorded in "HOST = **Masterserver**" is different from the current host name, run the **vi** command to change the host name in the **listener.ora** file to the current host name.
- If the host name recorded in "HOST = **Masterserver**" is the same as the current host name, proceed to next step.

- 4 Perform the following operations to check whether the database is running:

To check whether the Oracle database is running, run the following command:

```
> ps -ef | grep ora_
```

Information similar to the following is displayed:

```
oracle 4055 1 0 20:00 ? 00:00:00 ora_j000_U2KDB
oracle 4174 4107 0 20:00 pts/1 00:00:00 grep ora_
oracle 23333 1 0 Nov15 ? 00:00:20 ora_pmon_U2KDB
oracle 23335 1 0 Nov15 ? 00:00:00 ora_vktm_U2KDB
oracle 23339 1 0 Nov15 ? 00:00:00 ora_diag_U2KDB
oracle 23341 1 0 Nov15 ? 00:00:00 ora_dbrm_U2KDB
oracle 23343 1 0 Nov15 ? 00:00:01 ora_psp0_U2KDB
oracle 23347 1 0 Nov15 ? 00:03:35 ora_dia0_U2KDB
oracle 23349 1 0 Nov15 ? 00:00:00 ora_mman_U2KDB
oracle 23351 1 0 Nov15 ? 00:00:03 ora_dbw0_U2KDB
oracle 23353 1 0 Nov15 ? 00:00:13 ora_lgwr_U2KDB
```

```
oracle 23355 1 0 Nov15 ? 00:00:15 ora_ckpt_U2KDB
oracle 23357 1 0 Nov15 ? 00:00:06 ora_smon_U2KDB
```

...

 **NOTE**

If the displayed information contains the following processes, the database service is started successfully:

- ora\_pmon\_U2KDB
- ora\_dbw0\_U2KDB
- ora\_lgwr\_U2KDB
- ora\_ckpt\_U2KDB
- ora\_smon\_U2KDB

To check whether the listener is started, run the following commands:

```
> su - oracle
password:password_of_oracle_user
> lsnrctl status
> exit
```

Information similar to the following is displayed:

```
...
STATUS of the LISTENER

Alias LISTENER
Version TNSLSNR for Linux: Version 11.1.0.7.0 - Production
Start Date 17-DEC-2009 20:35:58
Uptime 0 days 0 hr. 5 min. 2 sec
Trace Level off
Security ON: Local OS Authentication
SNMP OFF
...
```

 **NOTE**

If the displayed information contains **Alias LISTENER**, the listener is started successfully:

## 5 Optional: If the database is running, perform the following operation to end the database process:

```
> su - oracle
password:oracle_user_password
> sqlplus / as sysdba
SQL> shutdown immediate
SQL> exit
> exit
```

## 6 Perform the following operation to start the database process and enable the monitoring function:

To start the Oracle database, run the following commands:

```
> su - oracle
password:password_of_oracle_user
> sqlplus / as sysdba
SQL> startup
ORACLE instance started.
```

```
Total System Global Area 1610612736 bytes
Fixed Size 2046264 bytes
Variable Size 385877704 bytes
Database Buffers 1207959552 bytes
Redo Buffers 14729216 bytes
Database mounted.
Database opened.
```

To exit the SQL Server database, run the following command:



```
SQL> exit
```

To start the listener, run the following command:

```
> lsnrctl start
```

To log out as the Oracle user, run the following command:

```
> exit
```

7 After the database process is started, synchronize network configurations by using the MSuite.

1. [Start the MSuite server process.](#)
2. [Log in to the MSuite client.](#)
3. [Synchronize network configurations.](#)

----End

## A.9.44 How to View the U2000 and Sybase Database Installation Paths

### Question

How do I view the U2000 and Sybase database installation paths?

### Answer

Generally, the U2000 installation path is **/opt/U2000** and the Sybase database installation path is **/opt/sybase**.

To view the installation paths, perform the following steps:

- 1 Log in to the OS as user **root**.
- 2 Check the **ICMR\_conf.xml** configuration file to confirm the installation paths.

Run the following commands to check the **ICMR\_conf.xml** configuration file:

```
cd /etc/ICMR
more ICMR_conf.xml
```

A message similar to the following will be displayed:

```
<CONFIGITEMS>
<NETCONFIGFILE>/etc/ICMR/netCfg/OS/os_net_config.cfg</NETCONFIGFILE>
<DATABASEINSTALLPATH>/opt/sybase</DATABASEINSTALLPATH>
<IFCONFIGSYSNET>no</IFCONFIGSYSNET>
<NMSINSTALLPATH>/opt/U2000</NMSINSTALLPATH>
<FINISHTASKLIST>tasks::installtype_request,tasks::instSybase_request,tasks::instNM
S_request,tasks::single_network_request,tasks::modify_sys_paras,tasks::enable_mult
ipath,tasks::mirrorDisk,tasks::mount_array_disks</FINISHTASKLIST>
<INSTALLTYPE>1</INSTALLTYPE>
<DEBUGLEVEL>9</DEBUGLEVEL>
</CONFIGITEMS>
```

Confirm the installation paths according to the preceding message:

- The Sybase database installation path is **/opt/sybase** if **<DATABASEINSTALLPATH>/opt/sybase</DATABASEINSTALLPATH>** is displayed.

- The U2000 installation path is **/opt/U2000** if **<NMSINSTALLPATH>/opt/U2000</NMSINSTALLPATH>** is displayed.

----End

## A.9.45 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 another 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).
- **HBIIPMP=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

## A.9.46 How to Rectify the Mouse Detection Failure and Open the GUI After the T5220 Is Connected to the KVM

### Question

The OS was installed by using the quick installation DVD. After the T5220 is connected to the KVM, the GUI cannot be opened. How do I rectify this fault?

### Answer

- 1 To set the I/O mode, run the following commands:

```
eeprom output-device=screen
```

```
eeprom input-device=keyboard
```

- 2 To set the screen resolution and refresh rate, perform the following operations:

1. To view information about the current video card, run the following command:

```
fbconfig -list
```

A message similar to the following will be displayed:

| Device File Name    | Device Model | Configuration Program |
|---------------------|--------------|-----------------------|
| -----               | -----        | -----                 |
| /dev/fbs/nfb0 [a b] |              | SUNWnfb_config        |

2. To view the screen resolution and refresh rate supported for the current video card, run the following command:

```
fbconfig -res \?
```

A message similar to the following will be displayed:

```
Valid values for -res option are:
```

```
VESA_STD_640x480x60
```

```
...
```

```
...
```

Notes:

Monitor 1 edid data not available, monitor may not support all resolutions.  
Monitor 2 edid data not available, monitor may not support all resolutions.

Use unsupported resolutions at your own risk.

\* Abbreviations such as "1280x1024x75" may also be used

3. To view the current configurations for the video card, run the following command:

```
fbconfig -propt
```

A message similar to the following will be displayed:

```
--- OpenWindows Configuration for /dev/fb0 ---
```

```
OWconfig: machine
```

```
Video Mode: not set
```

```
Screen Information:
```

```
Doublewide: Disable
```

```
Doublehigh: Disable
```

```
Clone: Disable
```

```
Offset/Overlap: [0, 0]
```

```
Output Configuration: Direct
Fake8 Rendering: Disable
```

4. The screen resolution and refresh rate are not set if **Video Mode** is set to **not set**. To set the screen resolution and refresh rate, run the following commands:

```
fbconfig -dev /dev/fbs/nfb0 -res 1024x768x60 now
```

A message similar to the following will be displayed:

```
SUNWnfb_config: Warning: no edid data available from monitor A
SUNWnfb_config: Cannot verify that 1024x768x60 is a supported
video resolution for this monitor
SUNWnfb_config: Use 1024x768x60 anyway (yes/no) ?
```

Enter **y**, and then press **Enter**. A message similar to the following will be displayed:

```
Setting 1024x768x60
```

5. To view the current configurations for the video card, run the following command:

```
fbconfig -propt
```

The setting has taken effect if a message similar to the following is displayed.

```
--- Open Windows Configuration for /dev/fb0 ---

OWconfig: machine
Video Mode: 1024x768x60

Screen Information:
 Doublewide: Disable
 Doublehigh: Disable
 Clone: Disable
 Offset/Overlap: [0, 0]
 Output Configuration: Direct
 Fake8 Rendering: Disable
```

- 3 To restart the OS, run the following command. After the OS is restarted, connect the T2550 to the KVM.

```
sync;sync;sync;sync
```

```
shutdown -y -g0 -i6
```

----End

## A.9.47 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

## A.9.48 How to Rectify the Failure to Connect to the Sybase Database During U2000 Installation

### Question

How to rectify the failure to connect to the Sybase database during U2000 installation?

### Answer

1. This fault occurs if the IP address recorded in the **interfaces** file in the Sybase database is different from the IP address of the U2000 server. To rectify this fault, modify the IP address recorded in the **interfaces** file.
2. To modify the **interfaces** file, run the following command:

```
$ vi /opt/sybase/interfaces
```

Information similar to the following is displayed:

```
DBSVR master tcp ether 129.9.1.20 4100 query tcp ether 129.9.1.20 4100 master tcp
ether 129.9.1.20 4100 query tcp ether 129.9.1.20 4100 master tcp ether 127.0.0.1
4100 query tcp ether 127.0.0.1 4100
```

```
DBSVR_back master tcp ether 129.9.1.20 4200 query tcp ether 129.9.1.20 4200 master
tcp ether 129.9.1.20 4200 query tcp ether 129.9.1.20 4200 master tcp ether
127.0.0.1 4200 query tcp ether 127.0.0.1 4200
```

Change the IP address (for example, 129.9.1.20) recorded in the **interfaces** file to the IP address of the U2000 server.

----End

## A.9.49 Reinstalling the U2000 on or Migrating the U2000 to Another Computer

### Question

In the U2000 single-server system, the U2000, for some reasons, may need to be reinstalled on or migrated to another computer from the currently running U2000 server. This topic describes how to reinstall or migrate the U2000.

### Answer



#### CAUTION

- Reinstalling the U2000 may interrupt the U2000 services and management. Therefore, you need to ensure that networks are not affected due to the shutdown of the U2000.
  - Reinstalling or migrating the U2000 may cause data loss of some configurations. Thus, re-configuration is required.
  - NE login conflicts may occur during the U2000 migration if the current U2000 is not stopped.
- 

- 1 Back up the license file. Licenses are related to the MAC addresses of NICs. Therefore, you need to apply for a new license after the change of computers.
- 2 Back up the U2000 database to a specified directory. Do not delete any data in the database for reinstalling the U2000.
- 3 Learn and manually record other existing information on the U2000. The reason is that some data, such as the IP address, host name, installed components, preferences, and NBI configuration, is not backed up during the backup of the U2000 database.
- 4 Reinstall the U2000. Make sure that the version of the U2000 (including the patch), the version of the database software and the installed components are the same as before.
- 5 Restore the U2000 database.
- 6 Restore other configurations of the U2000 according to your record. If NBIs are involved, you need to configure the NBIs again.

----End

## A.9.50 How to Set the Communication Mode on the U2000 server for the Single-Server System (Windows)

### Question

The U2000 server and client can communicate with each other in common or Security Socket Layer (SSL) mode. How to set the common or SSL mode?

## Answer

- 1 Log in to the OS on the U2000 server as an administrator and do as follows to query the communication mode in use:

Choose **Start > Run**. In the **Run** dialog box, enter **cmd** to open the command line interface (CLI). Enter **ssl\_adm -cmd query** to query the communication mode that the U2000 server is using.

- 2 Stop U2000 processes.

In the U2000 software installation path, for example, **D:\U2000\server\bin**, run the **stopnms.bat** file to stop U2000 processes.

- 3 Set the communication mode for the U2000 server and client.

Choose **Start > Run**. In the **Run** dialog box, enter **cmd** to open the CLI. Enter **ssl\_adm -cmd setmode mode parameter** and set the communication mode for the U2000 server and client.

### NOTE

The available options for *mode parameter* are **normal**, **ssl**, and **both**.

- **normal**: indicates that the U2000 server and client can communicate with each other only in common mode.
- **ssl**: indicates that the U2000 server and client can communicate with each other only in SSL mode. In this mode, communication security is guaranteed between the U2000 server and client.
- **both**: indicates that the U2000 server and client can communicate with each other in either common or SSL mode.

- 4 Start U2000 processes.

In the U2000 software installation path, for example, **D:\U2000\server\bin**, run the **startnms.bat** file to start U2000 processes.

----End

## A.9.51 How to Set the Communication Mode on the U2000 server for the Single-Server System (Solaris)

### Question

The U2000 server and client can communicate with each other in common or Security Socket Layer (SSL) mode. How to set the common or SSL mode?

### Answer

- 1 Log in to the OS on the U2000 server as **nmsuser** user and do as follows to query the communication mode in use:

```
$ ssl_adm -cmd query
```

- 2 Run the following command to stop U2000 processes.

```
$ cd /opt/U2000/server/bin
$./stopnms.sh
```

- 3 Set the communication mode for the U2000 server and client.

```
$ ssl_adm -cmd setmode mode parameter
```



 **NOTE**

The available options for *mode parameter* are **normal**, **ssl**, and **both**.

- **normal**: indicates that the U2000 server and client can communicate with each other only in common mode.
- **ssl**: indicates that the U2000 server and client can communicate with each other only in SSL mode. In this mode, communication security is guaranteed between the U2000 server and client.
- **both**: indicates that the U2000 server and client can communicate with each other in either common or SSL mode.

- 4 Run the following command to start U2000 processes.

```
$ cd /opt/U2000/server/bin
$./startnms.sh
```

----End

## A.9.52 How to Configure the Communication Mode for a Linux-based U2000 Server?

### Question

A Linux-based U2000 server has two communication modes: the normal mode and the security socket layer (SSL) mode. How to configure these two modes?

### Answer

- 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 Run the following commands to stop the U2000:

```
cd /opt/U2000/server/bin
./stopnms.sh
```

- 3 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.

- 4 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 daemon 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.
- 5 Restart the daemon 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
```
- 6 Run the following command on the master server to start the U2000 process as user **root**.

```
# cd /opt/U2000/server/bin
# ./startnms.sh
```

----End

A.9.53 How to Set the Communication Mode on the U2000 Server for the High Availability System (Windows)

Question

The U2000 server and client can communicate with each other in common or Security Socket Layer (SSL) mode. How to set the common or SSL mode?

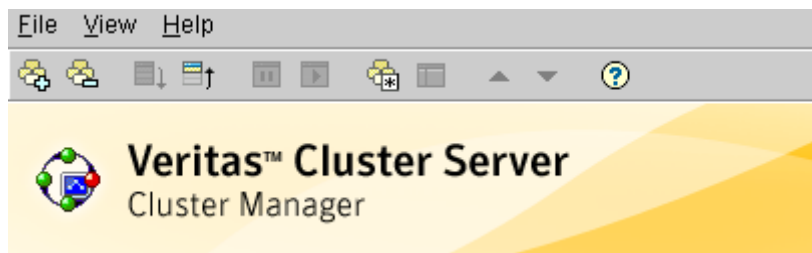
 NOTE

You need to set the communication mode for the U2000 server and client only on the primary site.

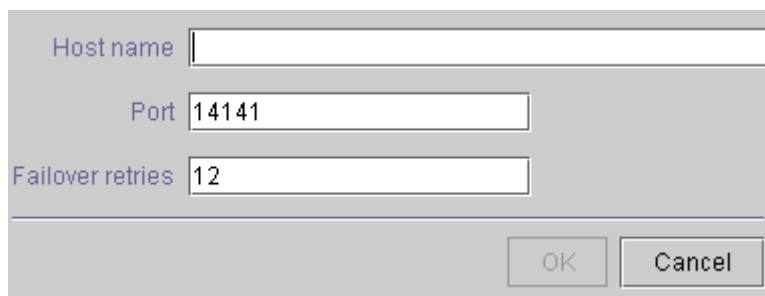
Answer

- 1 Log in to the OS on the U2000 server on the primary site as an administrator and do as follows to query the communication mode in use:
Choose **Start > Run**. In the **Run** dialog box, enter **cmd** to open the command line interface (CLI). Enter **ssl_adm -cmd query** to query the communication mode that the U2000 server is using.
- 2 On the primary site, do as follows to stop U2000 processes:

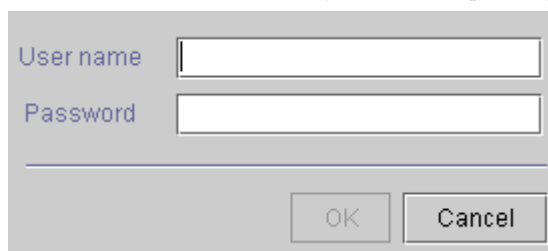
1. Choose **Start > Programs > Symantec > Veritas Cluster Server > Veritas Cluster Manager - Java Console** to start the VCS client.



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



3. Enter an IP address for the system of the primary site. Then, click **OK**.



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

Wait patiently. If all resources on the **Resources** tab page turn grey, it indicates that U2000 processes have been stopped.

- 3 Perform the following operations on the primary site to start the database:

1. In the navigation tree, right-click **AppService-SQLServer2000**, and then choose **Online > host_name** from the shortcut menu.
2. In the dialog box that is displayed, click **Yes**.

- 4 Set the communication mode for the U2000 server and client.

Choose **Start > Run**. In the **Run** dialog box, enter **cmd** to open the CLI. Enter **ssl_adm -cmd setmode mode parameter** and set the communication mode for the U2000 server and client.

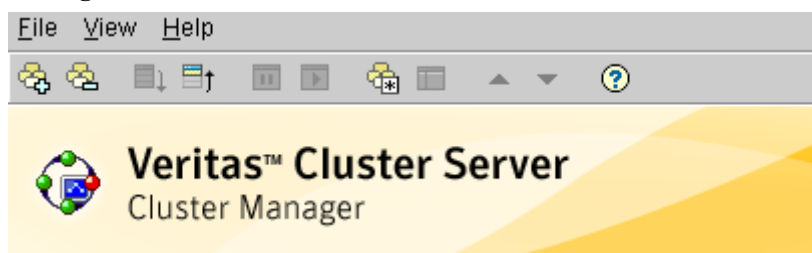
 NOTE

The available options for *mode parameter* are **normal**, **ssl**, and **both**.

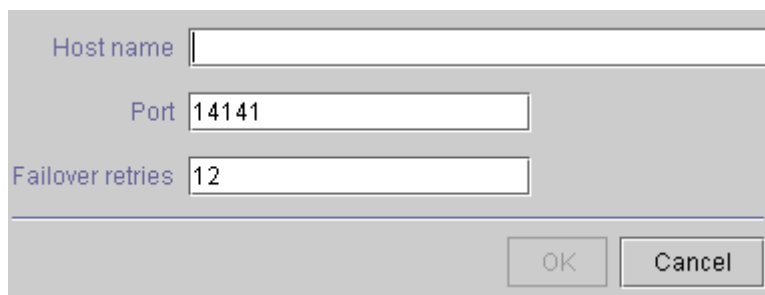
- **normal**: indicates that the U2000 server and client can communicate with each other only in common mode.
- **ssl**: indicates that the U2000 server and client can communicate with each other only in SSL mode. In this mode, communication security is guaranteed between the U2000 server and client.
- **both**: indicates that the U2000 server and client can communicate with each other in either common or SSL mode.

5 To stop U2000 processes, run the following commands on the primary site:

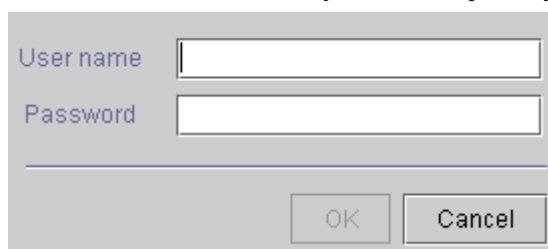
1. Choose **Start > Programs > Symantec > Veritas Cluster Server > Veritas Cluster Manager - Java Console** to start the VCS client.



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



3. Enter the IP address of the system of the primary site. Then, click **OK**.



4. Enter the default user name **admin** and the default password **password** of 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**.

----End

A.9.54 How to Set the Communication Mode of the Server in a High Availability System (Solaris)?

Question

The server in a high availability system (Solaris) has two communication modes, namely, common and Security Socket Layer (SSL). How to set the common or SSL mode?

Answer



CAUTION

In a high availability system (Solaris), the communication mode of the server is automatically synchronized from the primary site to the secondary site. Therefore, only the procedure for setting the communication mode on the primary site is described here.

- 1 Log in to the OS as the **root** user and run the following commands to query the communication mode in use:

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



NOTE

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

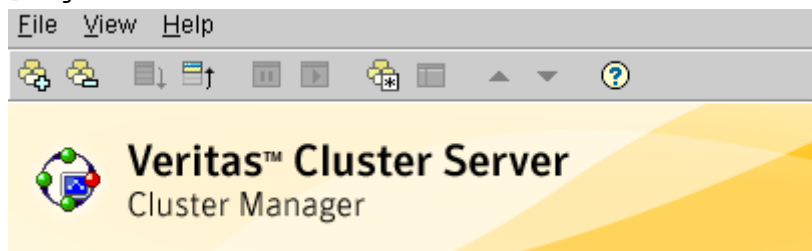
- 2 Stop the U2000 processes.

The U2000 processes consist of the U2000 server process and the Sybase process.

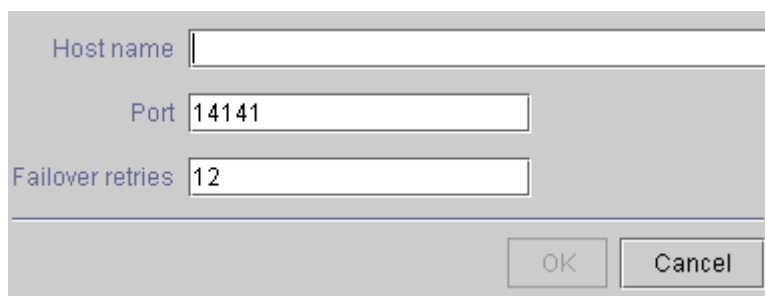
Check whether the U2000 processes are stopped and perform the following operations:

1. Access the **Java Desktop System, Release 3** session of the OS of the server of the active site as the **root** user.
2. Run the following command to start the VCS client:

```
# hagui &
```



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



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

5. Enter the default user name **admin** and the default password **password** of the VCS client. Then, click **OK**.
6. Select the **AppService** resource group from the navigation tree, click the **Status** tab, and then view the status of the U2000 processes.
 - If **Group Status on Member Systems** is displayed as **Offline**, it indicates that the U2000 processes are stopped.
 - If **Group Status on Member Systems** is displayed as **Online**, it indicates that the U2000 processes are started. Do as follows to stop the U2000 processes:
Right-click **AppService** and choose **Offline > host_name** from the shortcut menu.

- 3 Run the following commands to set the communication mode of the server:

```
# ssl_adm -cmd setmode mode parameter
```

NOTE

In the preceding command, *mode parameter* can be **normal**, **ssl**, or **both**. The description of each value is as follows:

- **normal**: Indicates that the U2000 server communicates with clients only in normal mode without security assurance.
- **ssl**: Indicates that the U2000 server communicates with clients only in security mode. This mode ensures the communication security.
- **both**: Indicates that both the normal and SSL modes are applicable to the U2000 server to communicate with clients.

- 4 In the **Cluster Explorer** window, right-click the **AppService** resource group in the navigation tree and choose **Online > primary** from the shortcut menu to start the Sybase process and U2000 server process.

TIP

Click the **Resources** tab to view the start status of each resource.

Normally, on the **Status** tab page, **Online** is displayed for **State** in the **Group Status on Member Systems** area on the active site, and **Online on primary** is displayed for **Status** in the **Resource Status** area.

NOTE

- In actual configuration, use the actual host name.
- If a fault has occurred during start of the AppService process, right-click **AppService** and choose **clear fault** from the shortcut menu to clear the fault. Then, choose **Online > host_name** to start the AppService process.

- 5 In the dialog box that is displayed, click **Yes**.

----End

A.9.55 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
```

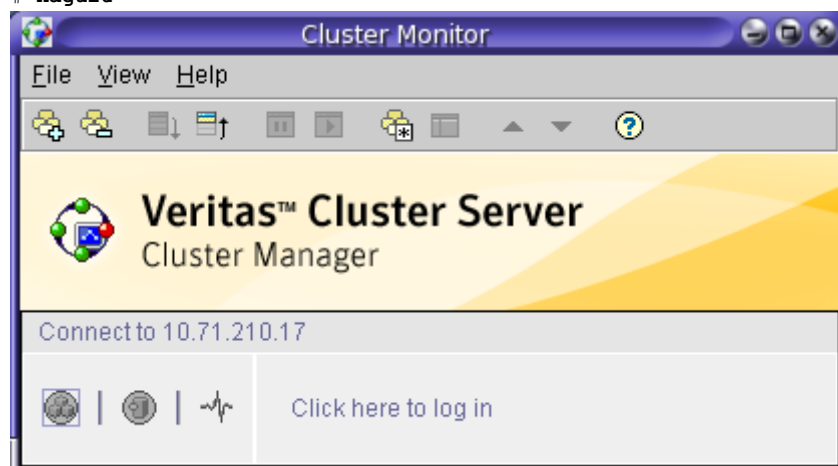


NOTE

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:

```
# hagu i &
```



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_admin -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 daemon process.

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

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

```
# ssl_admin -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 daemon 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**

B Configuring Controller IP Addresses for Workstation

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

[B.1 Configuring the IP Address for a System Controller on a T5220 Server](#)

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

[B.2 Configuring the IP Address for a System Controller on an M4000 Server](#)

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

B.1 Configuring the IP Address for a System Controller on a T5220 Server

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

Prerequisite

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

Context

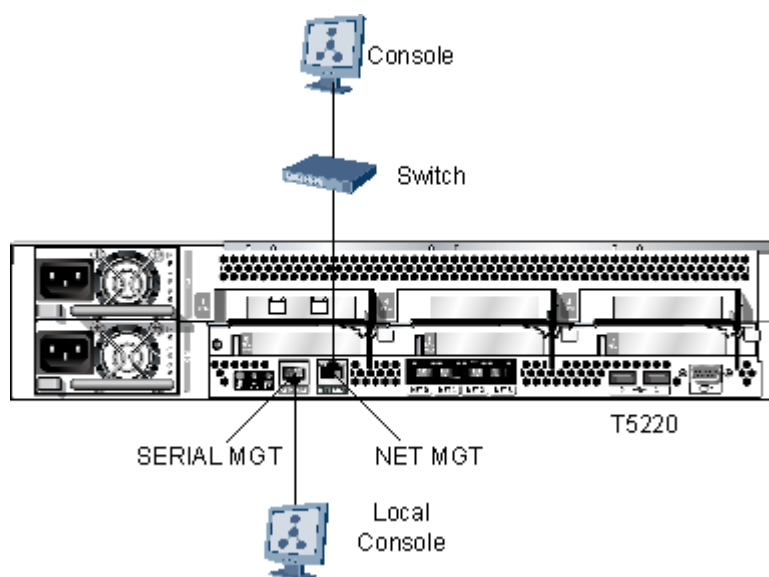
Installation engineers can configure server connections through system controllers so that Sun servers can be remotely controlled and maintained.

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

Procedure

1. Connect the computer and the server physically.
 1. Use a serial port (DB9-RJ45) to connect the serial port of the local console and the serial port (SERIAL MGT) of the server.
Use an RJ-45 connector at one end of the serial port cable to connect to the serial port (SERIAL MGT) of the server and use a DB-9 connector at the other end of the cable to connect to the serial port (COM1 or COM2) of the computer.
 2. Use a network cable to connect the network management port (NET MGT) of the system controller and the switch.

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



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

3 Press **Enter**.

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



NOTE

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

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

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

The following message will be displayed:

```
/SP/network
```

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

The following message will be displayed:

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

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

The following message will be displayed:

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

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

The following message will be displayed:

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

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

The following message will be displayed:

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

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

The following message will be displayed:

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

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

The following message will be displayed:

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

8. Enter **exit** to complete configuration.
- 5 Disconnect the serial port of the system controller from the HyperTerminal. Configuration is complete.

----End

B.2 Configuring the IP Address for a System Controller on an M4000 Server

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

Prerequisite

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

Context

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

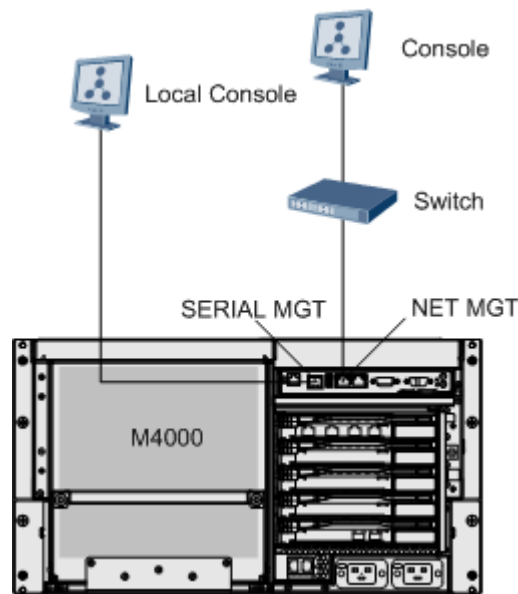
In the high availability (HA) system, operations must be performed at the primary and secondary sites.

Procedure

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

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

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



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

3 Press Enter.

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

```
login: default
```

A message similar to the following will be displayed:

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

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

A message similar to the following will be displayed:

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

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

A message similar to the following will be displayed:

XSCF>

 NOTE

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

6 Run the following commands to create a monitor user:

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

 NOTE

The password must contain the following:

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

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

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

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

8 Enter the password.

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

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

10 Run the following command to set the time zone:

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

 NOTE

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

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

11 Run the following command to set the time:

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

 NOTE

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

System time will be displayed in the following format:

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

A message similar to the following will be displayed:

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

12 Enter **n**.

13 Run the following command to set the altitude:

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

A message similar to the following will be displayed:

```
1000m
```

14 Run the following command to enable SSH:

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

A message similar to the following will be displayed:

Continue? [y|n]:

15 Enter **y**.

A message similar to the following will be displayed:

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

16 Run the following command to enable the Telnet function:

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

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

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

Press **Enter** to continue.

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

Press **Enter** to continue.

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

Press **Enter** to continue.

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

Press **Enter** to continue.

 NOTE

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

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

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

19 Run the following command:

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

20 Run the following command to apply network settings:

```
XSCF> applynetwork
```

A message similar to the following will be displayed:

The following network settings will be applied:

```
xscf#0 hostname :sc  
DNS domain name :huawei.com  
  
interface      :xscf#0-lan#0  
status         :up  
IP address     :IP_address_of_the_primary_controller  
netmask        :255.255.255.0  
route          :-n 0.0.0.0 -m 0.0.0.0 -g  
IP_address_of_the_network_gateway_of_the_primary_controller  
  
interface      :xscf#0-lan#1  
status         :up  
IP address     :IP_address_of_the_secondary_controller  
netmask        :255.255.255.0  
route          :-n 0.0.0.0 -m 0.0.0.0 -g  
IP_address_of_the_network_gateway_of_the_secondary_controller  
  
Continue? [y|n]
```

21 Enter **y**.

A message similar to the following will be displayed:

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

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

```
XSCF> rebootxscf
```

A message similar to the following will be displayed:

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

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

A message similar to the following will be displayed:

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

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

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

 TIP

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

1. Run the following command on the console:

```
# telnet IP_address_of_the_primary_controller
```

A message similar to the following will be displayed:

```
login:
```

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

A message similar to the following will be displayed:

```
password:
```

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

4. Run the following command to exit the connection to the primary controller:

```
XSCF> exit
```

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

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

 TIP

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

1. Run the following command on the console:

```
# telnet IP_address_of_the_secondary_controller
```

A message similar to the following will be displayed:

```
login:
```

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

A message similar to the following will be displayed:

```
password:
```

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

4. Run the following command to exit the connection to the primary controller:

```
XSCF> exit
```

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

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

----End

C Configuring the Management Console

This topic describes how to configure the remote management console of a blade server.

[C.1 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.

[C.2 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.

C.1 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.

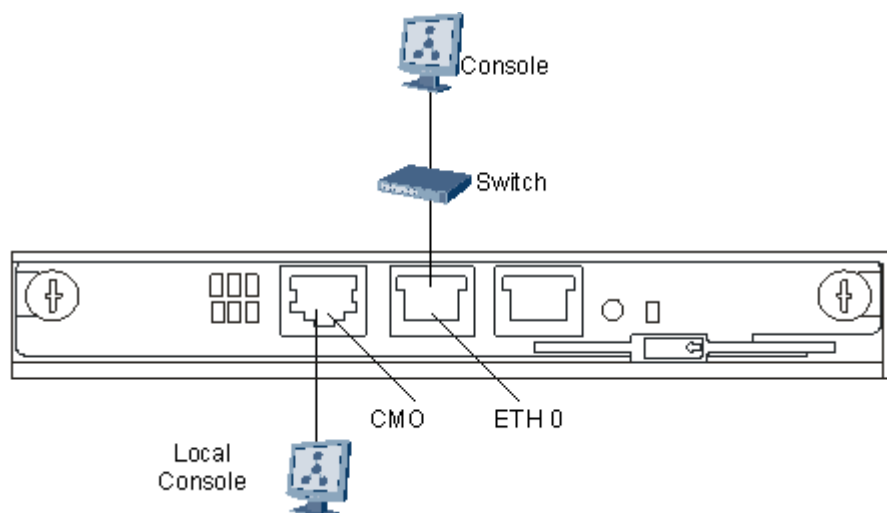
Prerequisite

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 C-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

C.2 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 then 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 C-1](#). After you set the parameters, click **Save** to save the settings.

Primary Management Module

This management module is in Bay 1 of the chassis

Hostname

MME41F1348D132

Domain name

Register this interface with DNS

☐

Advanced Ethernet Setup

DHCP

Disabled - Use static IP configuration

*** Currently the static IP configuration is active for this interface. *** This static configuration is shown below.

IPv4 Static IP Configuration

IP address

129.9.1.30

Subnet mask

255.255.255.0

Gateway address

129.9.1.254

Save

Advanced Failover

Normally, when a primary management module fails, the standby module assumes control automatically, takes the IP address of the primary module, and causes no downtime.

In some situations, however, control might not fail over to the standby management module when it in fact should. This includes, for example, situations in which the primary module is running but not reliably responding. To protect against these situations, you can configure additional network settings for failovers that will allow you to manually access the standby module when automatic failover does not happen. Specifically, this means you will assign a distinct IP address to the standby module, instead of just specifying a single IP address to be used for both.

Indicate below whether or not you wish to use advanced failover.

☐ Use Advanced Failover

Table C-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 <i>129.9.1.30</i> . Enters the subnet mask of the management module.
	Subnet mask	Enters the planned subnet mask of the management module, such as <i>255.255.255.0</i> .
	Gateway address	Enters the planned route address of the management module, such as <i>129.9.1.254</i> .

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

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

Issue 06 (2010-11-19)

Huawei Proprietary and Confidential
Copyright © Huawei Technologies Co., Ltd.

C-5

- 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

D MSuite

This topic describes the related concepts and common operations of the MSuite.

[D.1 Overview](#)

This topic describes the system structure, functions, features, and certain basic concepts of the MSuite.

[D.2 Starting and Stopping the MSuite](#)

This topic describes how to start and stop the MSuite.

[D.3 System Management](#)

This topic describes how to use the system management functions of the MSuite.

[D.4 U2000 Deployment](#)

This topic describes how to deploy the U2000. After the U2000 is installed, you can maintain or adjust the deployment of the U2000 through the MSuite.

[D.5 Adjusting the NMS](#)

This topic describes how to adjust the NMS. After the U2000 is installed, you can adjust the U2000 server parameters through the MSuite.

[D.6 Management of the High Availability System \(Veritas hot standby\)](#)

This topic describes the frequently used operations of managing and maintaining the high availability system (Veritas hot standby) through the MSuite.

[D.7 Maintaining a Distributed System](#)

This topic describes the daily operations used to maintain a distributed system through the MSuite. If you are using a centralized system, skip this topic.

[D.8 Configuring the Northbound Interface Instance](#)

This topic describes how to configure the northbound interface (NBI) instance. When the U2000 needs to access the upper-layer NMS, the related NBI should be configured as required. The NBIs that are commonly used by the U2000 are CORBA, SNMP, XML and TEXT NBIs.

[D.9 Managing Databases](#)

This topic describes how to manage databases. To ensure the security of system data, the MSuite provides the function of managing databases.

D.1 Overview

This topic describes the system structure, functions, features, and certain basic concepts of the MSuite.

D.1.1 Basic Concepts

This topic describes the basic concepts related to the MSuite.

D.1.2 System Architecture of the MSuite

This topic describes the system architecture of the MSuite.

D.1.3 Function Overview

This topic describes the functions and application scenarios of the MSuite.

D.1.4 Graphical User Interface

The MSuite client supports the graphic user interface (GUI). The GUI consists of menus, toolbar buttons, maintenance list column and the NMS vision.

D.1.5 Command Line Interface

This topic describes the CLI. The MSuite client allows you to perform operations through command lines. In the Solaris or SUSE Linux OS, if you cannot use the graphical desktop system, you can use command lines to deploy the U2000.

D.1.1 Basic Concepts

This topic describes the basic concepts related to the MSuite.

Terms

- **MSuite:** The MSuite is a graphical maintenance tool developed for the Huawei iManager U2000 (U2000), a type of Huawei network product. The MSuite is used to debug, maintain, and redeploy the U2000. For the system architecture of the MSuite, see [D.1.2 System Architecture of the MSuite](#). For the functions and features of the MSuite, see [D.1.3 Function Overview](#).
- **Server:** Usually, a computer running the server program is called a server. Here, the server refers to a computer that runs the U2000 server program. A set of U2000 can be deployed on multiple computers. In this case, the U2000 NMS has multiple servers.
- **Component:** It is the software functional unit that you can choose to install. Each component can include multiple deployment packages.
- **Deployment package:** It is the software unit deployed on a computer. In distributed mode, the deployment packages of one component may be deployed on different computers.
- **Instance:** It is a physical process that appears after the deployment package is deployed. You can add the instance during the installation of the U2000, or add the instance through the MSuite after the U2000 is installed.

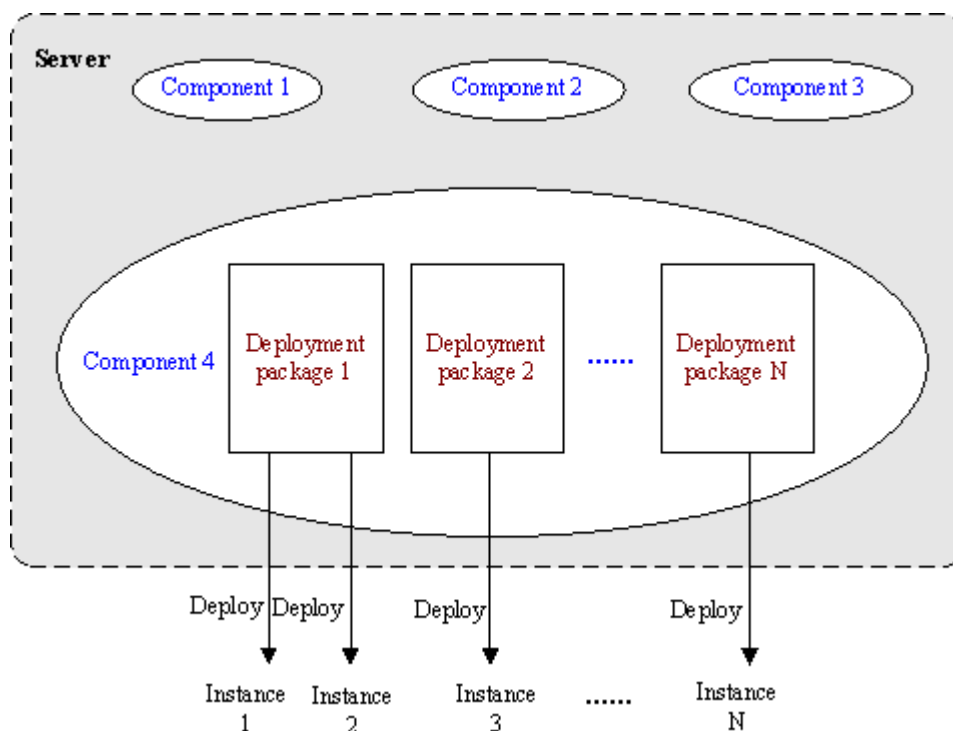
NOTE

Instance names are irrelevant with process names queried on the System Monitor. You can change instance names by using the MSuite.

- **NMS application IP address:** This type of IP address is used to provide external NMS services, such as the communication between the NMS server and the clients or NEs, the communication between MSuite client and MSuite server

Figure D-1 shows the relationships between the component, deployment package, and instance.

Figure D-1



NOTE

- The U2000 consists of multiple components. Each component implements one function of the U2000. For example, as shown in **Figure D-1**, four components are installed on the server. Theoretically, the U2000 has the functions of these four components.
- Each component is composed of one or multiple deployment package. One instance is generated each time the deployment package is deployed. A instance is an actual process. For example, as shown in **Figure D-1**, component 4 is composed of three deployment packages. deployment package 1 has been deployed twice; therefore, deployment package 1 has two instances. deployment package 2 and deployment package 3 have been deployed once each; therefore, either deployment package 2 or deployment package 3 has one instance. In the System Monitor, four processes related to component 4 are displayed. The U2000 has the function of component 4 only after these four processes are all in the running state.
- deployment package 1 has been deployed twice because the management capability of a single process is limited due to OS restrictions. Some deployment packages can be deployed several times to implement large-scale network management. Accordingly, multiple processes are generated and the management capability is improved greatly. For example, as shown in **Figure D-1**, assume that each process can manage a maximum of 2000 SDH NEs. Two processes are generated after deployment package 1 has been deployed twice; therefore, the U2000 can manage 4000 SDH NEs.

Deployment package Classification

According to the quantity of the instances supported, you can classify the deployment packages into the following types:

- **System single-instance:** In a set of U2000, the deployment package can be installed on only one of the servers and can be deployed with only one instance.

- Single-server single-instance: In a set of U2000, the deployment package can be installed on multiple servers but can be deployed with only one instance on each server.
- Single-server multi-instance: In a set of U2000, the deployment package can be installed on multiple servers and can be deployed with multiple instances on each server.

D.1.2 System Architecture of the MSuite

This topic describes the system architecture of the MSuite.

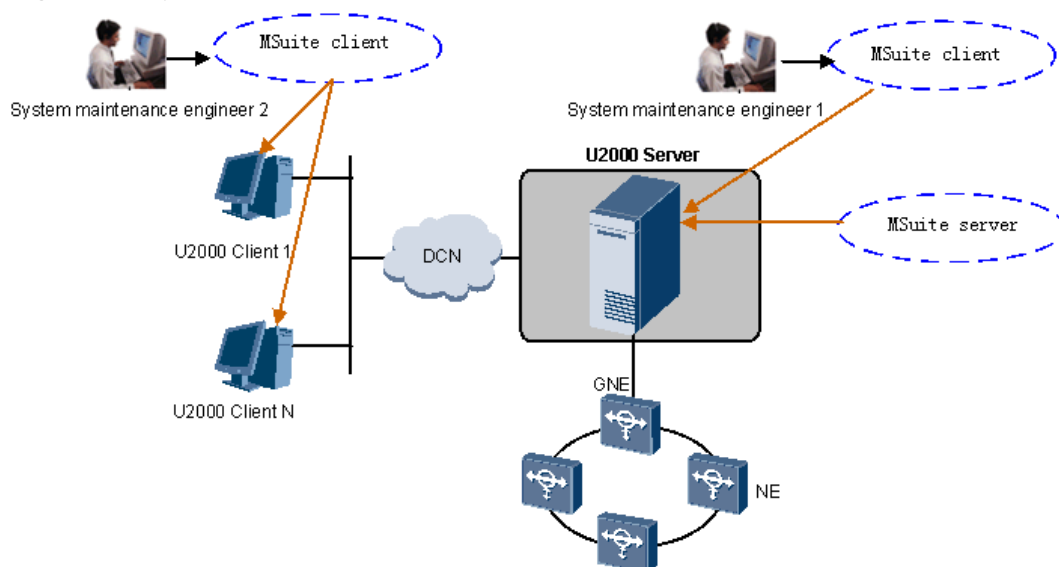
The MSuite adopts the client/server model. The client communicates with the server through the TCP/IP protocol. After receiving a request from the client, the server completes the specific task, and then sends the result back to the client. **Figure D-2** shows the system architecture.



CAUTION

The MSuite works in single-user mode. That is, only one MSuite client is allowed to log in to the MSuite server at one time.

Figure D-2 System architecture of the MSuite



The MSuite is automatically installed during the installation of the U2000.

- During the installation of the U2000 server, the MSuite server and MSuite client are automatically installed.
- During the installation of the U2000 client, the MSuite client are automatically installed.



CAUTION

The MSuite works in single-user mode. That is, only one MSuite client is allowed to log in to the MSuite server at one time. For example, in the **Figure D-2**, maintenance engineers 1 and 2 cannot log in to the MSuite client at the same time to operate the U2000.

D.1.3 Function Overview

This topic describes the functions and application scenarios of the MSuite.

After the U2000 is installed, you can deploy or maintain the U2000 through the MSuite. The specific functions are described as follows:



NOTE

In different OSs, the functions of the MSuite are different.

Table D-1 Functions of the MSuite

Type	Function	Description
Managing the NMS	Refreshing the NMS information	For details, see D.3.1 Refreshing the NMS Information .
	Synchronizing the NMS information	For details, see D.3.2 Synchronizing the NMS Information .
	Changing the password	For details, see D.3.4 Changing the Password of the MSuite .
	Logging out of the MSuite client	For details, see D.2.3 Exiting from the MSuite client .
	Exiting from the MSuite client	For details, see D.2.3 Exiting from the MSuite client .
Deploying and maintaining the NMS	Adding a component	For details, see D.4.1 Adding a Component .
	Deleting a component	For details, see D.4.2 Deleting a Component .
	Adding an instance	For details, see D.4.3 Adding an Instance .

Type	Function	Description
	Deleting an instance	For details, see D.4.5 Deleting an Instance .
	Modifying the instance name and description	For details, see D.4.6 Changing the Name and Remarks of an Instance .
	Modifying the system time and time zone	For details, see D.4.7 Setting the System Time and Time Zone .
	Changing the password of the administrator of the database	For details, see D.4.8 Changing the Password of the Administrator of the Database .
	Changing the password of the NMS user of the database	For details, see D.4.9 Changing the Password of the User of the Database .
	Configuring NTP	For details, see D.4.10 Configuring the NTP Service .
Maintaining the high availability system (Veritas hot standby)	Synchronizing the primary and secondary sites	For details, see D.6.1 Establishing the HA Relationship Between the Primary and Secondary Sites .

Type	Function	Description
	Separating the primary and secondary sites	For details, see D.6.2 Deleting the HA Relationship Between the Primary and Secondary Sites .
	Deleting replication relations	For details, see D.6.3 Deleting Replication Relations .
	Configuring the local site as the primary site forcibly	For details, see D.6.4 Configuring the Current Server as the Active Server Forcibly .
	Performing the dual-active operation	For details, see D.6.5 Performing the Dual-Active Operation .
Maintaining the distributed system	Adding a slave server	For details, see D.7.1 Adding a Slave Server .
	Deleting a slave server	For details, see D.7.2 Deleting a Slave Server .
	Migrating an instance	For details, see D.7.3 Migrating an Instance .
Managing the database	Backing up the system database	For details, see D.9.1 Backing Up the System Database .

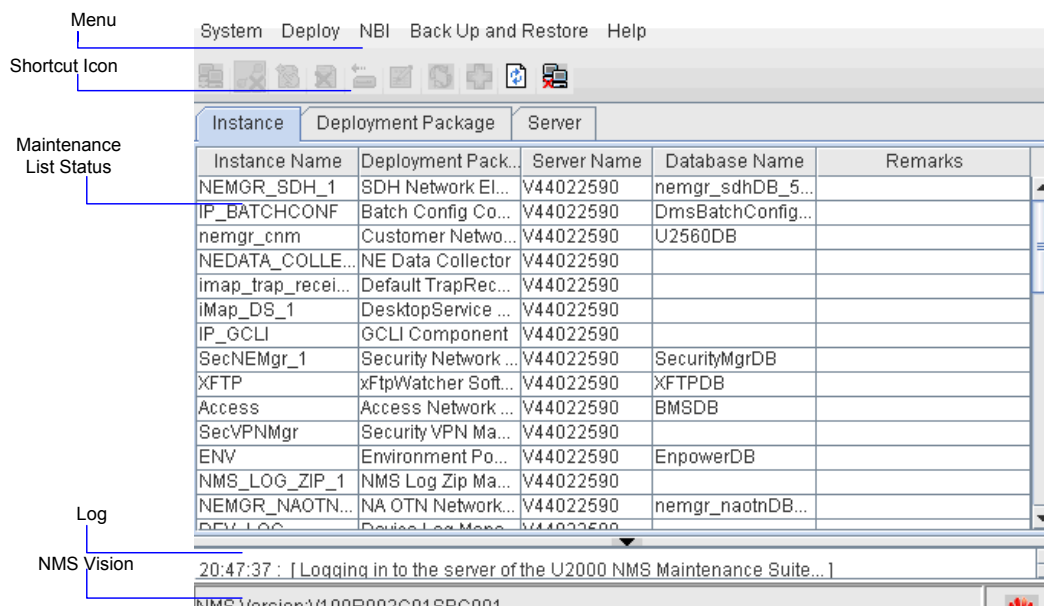
Type	Function	Description
	Restoring the system database	For details, see: ● D.9.2 Restoring Data of a U2000 Single-Server System (Windows) ● D.9.3 Restoring U2000 Single-Server System (Solaris) Data ● D.9.4 Restoring U2000 Single-Server System (SUSE Linux-Distributed) Data ● D.9.5 Restoring U2000 High Availability System (Windows) Data ● D.9.6 Restoring U2000 High Availability System (Solaris) Data ● D.9.7 Restoring U2000 High Availability System (SUSE Linux-Distributed) Data
	Initializing the U2000 database	For details, see D.9.9 Initializing the U2000 Database .
Adjusting the NMS	Changing the host name and IP address	For details, see D.5.1 Changing the Host Name and IP Address .
	Configuring routes	For details, see D.5.2 Configuring Routes .
	Synchronizing the network configuration	For details, see D.5.3 Synchronizing Network Configurations .
Configuring NBI instances	-	For details, see D.8 Configuring the Northbound Interface Instance .

D.1.4 Graphical User Interface

The MSuite client supports the graphic user interface (GUI). The GUI consists of menus, toolbar buttons, maintenance list column and the NMS vision.

Main Window

Figure D-3 shows the GUI of the MSuite client.

Figure D-3 GUI of the MSuite client

GUI Components

Component	Meaning
Menu item	Serves as a navigation path to enter the GUI of the corresponding function.
Shortcut icon	Serves as a shortcut to enter the GUI of the corresponding function. The same function can be accessed through the corresponding menu. TIP Move the pointer over the shortcut icon. The system prompts you the function of the shortcut icon.
Maintenance list column	- On the Instance tab page, you can view the names, running status, related deployment packages, related host names, and database names of all instances. - On the "Deployment package" tab page, you can view the names, types, descriptions, and number of instances of all deployment packages. - On the Server tab page, you can view the hostnames, IP addresses, NMS status, and resource usage of all servers.
Log bar	Displays the log information when a task is executed.

Component	Meaning
NMS vision bar	Displays the U2000 version.

D.1.5 Command Line Interface

This topic describes the CLI. The MSuite client allows you to perform operations through command lines. In the Solaris or SUSE Linux OS, if you cannot use the graphical desktop system, you can use command lines to deploy the U2000.

Frequently Used Commands in the CLI

Table D-2 shows the frequently used command lines of the MSuite. For details about how to use these command lines, see the help information on the CLI. On Solaris OS, run the following command as user **nmsuser**. On SUSE Linux OS, run the following command as user **root**.

```
cd /opt/U2000/engineering
./startclient.sh deploy -ip 127.0.0.1 -port 12212 -username admin -password admin -help
```

NOTE

- Before you perform operations through the CLI, make sure that the NMS maintenance suite server is started. Otherwise, run the following commands as the **root** user to start the NMS maintenance suite server:

```
# cd /opt/HWENGR/engineering
# ./startserver.sh
```
- In the CLI of the Solaris OS, you need to run commands as the **nmsuser** user. In the CLI of the SUSE Linux OS, you need to run commands as the **root** user.
- The information in italic type in the following table indicates the variable parameters that can be changed as required.
- When using the command lines of the MSuite, you need to run the **cd /opt/U2000/engineering** command to switch to the directory where the MSuite is installed.

Table D-2 Common CLI commands for the MSuite

Syntax of Command Line	Meaning
./startclient.sh deploy -ip 127.0.0.1 -port 12212 -username admin -password admin query -type <i>querytype</i>	Query information. - Querying instance information: query -type 0 - Querying deployment package information: query -type 1 - Querying server information: query -type 2
./startclient.sh deploy -ip 127.0.0.1 -port 12212 -username admin -password admin deployins -destip <i>ipaddress</i> -sys <i>sysname</i> -ins <i>instance_name</i> -memo <i>memo</i>	Add an instance.

Syntax of Command Line	Meaning
<code>./startclient.sh deploy -ip 127.0.0.1 -port 12212 -username admin -password admin rmins -ins <i>insname</i></code>	Delete an instance.
<code>./startclient.sh deploy -ip 127.0.0.1 -port 12212 -username admin -password admin buildHA -secondaryip <i>System IP address of the peer site</i></code>	Synchronize the primary and secondary sites.
<code>./startclient.sh deploy -ip 127.0.0.1 -port 12212 -username admin -password admin splitHA</code>	Separate the primary site from secondary sites.
<code>./startclient.sh deploy -ip 127.0.0.1 -port 12212 -username admin -password admin modifyhostname -hostip <i>ipaddress</i> -hostname <i>hostname</i></code>	Change the host name.
<code>./startclient.sh deploy -ip 127.0.0.1 -port 12212 -username admin -password admin modifyip -oldip <i>ipaddress</i> -newip <i>ipaddress</i> -netmask <i>netmask</i></code>	Change the IP address.
<code>./startclient.sh deploy -ip 127.0.0.1 -port 12212 -username admin -password admin changesapassword -username <i>username</i> -oldpassword <i>password</i> -newpassword <i>password</i></code>	Change the password of the database administrator

 NOTE

The maximum number of characters in a CLI command line is 255. Try to make the command strings simple and convenient.

Example for Using Command Lines

The following takes the operation of querying the deployment package installed on the U2000 on Solaris through command lines as an example:

1. Log in to the OS as the **nmsuser** user to open the terminal window.
2. Run the following commands to query the installed deployment package:

```
$ cd /opt/U2000/engineering
$ ./startclient.sh deploy -ip 127.0.0.1 -port 12212 -username admin -password admin query -type 1
```

D.2 Starting and Stopping the MSuite

This topic describes how to start and stop the MSuite.

D.2.1 Starting the Process of the MSuite Server

This topic describes how to start the process of the MSuite server.

D.2.2 Logging In to the MSuite Client

This topic describes how to log in to the MSuite client.

D.2.3 Exiting from the MSuite client

This topic describes how to exit from the MSuite client.

D.2.4 Ending the Process of the MSuite Server

This topic describes how to end the process of the MSuite server.

D.2.1 Starting the Process of the MSuite Server

This topic describes how to start the process of the MSuite server.

Context

Generally, the process of the MSuite server is started with the OS startup. If the process is not started, perform the following operations to start it.



NOTE

If the server is a Netra 240, V240, or V440 workstation, the process of the MSuite server is not started with the OS startup.

Procedure

- In Windows OS, check whether the **msdaemon.exe** and **msserver.exe** processes are started in the **Task Manager** window. If you can find the two processes in the process list, the MSuite server is running. If the two processes do not exist in the process list, the MSuite server is not running. In this case, perform the following operations to start the MSuite server:

Go to the **C:\HWENGR\engineering** path, and double-click the **startserver.bat** file.

- In Solaris or SUSE Linux OS, run the following command as user **root** to verify that the MSuite server is running:

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

The MSuite server is running if **/opt/HWNMSJRE/jre_sol/bin/java -server** is displayed. Run the following commands to start the MSuite server if it is not running:

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

----End

D.2.2 Logging In to the MSuite Client

This topic describes how to log in to the MSuite client.

Prerequisite

The MSuite server must be started.

Procedure

- 1 On a computer installed with the MSuite client, double-click the **U2000 NMS Maintenance Suite** shortcut icon on the desktop and then wait about one minute. The **Login** dialog box is displayed.

 NOTE

- In Solaris OS, log in to the Java desktop system as user **nmsuser**. Otherwise, the **U2000 NMS Maintenance Suite** shortcut icon is not displayed on the desktop. To start the MSuite client by running commands, run the following commands as user **nmsuser**:

```
cd /opt/U2000/engineering
./startclient.sh
```
- In SUSE Linux OS, log in to GUI-based desktop system as user **root**. Otherwise, the **U2000 NMS Maintenance Suite** shortcut icon is not displayed on the desktop. To start the MSuite client by running commands, you need to run the following command as the **nmsuser** user:

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

2 Set the login parameters.

The login parameters are described as follows:

- IP Address:
 - To log in to the local MSuite server, use the default IP address **127.0.0.1**.
 - To log in to the remote MSuite server, enter the IP address of the computer where the MSuite server is installed. If multiple IP addresses are configured for the computer, use the NMS application IP address.
- Port No.: The default port ID is **12212**. There is no need to change the default value during login but ensure that the port is not occupied.
- User Name: The default user name is **admin**.
- Password: The default password is **admin**.

3 Click **Login**.

 NOTE

- When you log in to the MSuite client, a progress bar is displayed showing the progress of querying components and instances. Wait until the operation is complete.
- The MSuite works in single-user mode. Specifically, only one MSuite client can log in to the MSuite at one time.

----End

Exception Handling

If a dialog box is displayed during the login, indicating that network configuration information is inconsistent and re-synchronization is required after login, read through the message to learn the server that needs to be synchronized. Then, synchronize the network configuration, for details, see [D.5.3 Synchronizing Network Configurations](#).

D.2.3 Exiting from the MSuite client

This topic describes how to exit from the MSuite client.

Procedure

- 1** On the MSuite client, choose **System > Exit**. The **Exit** dialog box is displayed.
- 2** Click **OK**.

----End

D.2.4 Ending the Process of the MSuite Server

This topic describes how to end the process of the MSuite server.

Procedure

- In Windows OS, go to the **C:\HWENGR\engineering** path, double-click the **stopserver.bat** file, and end the MSuite server process.
- In Solaris or SUSE Linux OS, run the following commands as user **root** to end the process of the MSuite server.

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

----End

D.3 System Management

This topic describes how to use the system management functions of the MSuite.

D.3.1 Refreshing the NMS Information

This topic describes how to refresh the NMS information. The information displayed on the MSuite client is not refreshed in real time. You can manually refresh the U2000 information immediately, such as the U2000 status and instance enabling status.

D.3.2 Synchronizing the NMS Information

This topic describes how to synchronize the component and instance deployment information on the U2000 server to the MSuite server in the U2000 single-server System.

D.3.3 Synchronizing the NMS Information (High Availability System)

This topic describes how to synchronize the component and instance deployment information on the U2000 server to the MSuite server in the U2000 high availability system.

D.3.4 Changing the Password of the MSuite

This topic describes how to change the password of the MSuite. To ensure the security of the U2000, change the password of the MSuite immediately and record the password after installing the U2000 server.

D.3.5 Logging Out of the MSuite Client

This topic describes how to log out of the current MSuite client. After you perform the logout operation, the **Login** dialog box is displayed.

D.3.1 Refreshing the NMS Information

This topic describes how to refresh the NMS information. The information displayed on the MSuite client is not refreshed in real time. You can manually refresh the U2000 information immediately, such as the U2000 status and instance enabling status.

Procedure

- 1 Log in to the MSuite client. For details, see [D.2.2 Logging In to the MSuite Client](#).

- 2 On the MSuite client, choose **System > Refresh NMS Information**. Alternatively, you can click the  icon on the toolbar.

----End

D.3.2 Synchronizing the NMS Information

This topic describes how to synchronize the component and instance deployment information on the U2000 server to the MSuite server in the U2000 single-server System.

Prerequisite

The database must be in the running state.

Context



CAUTION

The operations in this topic are applicable to the U2000 system.

- Single-Server System (Windows)
 - Single-Server System (Solaris)
 - Single-Server System (SUSE Linux-Distributed)
-

Procedure

- 1 Log in to the MSuite client. For details, see [D.2.2 Logging In to the MSuite Client](#).
- 2 On the MSuite client, choose **System > Synchronize NMS Information**. The **Synchronize Data** dialog box is displayed.
- 3 Click **OK**. The progress bar of data synchronization is displayed. Wait until a message is displayed indicating that data synchronization is complete.
- 4 Click **OK**. The deployment is successfully synchronized.
- 5 After the NMS information is synchronized, do as follows to restart the MSuite server.
 - In Windows OS, go to the **C:\HWENGR\engineering** path, double-click the **stopserver.bat** file, and end the MSuite server process.
After the NMS maintenance suite server is stopped, double-click the **startserver.bat** file to start the MSuite server process.
 - On Solaris or SUSE Linux OS, run the following commands as the **root** user:

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


After the MSuite server is stopped, run the following command to start it:

```
# ./startserver.sh
```

----End

D.3.3 Synchronizing the NMS Information (High Availability System)

This topic describes how to synchronize the component and instance deployment information on the U2000 server to the MSuite server in the U2000 high availability system.

Context



CAUTION

The operations in this topic are applicable to the U2000 system.

- High Availability System (Windows)
 - High Availability System (Solaris)
 - High Availability System (SUSE Linux-Distributed)
-

Procedure

- If the high availability system is running properly, do as follows:
 1. Log in to the MSuite server of the primary site.
 2. On the MSuite client, choose **System > Synchronize NMS Information**. The **Synchronize Data** dialog box is displayed.
 3. Click **OK**. The progress bar of data synchronization is displayed. Wait until a message is displayed indicating that data synchronization is complete.
 4. Click **OK**. The deployment is successfully synchronized.
 5. Log out of the MSuite client. For details, see [D.3.5 Logging Out of the MSuite Client](#).
 6. Switch the U2000 service to the standby site.
 7. After the service switching on the active and standby sites is complete, log in to the MSuite server of the secondary site.
 8. On the MSuite client, choose **System > Synchronize NMS Information**. The **Synchronize Data** dialog box is displayed.
 9. Click **OK**. The progress bar of data synchronization is displayed. Wait until a message is displayed indicating that data synchronization is complete.
 10. Click **OK**. The deployment is successfully synchronized.
 11. Log out of the MSuite client.
 12. Switch the U2000 service back to the primary site.
- If the high availability system is in dual-active state, do as follows:
 1. Log in to the MSuite server of the primary site.
 2. On the MSuite client, choose **Deploy > Dual primary**.
The process bar showing the dual-active process is displayed. Wait about five minutes until the dialog box indicating the dual-active success is displayed.
 3. On the MSuite client, choose **System > Synchronize NMS Information**. The **Synchronize Data** dialog box is displayed.

4. Click **OK**. The progress bar of data synchronization is displayed. Wait until a message is displayed indicating that data synchronization is complete.
5. Click **OK**. The deployment is successfully synchronized.
6. Log out of the MSuite client. For details, see [D.3.5 Logging Out of the MSuite Client](#).
7. Log in to the MSuite server of the secondary site.
8. On the MSuite client, choose **System > Synchronize NMS Information**. The **Synchronize Data** dialog box is displayed.
9. Click **OK**. The progress bar of data synchronization is displayed. Wait until a message is displayed indicating that data synchronization is complete.
10. Click **OK**. The deployment is successfully synchronized.
11. Log out of the MSuite client.
12. Log in to the MSuite server of the primary site.
13. On the MSuite client, choose **Deploy > Fore local site be primary**.
14. Click **OK**.
15. Log out of the MSuite client.

----End

Follow-up Procedure

After the NMS information is synchronized, do as follows on the primary and secondary sites to restart the MSuite server.

- In Windows OS, go to the **C:\HWENGR\engineering** path, double-click the **stopserver.bat** file, and end the MSuite server process.

After the NMS maintenance suite server is stopped, double-click the **startserver.bat** file to start the MSuite server process.

- On Solaris or SUSE Linux OS, run the following commands as the **root** user:
`cd /opt/HWENGR/engineering`
`./stopserver.sh`

After the MSuite server is stopped, run the following command to start it:

```
# ./startserver.sh
```

D.3.4 Changing the Password of the MSuite

This topic describes how to change the password of the MSuite. To ensure the security of the U2000, change the password of the MSuite immediately and record the password after installing the U2000 server.

Context

- In the single-server system (SUSE Linux-distributed), you only need to log in to the MSuite server of the master server and change the password of the MSuite. The passwords of the MSuites of slave servers are then automatically changed.
- In the high availability system (Windows) or high availability system (Solaris), you only need to log in to the MSuite server on the primary site and change the password of the MSuite. The password of the MSuite on the secondary site is then automatically changed.

- In the high availability system (SUSE Linux-distributed), you only need to log in to the MSuite server of the master server on the primary site and change the password of the MSuite. The passwords of the MSuites of other servers are then automatically changed.

Procedure

- 1 Log in to the MSuite client. For details, see [D.2.2 Logging In to the MSuite Client](#).
- 2 On the MSuite client, choose **System > Change Password** from the main menu. The **Change Password** dialog box is displayed.
- 3 Click **OK**. The **Change Password** dialog box is displayed.
- 4 Enter the old password and new password.



NOTE

The initial password is **admin**.

- 5 Click **OK**. The password is changed.

----End

D.3.5 Logging Out of the MSuite Client

This topic describes how to log out of the current MSuite client. After you perform the logout operation, the **Login** dialog box is displayed.

Procedure

- 1 On the MSuite client, choose **System > Logout**. The **Logout** dialog box is displayed.
- 2 Click **OK**.

----End

D.4 U2000 Deployment

This topic describes how to deploy the U2000. After the U2000 is installed, you can maintain or adjust the deployment of the U2000 through the MSuite.

[D.4.1 Adding a Component](#)

This topic describes how to add a component. After the U2000 is installed, if you need to add a certain function, you can use the MSuite to add the component for this function.

[D.4.2 Deleting a Component](#)

This topic describes how to delete a subsystem. If a certain function is unnecessary during the maintenance of the U2000, you can delete the component for this function to increase the running efficiency of the NMS.

[D.4.3 Adding an Instance](#)

This topic describes how to add an instance. When you install the U2000, the MSuite deploys an instance for each selected NE Explorer by default. When the number of NEs is beyond the management capability of an NE Explorer, you need to use the MSuite to add more NE Explorer instances to expand the management capability of the system.

[D.4.4 Deploying instances by License](#)

This topic describes how to deploy instances by license. If the U2000 license is already obtained, you can deploy instances in batches according to the type and number of devices supported by the license.

[D.4.5 Deleting an Instance](#)

This topic describes how to delete an instance. If an instance is unnecessary, you can delete this instance to improve the running efficiency of the NMS.

[D.4.6 Changing the Name and Remarks of an Instance](#)

This topic describes how to change the name and remarks of an instance. To distinguish instances, you can change the name of an instance or add the remarks of an instance.

[D.4.7 Setting the System Time and Time Zone](#)

This topic describes how to set the system time and time zone. During the maintenance of the U2000, you can use the MSuite to set the time and time zone of the U2000 server.

[D.4.8 Changing the Password of the Administrator of the Database](#)

This topic describes how to change the password of the administrator of the database. After installing the U2000, you can change the password of the administrator of the database through the MSuite.

[D.4.9 Changing the Password of the User of the Database](#)

This topic describes how to change the password of the user of the database. After the U2000 is installed, you can change the password of the user of the database through the MSuite.

[D.4.10 Configuring the NTP Service](#)

This topic describes how to configure the NTP service. After installing the U2000, you can configure the NTP service through the MSuite.

D.4.1 Adding a Component

This topic describes how to add a component. After the U2000 is installed, if you need to add a certain function, you can use the MSuite to add the component for this function.

Prerequisite

Ensure that the **/opt** directory has available space. You can run the **df -hk /opt** command to view the remaining space of the **/opt** directory.

Context

- In a distributed system, you only need to log in to the MSuite server of the master server to perform this operation.
- In a high availability system, you only need to log in to the MSuite server of the primary site to perform this operation.

**CAUTION**

- The operation of adding a component is not applicable to this scenario. You need to install the U2000 through the software package and only the single-domain component needs to be installed. For example, you need to upload only the component of the transport domain to the server for decompression and installation. The components of other domains need to be added later.
- If the U2000 patch is installed before you add a component, you need to reinstall the U2000 patch after adding the component. For details about the patch, see the *iManager U2000 Patch Release Notes* of the associated version. For details about how to install the patch, see the *iManager U2000 Patch Installation Guide* of the associated version.

Procedure

- 1 Log in to the MSuite client. For details, see [D.2.2 Logging In to the MSuite Client](#).
- 2 On the MSuite client, choose **Deploy > Add Component**. The **Add Component** dialog box is displayed.
- 3 Select the components to be added and click **OK**.

**NOTE**

Determine which component needs to be added according to the equipment and services managed by the U2000. If a component is already installed on the current server, you cannot install the second time. When you install a component for the second time, the system displays a message indicating that the component is already installed.

- 4 Wait until the dialog box is displayed to prompt the message **The component is successfully added**.
- 5 Click **OK**.

----End

Follow-up Procedure

After the component is added, the deployment package of the component is displayed on the **Deploy package** tab page. You need to deploy an instance for the component. Add an instance. For details about how to add an instance, see [D.4.3 Adding an Instance](#).

D.4.2 Deleting a Component

This topic describes how to delete a subsystem. If a certain function is unnecessary during the maintenance of the U2000, you can delete the component for this function to increase the running efficiency of the NMS.

Prerequisite

- Ensure that all MSuite servers are started.
- Ensure that no instance is deployed for the component.

Context

- If the component is deployed with instances, you need to delete the instances of this component first. For details, see [D.4.5 Deleting an Instance](#).
- In a distributed system, you only need to log in to the MSuite server of the master server to perform this operation.
- In a high availability system, you only need to log in to the MSuite server of the primary site to perform this operation.

Procedure

- 1 Log in to the MSuite client. For details, see [D.2.2 Logging In to the MSuite Client](#).
- 2 On the MSuite client, choose **Deploy > Remove Component**. The **Remove Component** dialog box is displayed.
- 3 Select the components to be deleted and click **OK**.



NOTE

The basic component and the components that are not installed cannot be deleted. You cannot select the components that cannot be deleted.

- 4 Wait until the dialog box is displayed to prompt the message **The component is successfully removed**.
- 5 Click **OK**.

----End

D.4.3 Adding an Instance

This topic describes how to add an instance. When you install the U2000, the MSuite deploys an instance for each selected NE Explorer by default. When the number of NEs is beyond the management capability of an NE Explorer, you need to use the MSuite to add more NE Explorer instances to expand the management capability of the system.

Prerequisite

- Ensure that the **/opt** directory has available space. You can run the **df -hk /opt** command to view the remaining space of the **/opt** directory.
- Ensure that the database is running.
- Ensure that the component for the instance to be added is installed. If the component is not installed, install it first. For details, see [D.4.1 Adding a Component](#).

Context

- In the single-server system (SUSE Linux-distributed), perform operations described here only on the MSuite server of the master server.
- In the high availability system (Windows) or high availability system (Solaris), you need to perform operations described here only on the MSuite server on the primary site.
- In the high availability system (SUSE Linux-distributed), perform operations described here only on the MSuite server of the master server at the primary site.
- Limited by the port quantity, the maximum instance number of a single-server multi-instance deployment package for the transport domain is 25.

Procedure

- 1 Log in to the MSuite client. For details, see [D.2.2 Logging In to the MSuite Client](#).
- 2 On the MSuite client, click the **Deployment Package** tab. Right-click the subsystem where the instance is added and choose **Add Instance** from the shortcut menu. The **Add Instance** dialog box is displayed.

 NOTE

If **Add Instance** is unavailable, the number of instances reaches the limit or the component does not support the addition of an instance.

- 3 Set the name of the instance to be added and click **OK**.
- 4 Wait until the dialog box is displayed prompting "The instance is successfully added."
- 5 Click **OK**.
- 6 **Optional:** If the system prompts you to restart the NMS, you need to perform this step on the System Monitor; otherwise, skip this step.

You can do as follows to restart NMS processes:

1. In the main window of the System Monitor, click the **Process Monitor** tab.
2. Choose **Administration > Stop All NMS Process** from the main menu.
3. After all processes are successfully stopped, choose **Administration > Start All NMS Process**.

----End

Operations Through the CLI

On Solaris or SUSE Linux OS, if you fail to log in to the GUI desktop system, add instances through the CLI.

The operations in CLI mode are as follows:

On Solaris OS, run the following command as user **nmsuser**. On SUSE Linux OS, run the following command as user **root**.

```
cd /opt/U2000/engineering
./startclient.sh deploy -ip 127.0.0.1 -port 12212 -username admin -password admin
deployins -destip ipaddress -sys sysname -ins instance_name -memo memo
```

 NOTE

The command parameters are described as follows:

- *sysname* indicates the ID of the deployment package. Run the following command to query the ID of the deployment package: `./startclient.sh deploy -ip 127.0.0.1 -port 12212 -username admin -password admin query -type 1`
- *ipaddress* indicates the NMS application IP address of the server where the MSuite is installed.

D.4.4 Deploying instances by License

This topic describes how to deploy instances by license. If the U2000 license is already obtained, you can deploy instances in batches according to the type and number of devices supported by the license.

Prerequisite

- Ensure that the database is running.
- You must ensure that the U2000 license is updated. For details about how to update the U2000 license.
- You must ensure that all MSuite servers are started.

Context

- Limited by the port quantity, the maximum instance number of a single-server multi-instance deployment package of the transport domain is 25.
- During the deployment of instances by license, the MSuite automatically checks whether the components corresponding to the instances are already installed. If the components are not installed, you need to add them one by one at the system prompt. For details about how to add components, see [D.4.1 Adding a Component](#).

Procedure

- 1 Log in to the MSuite client. For details, see [D.2.2 Logging In to the MSuite Client](#).
- 2 On the MSuite client, choose **Deploy > Deploy by License** from the main menu. The **Deploy by License** dialog box is displayed.
- 3 Click **Browser** to select the path of the folder where the license is stored. Then, click **Next**.
- 4 Click **OK**.



NOTE

If the system prompts you that the components corresponding to the instances are not installed, record the components that need to be installed, and then click **Exit**. Then, add the components by referring to [D.4.1 Adding a Component](#). After these component are added, perform the preceding operations again.

- 5 Click **OK**. The instances are deployed.
- 6 On the System Monitor, restart all NMS processes.
You can do as follows to restart NMS processes:
 1. In the main window of the System Monitor, click the **Process Monitor** tab.
 2. Choose **Administration > Stop All NMS Process** from the main menu.
 3. After all processes are successfully stopped, choose **Administration > Start All NMS Process**.

----End

D.4.5 Deleting an Instance

This topic describes how to delete an instance. If an instance is unnecessary, you can delete this instance to improve the running efficiency of the NMS.

Prerequisite

The database must be running.

Context

- In the single-server system (SUSE Linux-distributed), perform operations described here only on the MSuite server of the master server.
- In the high availability system (Windows) or high availability system (Solaris), you need to perform operations described here only on the MSuite server on the primary site.
- In the high availability system (SUSE Linux-distributed), perform operations described here only on the MSuite server of the master server at the primary site.

Procedure

- 1 Log in to the MSuite client. For details, see [D.2.2 Logging In to the MSuite Client](#).
- 2 On the MSuite client, click the **Instance** tab.
- 3 Right-click the instance to be deleted and choose **Delete Instance** from the shortcut menu. The **Delete Instance** dialog box is displayed.
- 4 Click **OK** to begin to delete the instance.
- 5 Wait while the system is deleting the instance. When the message **The instance is successfully deleted** is displayed, it indicates that the instance is successfully deleted.
- 6 Click **OK**.
- 7 **Optional:** If the system prompts you to restart the NMS, you need to perform this step on the System Monitor; otherwise, skip this step.
You can do as follows to restart NMS processes:
 1. In the main window of the System Monitor, click the **Process Monitor** tab.
 2. Choose **Administration > Stop All NMS Process** from the main menu.
 3. After all processes are successfully stopped, choose **Administration > Start All NMS Process**.

----End

Operations Through the CLI

On Solaris or SUSE Linux OS, if you fail to log in to the GUI desktop system, delete instance through the CLI.

The operations in CLI mode are as follows:

On Solaris OS, run the following command as user **nmsuser**. On SUSE Linux OS, run the following command as user **root**.

```
cd /opt/U2000/engineering
./startclient.sh deploy -ip 127.0.0.1 -port 12212 -username admin -password admin
rmins -ins insname
```

D.4.6 Changing the Name and Remarks of an Instance

This topic describes how to change the name and remarks of an instance. To distinguish instances, you can change the name of an instance or add the remarks of an instance.

Prerequisite

The database must be in the running state.

Procedure

- 1 Log in to the MSuite client. For details, see [D.2.2 Logging In to the MSuite Client](#).
- 2 On the MSuite client, select the instance whose information needs to be modified.
- 3 Right-click the instance and choose **Modify Instance Information** from the shortcut menu. Alternatively, choose **Deploy > Modify Instance Information** from the main menu. The **Modify Instance Information** dialog box is displayed.
- 4 Enter the new name and remarks of the instance.
- 5 Click **OK**. Wait until a message is displayed indicating that the instance information is successfully modified.
- 6 Click **OK**.

----End

D.4.7 Setting the System Time and Time Zone

This topic describes how to set the system time and time zone. During the maintenance of the U2000, you can use the MSuite to set the time and time zone of the U2000 server.

Prerequisite

The U2000 and database must be shut down. For details, see [E Shutting Down the U2000](#).

Context

- In a high availability system (Veritas hot standby), you need to log in to the MSuite server of the primary and secondary sites to respectively change the time and time zones of the primary and secondary sites. The time and time zone of the primary site can be different from those of the secondary site.
- In the Windows OS, the MSuite does not support this function.

Procedure

- 1 Log in to the MSuite client. For details, see [D.2.2 Logging In to the MSuite Client](#).
- 2 On the MSuite client, choose **Deploy > Modify time zone**. The **Modify the system time zone** dialog box is displayed.
- 3 Set the time zone and system time according to the local time zone and standard time.
- 4 Click **OK**.

----End

Follow-up Procedure

After changing the time and time zone, you need to restart the OS to make the modifications take effect. Restart the OS according to the displayed prompt.

D.4.8 Changing the Password of the Administrator of the Database

This topic describes how to change the password of the administrator of the database. After installing the U2000, you can change the password of the administrator of the database through the MSuite.

Prerequisite

- The NMS processes are ended. Perform the following operations to end the NMS processes if they are running:
 - For the Single-Server System (Windows), see [A.9.18 How to End the Processes of the U2000 Single-Server System on Windows](#).
 - For the Single-Server System (Solaris), see [A.9.21 How to End the Processes of the U2000 Single-Server System on Solaris](#).
 - For the Single-Server System (SUSE Linux-Distributed), see [A.9.24 How to End the Processes of the U2000 Single-Server System \(SUSE Linux-Distributed\)](#).
 - For the High Availability System (Windows), see [A.9.27 How to End the U2000 Processes of the High Availability System \(Windows\)](#).
 - For the High Availability System (Solaris), see [A.9.30 How to End the U2000 Processes of the High Availability System \(Solaris\)](#).
 - For the High Availability System (SUSE Linux-Distributed), see [A.9.33 How to End the U2000 Processes of the High Availability System \(SUSE Linux-Distributed\)](#).
- The database is running. Perform the following operations to start the database if it is not running:
 - For the Single-Server System (Windows), see [A.5.4 How to Start the SQL Server Database](#).
 - For the Single-Server System (Solaris), see [A.6.1.2 How to Start the Sybase Database Service](#).
 - For the Single-Server System (SUSE Linux-Distributed), see [A.7.5 How Can I Start the Oracle Database \(Single-Server System\)?](#).
 - For the High Availability System (Windows), see [A.5.4 How to Start the SQL Server Database](#).
 - For the High Availability System (Solaris), see [A.6.1.2 How to Start the Sybase Database Service](#).
 - For the High Availability System (SUSE Linux-Distributed), see [A.7.4 How to Start the Oracle Database in the High Availability System](#).

Context

- In Solaris OS, the Sybase database is installed and the administrator is user **sa**.
- In Windows OS, the SQL Server database is installed and the administrator is user **sa**.
- In SUSE Linux OS, the Oracle database is installed and the administrator is user **system**.



NOTE

In the high availability system (Veritas hot standby), change the password of the administrator of the database only on the MSuite server at the primary site. The passwords of the administrators of the databases at both the primary and secondary sites are changed.

Procedure

- 1 Log in to the MSuite client.
- 2 On the MSuite client, choose **Deploy > Change Database Administrator Password**. The **Change Database Administrator Password** dialog box is displayed.
- 3 Enter the old password and new password.

 NOTE

- In Solaris OS, the Sybase database is installed. The password of user **sa** of the Sybase database must be 6-30 characters long and consists of letters or digits. Special characters are not allowed.
- In Windows OS, the MS SQL Server database is installed. The password of user **sa** of the MS SQL Server database must consist of 6 to 30 characters that can be letters, digits, and underscores (_).
- In SUSE Linux OS, the Oracle database is installed. The password of user **system** of the Oracle database must be at least six characters long and consist of letters or digits. Special characters are not allowed.

- 4 Click **OK**. The password is changed.

----End

Operations Through the CLI

On Solaris or SUSE Linux OS, if you fail to log in to the GUI desktop system, change the password of the administrator of the database through the CLI.

The operations in CLI mode are as follows:

On Solaris OS, run the following command as user **nmsuser**. On SUSE Linux OS, run the following command as user **root**.

```
cd /opt/U2000/engineering
./startclient.sh deploy -ip 127.0.0.1 -port 12212 -username admin -password admin
changesapassword -username username -oldpassword password -newpassword password
```

D.4.9 Changing the Password of the User of the Database

This topic describes how to change the password of the user of the database. After the U2000 is installed, you can change the password of the user of the database through the MSuite.

Prerequisite

- Ensure that the NMS server programs are already stop.
- Ensure that the database is running.

Procedure

- 1 Log in to the MSuite client.
- 2 On the MSuite client, choose **Deploy > Change Database User Password**. The **Change Database User Password** dialog box is displayed.
- 3 Enter the old password and new password.

**NOTE**

- In the Solaris OS, the password must consist of no less than six characters that can be letters and digits. Special character is not allowed.
- In the Windows OS, the password must consist of no less than six characters that can be letters and digits. Special character is not allowed.
- In the SUSE Linux OS, the password must consist of no less than six characters that can be letters and digits. Special character is not allowed.

4 Click **OK**. The password is changed.

----End

D.4.10 Configuring the NTP Service

This topic describes how to configure the NTP service. After installing the U2000, you can configure the NTP service through the MSuite.

Prerequisite

- The U2000 and database must be shut down. For details, see [E Shutting Down the U2000](#).
- The time zone of the workstation must be the same as that of the tracked clock source.

Context

- The MSuite does not support the operation of configuring the U2000 server as the NTP server at the medium layer.
- In the Windows OS, using the MSuite to configure NTP is unavailable.

Procedure

- 1 Log in to the MSuite client. For details, see [D.2.2 Logging In to the MSuite Client](#).
- 2 On the MSuite client, choose **Deploy > Configure NTP**. The **Configure NTP** dialog box is displayed.
- 3 Enter the IP address of the NTP server, and then click **OK**.

 TIP

- If you need to configure the NMS server as the NTP server at the top layer, that is, external clock sources are not traced, set **NTP server IP** to *127.0.0.1*.
- If you need to configure the NMS server as the NTP client, that is, external clock sources are traced, set **NTP server IP** to the IP address of the server that is traced.

- 4 Click **OK**.
- 5 Restart the OS.

----End

Example

How to Configure the Primary Site as the NTP Server of the Highest Stratum and the Secondary Site as the NTP Client in the high availability system (Veritas hot standby), as Defined in the NTP Configuration Scheme, When No External Clock Source Is Available?

1. Configure the primary site as the NTP server of the highest stratum. Log in to the MSuite server of the primary site and configure the primary site by referring to the preceding steps. In the **NTP server IP** field, enter *127.0.0.1*.
2. Configure the secondary site as the NTP client. Log in to the MSuite server of the secondary site and configure the secondary site by referring to the preceding steps. In the **NTP server IP** field, enter the system IP address of the primary site.

D.5 Adjusting the NMS

This topic describes how to adjust the NMS. After the U2000 is installed, you can adjust the U2000 server parameters through the MSuite.

D.5.2 Configuring Routes

This topic describes how to configure routes. After the U2000 is installed, if the network configurations of the server change, you can configure the routes of the server through the MSuite.

D.5.3 Synchronizing Network Configurations

This topic describes how to synchronize network configurations. When a network configuration of the NMS server changes, you need to synchronize the network configuration so that the IP addresses of the MSuite and server are synchronized. Otherwise, the system displays a failure message during the login to the MSuite client.

D.5.1 Changing the Host Name and IP Address

If network configurations change, you must use the MSuite to change the IP address, host name, and route of the server.

If network configurations change, you must change the IP address, host name, and route of the server to ensure normal running the U2000. If the U2000 has been installed on the server, you must use the MSuite to change the IP address, host name, and route of the server in compliance with the following rules:

- In the scenario of a high availability system, you must separate the primary site from the secondary site and then change the host names and IP addresses for the primary site and secondary site.
- The U2000 processes must be stopped.
- The database must be running.
- The new host name must comply with the host name naming rule.
 - 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
remoteclass

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								

- If NBIs and instances are deployed and the xFtp monitor is configured before the host name and IP address are changed, you must configure NBIs on the MSuite client and re-configure the xFtp monitor on the U2000 client after changing the IP address and host name.
- It is recommended that you back up the database in time after changing the IP address and host name.

Example

The procedure for changing the IP address and host name varies according to U2000 deployment schemes. Details are as follows:

- For information on how to change the IP address and host name on a GUI for a single-server system (Windows), see [D.5.1.1 How to Change the IP Address of the Single-Server System on Windows](#) and [D.5.1.2 How to Change the Host Name of the Single-Server System on Windows](#).
- For information on how to change the IP address and host name on a GUI for a single-server system (Solaris), see [D.5.1.3 How to Change the IP Address and Host Name for the Single-Server System \(Solaris\)](#).
- For information on how to change the IP address and host name on a GUI for a single-server system (SUSE Linux-distributed), see [D.5.1.4 How to Change the IP Address and Host Name of the Single-Server System \(SUSE Linux-Distributed\)](#).
- For information on how to change IP addresses and host names on a GUI for a high availability system (Windows), see [D.5.1.5 How to Modify the Server IP Address of High Availability System \(Windows\)](#) and [D.5.1.6 How to Change the Host Name of the High Availability System \(Windows\)](#).
- For information on how to change IP addresses and host names on a GUI for a high availability system (Solaris), see [D.5.1.7 How to Change the IP Address and Host name for the High Availability System \(Solaris\)](#).
- For information on how to change IP addresses and host names on a GUI for a high availability system (SUSE Linux-distributed), see [D.5.1.8 How to Change the IP Address and Host Name of the High Availability System \(SUSE Linux-Distributed\)](#).

 NOTE

On Solaris or SUSE Linux OS, if you fail to log in to the GUI desktop system, modify the IP address and host name of the server through the CLI.

Before using commands to change the IP address and host name, make sure that the preceding requirements are met. Details are as follows:

On Solaris OS, run the following command as user **nmsuser**. On SUSE Linux OS, run the following command as user **root**.

- Run the following command to change the IP address:

```
cd /opt/U2000/engineering
./startclient.sh deploy -ip 127.0.0.1 -port 12212 -username admin -
password admin modifyip -oldip ipaddress -newip ipaddress -netmask netmask
```

After this operation, restart the OS to make the new IP address take effect.

- Run the following commands to change the host name:

```
cd /opt/U2000/engineering
./startclient.sh deploy -ip 127.0.0.1 -port 12212 -username admin -
password admin modifyhostname -hostip ipaddress -hostname hostname
```

After this operation, restart the OS to make the new host name take effect.

D.5.1.1 How to Change the IP Address of the Single-Server System on Windows

Question

How do I to change the server IP address when the networking plan is changed?



CAUTION

If the server IP address or host name is changed, the previously backed up data cannot be used for restoration. In such a case, you need to back up the data again.

Do not change an IP address and a host name at the same time. Otherwise, the U2000 fails to be started.

Changing an IP address includes the following major steps:

1. Shut down the U2000 server and client, and ensure that the database is running.
2. Shut down the U2000 MSuite server.
3. Change the IP address of the U2000 server.
4. Start the U2000 MSuite server.
5. Log in to the U2000 MSuite client and synchronize IP address changes in configuration files. If the IP address changes are not synchronized, the U2000 fails to start properly.
6. Restart the OS.

Answer

- 1 Shut down the NMS server and client.

In the directory of the NMS software after the installation, for example, the **D:\U2000\server\bin** directory, run the **stopnms.bat** file to end the NMS processes.

**NOTE**

Ensure that the database is started.

2 End the server process of the MSuite.

In the **C:\HWENGR\engineering** directory, double-click the **stopserver.bat** file to end the server process of the MSuite.

3 In the classic start menu mode, choose **Start > Settings > Network Connections**.**4** In the **Network Connections** dialog box that is displayed, right-click the network connection to be configured and choose **Properties** from the shortcut menu.**5** On the **General** tab page (for the local connection) or **Network** tab page (for all other connections), select **Internet Protocol (TCP/IP)**. Then, click **Properties**.**6** In the **Internet Protocol (TCP/IP) Properties** dialog box that is displayed, enter the new IP address, subnet mask, and default gateway address, and perform the related modification. Click **OK**.**7** Start the server process of the MSuite.

In the **C:\HWENGR\engineering** directory, double-click the **startserver.bat** file to start the server process of the MSuite.

8 Log in to the MSuite client.

1. On the computer where the MSuite client is installed, double-click the **U2000 MSuite** shortcut icon on the desktop. Wait about one minute. The **Login** dialog box is displayed.
2. Set the related login parameters and click **OK**. The **NMS maintenance suite** window is displayed.
 - **IP Address**: Indicates the system IP address of the computer where the MSuite server is installed.
 - **Port No.**: The default port number is **12212**. You do not need to change the default value during login.
 - **User Name and Password**: Both the default user name and default password are **admin**.

**NOTE**

A dialog box may be displayed during the process of logging in to the MSuite client. Click **OK** according to the prompt.

9 On the **Server** tab page, right-click the server to be configured and choose **Synchronize the network configuration** from the shortcut menu. Click **OK**.**10** Restart the OS.**NOTE**

If NBIs and instances are deployed and the xFtp monitor is configured before the IP address is changed, you must configure NBIs on the MSuite client and re-configure the xFtp monitor on the U2000 client after changing the IP address.

- For details about how to configure NBIs, see the related NBI user guide.
- For details about how to configure the xFtp monitor, see the U2000 Help.

----End

D.5.1.2 How to Change the Host Name of the Single-Server System on Windows

Question

How do I change the host name of the single-server system on Windows?



CAUTION

If the server IP address or host name is changed, the previously backed up data cannot be used for restoration. In such a case, you need to back up the data again.

Do not change an IP address and a host name at the same time. Otherwise, the U2000 fails to be started.

Changing the host name includes the following major steps:

1. Shut down the U2000 server and client.
2. Change the host name of the U2000 server.
3. Restart the OS.
4. Log in to the U2000 MSuite client and synchronize host name changes in configuration files. If the host name changes are not synchronized, the U2000 fails to start properly.

Answer

- 1 Log in to the OS as a user with administrator rights.
- 2 Shut down the NMS server and client.

In the directory of the NMS software after the installation, for example, the **D:\U2000\server\bin** directory, run the **stopnms.bat** file to end the NMS processes.

- 3 Perform the following operations to change the host name of the server:
 1. On the desktop, right-click the **My Computer** icon and choose **Properties** from the shortcut menu.
 2. In the dialog box that is displayed, click the **Computer Name** tab, and then click **Change**.
 3. In the dialog box that is displayed, change the computer name, and then click **OK**.
 4. Restart the OS.
- 4 Log in to the MSuite client.
 1. On the computer where the MSuite client is installed, double-click the **U2000 MSuite** shortcut icon on the desktop. Wait about one minute. The **Login** dialog box is displayed.
 2. Set the related login parameters and click **OK**. The **NMS maintenance suite** window is displayed.
 - IP Address: Indicates the system IP address of the computer where the MSuite server is installed.
 - Port No.: The default port number is **12212**. You do not need to change the default value during login.

- User Name and Password: Both the default user name and default password are **admin**.

**NOTE**

A dialog box may be displayed during the process of logging in to the MSuite client. Click **OK** according to the prompt.

- 5 On the **Server** tab page, right-click the server to be configured and choose **Synchronize the network configuration** from the shortcut menu. Click **OK**.

----End

D.5.1.3 How to Change the IP Address and Host Name for the Single-Server System (Solaris)

Question

How to change the IP address and host name for the single-server system (Solaris)?

Answer

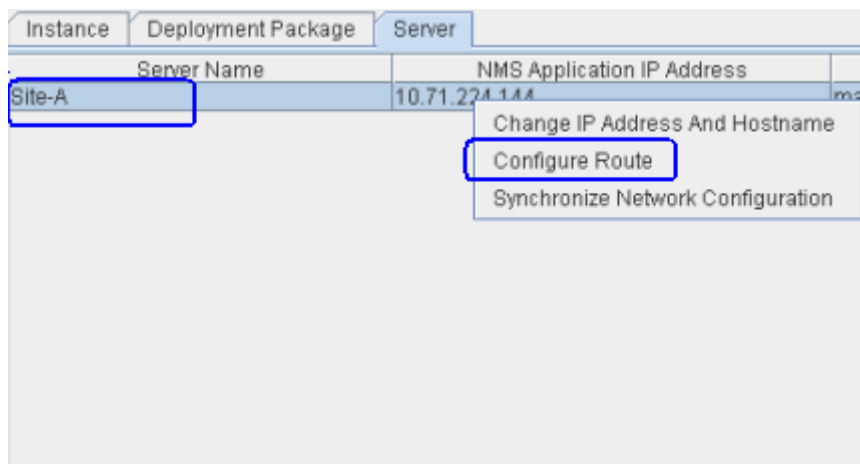
**NOTE**

To change the IP address and host name for the single-server system (Solaris), do as follows:

1. Stop U2000 server processes.
2. Use the MSuite to change the IP address and host. If a route is changed, reconfigure the route.
3. Restart the OS to make the modifications take effect.

- 1 Log in to the OS of the server as user **nmsuser**.
- 2 Open a terminal window and run the following commands to end U2000 processes.

```
$ cd /opt/U2000/server/bin
$ ./stopnms.sh
```
- 3 After the processes are ended, **log in to the MSuite client**.
- 4 On the MSuite client, click the **Server** tab.
- 5 If the route changes, do as follows to add a route. If the route does not change, you do not need to change the IP address or host name. Instead, skip this step.
 1. Right-click the server name and choose **Configure Route** from the shortcut menu.



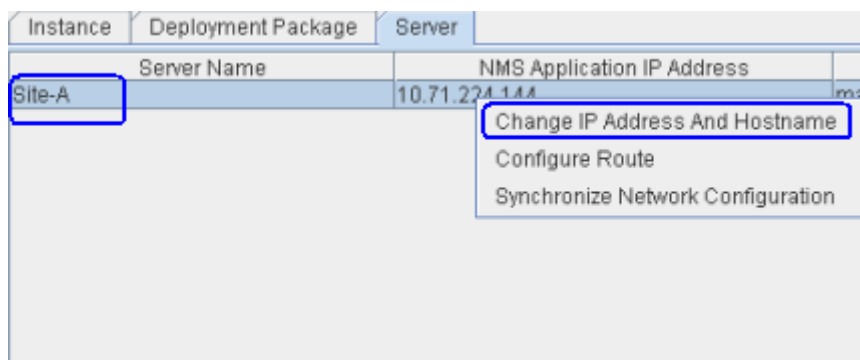
2. In the dialog box that is displayed, click **Add** or **Delete** according to actual route conditions to re-configure the route.

Destination	Subnet Mask	Route
0.0.0.0	0.0.0.0	10.71.224.1
10.71.224.0	255.255.254.0	10.71.224.144
127.0.0.1	255.255.255.255	127.0.0.1

3. Click **OK**.

6 Do as follows to change the host name and IP address.

1. Right-click the server name and choose **Change IP Address And Hostname** from the shortcut menu.



2. In the **Change IP Address And Hostname** dialog box, enter the new host name, IP address, and subnet mask.

Local IP Address:

Interface	IP Address	Host Name	Subnet Mask	IP Type
e1000g0	10.71.210.31	T522021031	255.255.254.0	SYSIP

3. Click **OK**. The progress bar is displayed. Wait patiently.
 4. After the configuration is complete, the **Message** dialog box is displayed, asking you to restart the OS and back up the database in time. click **OK**.
- 7** Restart the OS for the settings to take effect.

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

 NOTE

If NBIs and instances are deployed and the xFtp monitor is configured before the host name and IP address are changed, you must configure NBIs on the MSuite client and re-configure the xFtp monitor on the U2000 client after changing the IP address and host name.

- For details about how to configure NBIs, see the related NBI user guide.
- For details about how to configure the xFtp monitor, see the U2000 Help.

----End

D.5.1.4 How to Change the IP Address and Host Name of the Single-Server System (SUSE Linux-Distributed)

Question

How to change the IP address and host name of the Single-Server System (SUSE Linux-Distributed)?

Answer

 NOTE

To change the IP address and host name for the single-server system (Solaris), do as follows:

1. Stop U2000 server processes.
2. Use the MSuite to change the IP address and host. If a route is changed, reconfigure the route.
3. Restart the OS to make the modifications take effect.

- 1 Log in to the OS of the master server as user **root**.
- 2 Open a terminal window and run the following commands to end U2000 processes.

```
# cd /opt/U2000/server/bin  
# ./stopnms.sh
```
- 3 Log in to the slave server as user **root**. Open a terminal window and run the following command to end the **daem** process of the slave server:

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



CAUTION

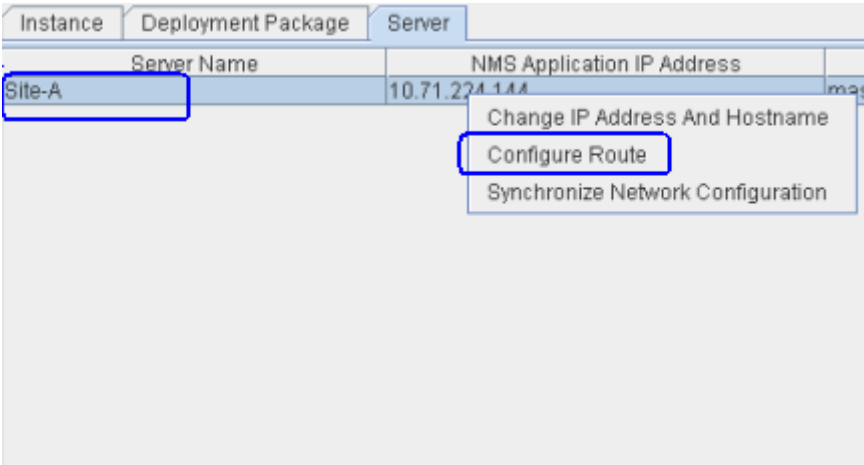
If multiple slave servers are installed, perform this step on every slave server.

- 4 After the **daem** process is ended, **log in to the MSuite client**.

 NOTE

The IP address entered during login is the system IP address of the master server.

- 5 On the MSuite client, click the **Server** tab.
- 6 If the route changes, do as follows to add a route. If the route does not change, you do not need to change the IP address or host name. Instead, skip this step.
 1. Right-click the server name and choose **Configure Route** from the shortcut menu.



2. In the dialog box that is displayed, click **Add** or **Delete** according to actual route conditions to re-configure the route.

Destination	Subnet Mask	Route
0.0.0.0	0.0.0.0	10.71.224.1
10.71.224.0	255.255.254.0	10.71.224.144
127.0.0.1	255.255.255.255	127.0.0.1

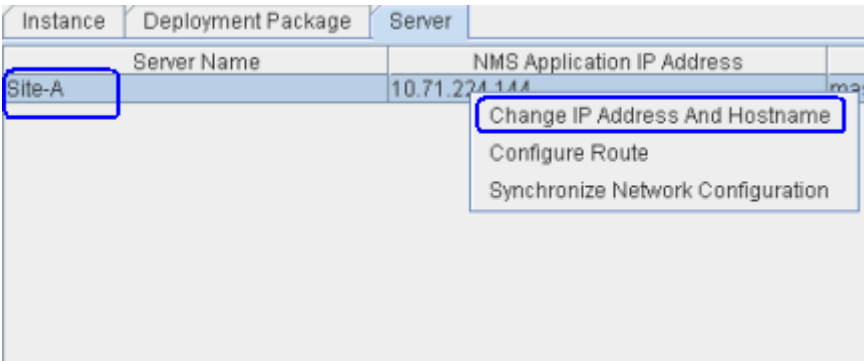
Add

Delete

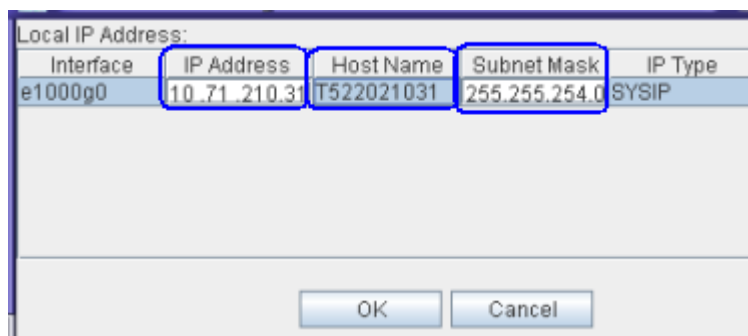
3. Click **OK**.

7 Do as follows to change the host name and IP address.

1. Right-click the server name and choose **Change IP Address And Hostname** from the shortcut menu.



2. In the **Change IP Address And Hostname** dialog box, enter the new host name, IP address, and subnet mask.



3. Click **OK**. The progress bar is displayed. Wait patiently.
4. After the configuration is complete, the **Message** dialog box is displayed, asking you to restart the OS and back up the database in time. click **OK**.
- 8 Restart the OS of the server whose host name and IP address are changed for the settings to take effect.

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

NOTE

1. If NAT networking was used, you must re-configure the **ipmap.cfg** file after the OS is restarted. For details, see [A.9.36 How to Configure the ipmap.cfg Mapping File](#).
2. If NBIs and instances are deployed and the xFtp monitor is configured before the host name and IP address are changed, you must configure NBIs on the MSuite client and re-configure the xFtp monitor on the U2000 client after changing the IP address and host name.
 - For details about how to configure NBIs, see the related NBI user guide.
 - For details about how to configure the xFtp monitor, see the U2000 Help.

----End

D.5.1.5 How to Modify the Server IP Address of High Availability System (Windows)

Question

How do I to change the server IP address when the networking plan is changed?



CAUTION

If the server IP address or host name is changed, the previously backed up data cannot be used for restoration. In such a case, you need to back up the data again.

Do not change an IP address and a host name at the same time. Otherwise, the U2000 fails to be started.

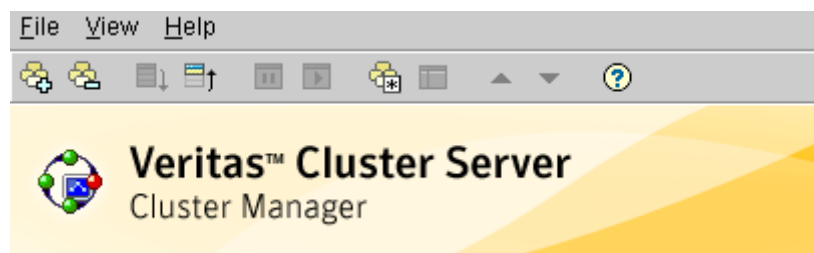
Changing an IP address includes the following major steps:

1. Separate the primary and secondary sites.
2. Shut down the U2000 server and client, and ensure that the database is running.
3. Shut down the U2000 MSuite server.

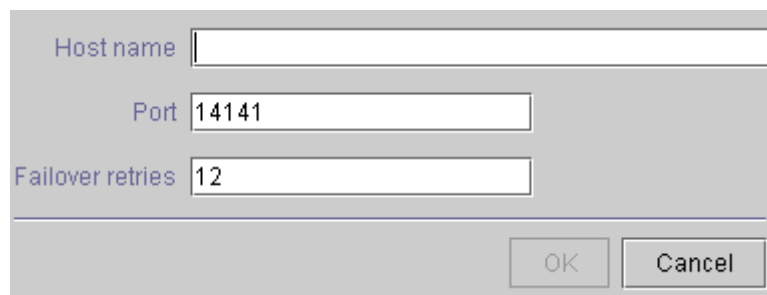
4. Change the IP address of the U2000 server.
5. Change the system IP address that is set in the VCS.
6. Start the U2000 MSuite server.
7. Log in to the U2000 MSuite client and synchronize IP address changes in configuration files. If the IP address changes are not synchronized, the U2000 fails to start properly.
8. Restart the OS.
9. Import the datadg disk group.
10. Synchronize the primary and secondary sites and reestablish their high availability relationship.

Answer

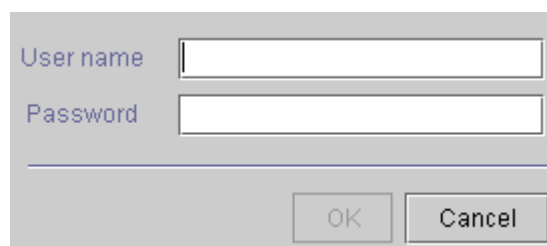
- 1 Log in to the NMS maintenance tool client. Choose **Deploy > Separate the primary and secondary sites**. The **Separate the primary and secondary sites** dialog box is displayed.
- 2 Click **OK**. The progress bar is displayed indicating the status of separating the primary and secondary sites. Wait until the dialog box is displayed indicating that the separation is complete.
- 3 Click **OK**.
- 4 On the primary site, perform the following operations to end the U2000 processes:
 1. Choose **Start > Programs > Symantec > Veritas Cluster Server > Veritas Cluster Manager - Java Console** to start the VCS client.



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



3. Enter the IP address of the system of the primary site. Then, click **OK**.



4. Enter the default user name **admin** and the default password **password** of the VCS client. Then, click **OK**.
5. Right-click **AppService** in the navigation tree and choose **Offline** > *host_name* from the shortcut menu.
6. In the dialog box that is displayed, click **Yes**.
- 5 Perform the following operations on the primary site to start the database:
 1. In the navigation tree, right-click **AppService-SQLServer2000**, and then choose **Online** > *host_name* from the shortcut menu.
 2. In the dialog box that is displayed, click **Yes**.
- 6 **Optional:** If the IP address is required to be changed on the secondary site, perform the preceding operations to start the database on the secondary site.
- 7 End the server process of the MSuite.

In the **C:\HWENGR\engineering** directory, double-click the **stopserver.bat** file to end the server process of the MSuite.
- 8 In the classic start menu mode, choose **Start** > **Settings** > **Network Connections**.
- 9 In the **Network Connections** dialog box that is displayed, right-click the network connection to be configured and choose **Properties** from the shortcut menu.
- 10 On the **General** tab page (for the local connection) or **Network** tab page (for all other connections), select **Internet Protocol (TCP/IP)**. Then, click **Properties**.
- 11 In the **Internet Protocol (TCP/IP) Properties** dialog box that is displayed, enter the new IP address, subnet mask, and default gateway address, and perform the related modification. Click **OK**.
- 12 Modify the system IP address in the VCS. Open the CLI and run the following commands:

C : \> **haconf -makerw**

C : \> **haclus -modify ClusterAddress** *system IP address of the primary site*

 **NOTE**

When running the preceding commands on the secondary site, enter the system IP address of the secondary site.

C : \> **haconf -dump -makero**
- 13 Start the server process of the MSuite.

In the **C:\HWENGR\engineering** directory, double-click the **startserver.bat** file to start the server process of the MSuite.
- 14 Log in to the MSuite client.
 1. On the computer where the MSuite client is installed, double-click the **U2000 MSuite** shortcut icon on the desktop. Wait about one minute. The **Login** dialog box is displayed.
 2. Set the related login parameters and click **OK**. The **NMS maintenance suite** window is displayed.
 - **IP Address:** Indicates the system IP address of the computer where the MSuite server is installed.

- Port No.: The default port number is **12212**. You do not need to change the default value during login.
- User Name and Password: Both the default user name and default password are **admin**.



NOTE

A dialog box may be displayed during the process of logging in to the MSuite client. Click **OK** according to the prompt.

- 15 On the **Server** tab page, right-click the server to be configured and choose **Synchronize the network configuration** from the shortcut menu. Click **OK**.
- 16 Restart the OS.
- 17 After the OS is restarted, run the following command to import the disk group **datadg**:
`C : \> vxdg -g datadg -s import`
- 18 Choose **Deploy > Synchronize the primary and secondary sites** on the primary site. The **Synchronize the primary and secondary sites** dialog box is displayed.
- 19 Enter the IP address of the remote server.



NOTE

Here, **Remote IP** refers to the IP address of the secondary site.

- 20 Click **OK**. A progress bar is displayed indicating the synchronization progress between the primary and secondary sites. Wait approximately 20 minutes until a dialog box is displayed indicating that the synchronization is completed.
- 21 Click **OK**. The synchronization between the primary and secondary sites is complete.

----End

Postrequisite



NOTE

If NBIs and instances are deployed and the xFtp monitor is configured before the IP address is changed, you must configure NBIs on the MSuite client and re-configure the xFtp monitor on the U2000 client after changing the IP address.

- For details about how to configure NBIs, see the related NBI user guide.
- For details about how to configure the xFtp monitor, see the U2000 Help.

D.5.1.6 How to Change the Host Name of the High Availability System (Windows)

Question

How do I change the host name of the high availability system (Windows)?



CAUTION

If the server IP address or host name is changed, the previously backed up data cannot be used for restoration. In such a case, you need to back up the data again.

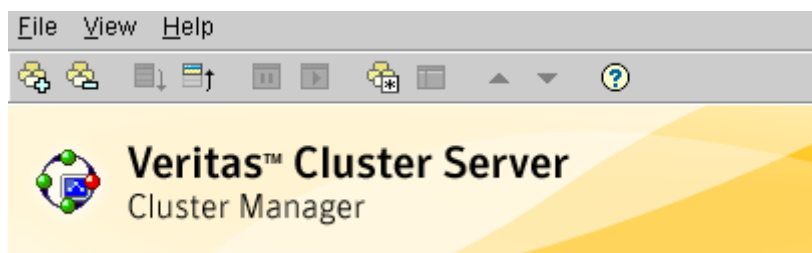
Do not change an IP address and a host name at the same time. Otherwise, the U2000 fails to be started.

Changing the host name includes the following major steps:

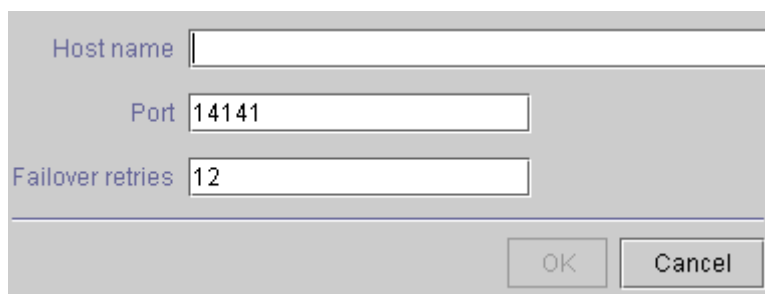
1. Shut down the U2000 server and client.
2. Stop the VCS service and communication.
3. Change the host name changes in configuration files.
4. Change the host name of the U2000 server.
5. Restart the OS.
6. Log in to the U2000 MSuite client and synchronize host name changes in configuration files. If the host name changes are not synchronized, the U2000 fails to start properly.

Answer

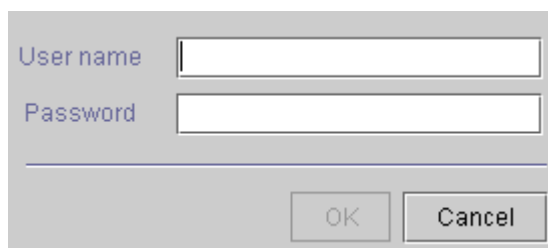
- 1 Log in to the OS as a user with administrator rights.
- 2 At the primary site, perform the following operations to end the U2000 processes:
 1. Choose **Start > Programs > Symantec > Veritas Cluster Server > Veritas Cluster Manager - Java Console** to start the VCS client.



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



3. Enter the IP address of the system of the primary site. Then, click **OK**.



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

- 3 To stop the VCS service, run the following command on the server whose host name is to be changed:
C : \> hstop -all -force
 - 4 To stop the VCS communication, run the following command on the server whose host name is to be changed:
C : \> net stop llt

Enter **y** and press Enter at prompt.
 - 5 Navigate to the **C:\Program Files\Veritas\comms\llt** path. Then, change the host name in the **llthosts.txt** file to a new one. You need to perform this step on the server whose host name is to be changed.
 - 6 Navigate to the **C:\Program Files\Veritas\comms\llt** path. Then, change the host name in the **llttab.txt** file to a new one. You need to perform this step on the server whose host name is to be changed.
 - 7 Navigate to the **C:\Program Files\Veritas\Cluster Server\conf** path. Then, change the host name in the **sysname** file to the new host name. You need to perform this step on the server whose host name is to be changed.
 - 8 Navigate to the **C:\Program Files\Veritas\cluster server\conf\config** path. Then, change the host name in the **main.cf** file to the new host name. You need to perform this step on the server whose host name is to be changed.
 - 9 Perform the following operations to change the host name of the server:
 1. On the desktop, right-click the **My Computer** icon and choose **Properties** from the shortcut menu.
 2. In the dialog box that is displayed, click the **Computer Name** tab, and then click **Change**.
 3. In the dialog box that is displayed, change the computer name, and then click **OK**.
 4. Restart the OS.
 - 10 Log in to the MSuite client.
 1. On the computer where the MSuite client is installed, double-click the **U2000 MSuite** shortcut icon on the desktop. Wait about one minute. The **Login** dialog box is displayed.
 2. Set the related login parameters and click **OK**. The **NMS maintenance suite** window is displayed.
 - **IP Address**: Indicates the system IP address of the computer where the MSuite server is installed.
 - **Port No.**: The default port number is **12212**. You do not need to change the default value during login.
 - **User Name and Password**: Both the default user name and default password are **admin**.
-  **NOTE**
A dialog box may be displayed during the process of logging in to the MSuite client. Click **OK** according to the prompt.
- 11 On the **Server** tab page, right-click the server to be configured and choose **Synchronize the network configuration** from the shortcut menu. Click **OK**.

- 12 Optional:** If the host name of the Veritas high availability system on the secondary site also needs to be changed, perform primary/secondary site switchover and then repeat the preceding steps to change the host name of the Veritas high availability system on the secondary site.

----End

D.5.1.7 How to Change the IP Address and Host name for the High Availability System (Solaris)

Question

How do I change the IP address and host name for the High Availability System (Solaris)?

Answer



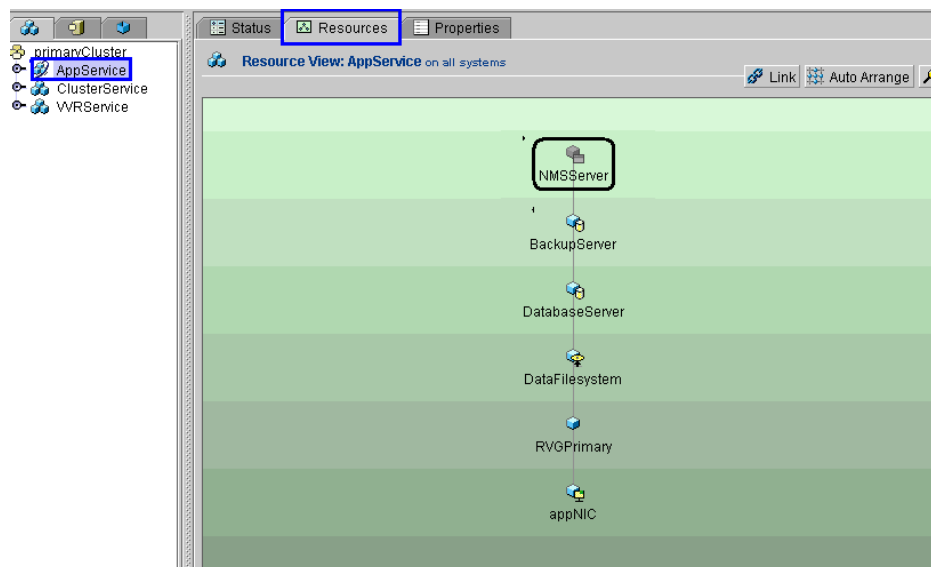
NOTE

To change the IP address and host name for the single-server system (Solaris), do as follows:

1. Use the MSuite to separate the primary site from the secondary site.
2. Log in to a VCS client and ensure that the **NMSServer** resource is in **offline** state and other resources are in **online** state on the primary site.
3. Use the MSuite to change the IP address and host name for the primary site. If a route is changed, reconfigure the route.
4. Restart the OS to make the modifications take effect.
5. Log in to a VCS client and ensure that the **NMSServer** resource is in **offline** state and other resources are in **online** state on the secondary site.
6. Use the MSuite to change the IP address and host name for the secondary site. If a route is changed, reconfigure the route.
7. Restart the OS to make the modifications take effect.
8. Use the MSuite to reconnect the primary and secondary sites.

- 1 Log in to the MSuite of primary site.**
- 2 Separate the primary site from the secondary site.** For details, see [D.6.2 Deleting the HA Relationship Between the Primary and Secondary Sites](#).
- 3 Log in to the VCS clients of the primary site.** For details, see [A.4.3.2 How to Log in and Exit the VCS \(Veritas Cluster Server\)](#).
- 4 On the VCS client, choose **AppService > Resources** and ensure that the **NMSServer** resource of the primary site is in the **offline** state and other resources are in the **online** state.**

Figure D-4 High Availability System (Solaris) resources



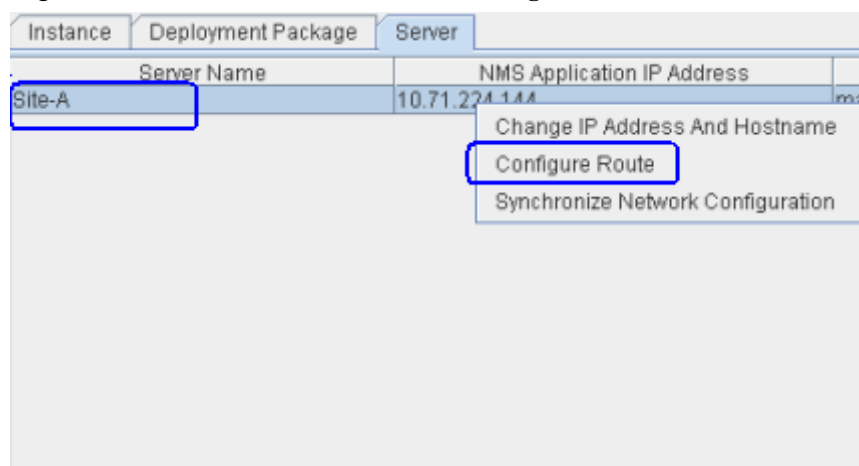
NOTE

- Resources whose icons are grayed out are in the **offline** state. For example, the **NMSServer** resource in the preceding figure. Resources whose resource icons are not grayed out are in the **online** state. For example, the **BackupServer** resource in the preceding figure.
- Check the status of all resources and ensure that the **NMSServer** resource is in the **offline** state and other resources are in the **online** state.
- To make a resource online, right-click the resource and choose **online > hostname** from the shortcut menu. In the **Question** dialog box, click **Yes**.
- To make a resource offline, right-click the resource and choose **offline > hostname** from the shortcut menu. In the **Question** dialog box, click **Yes**.

5 On the MSuite client, click the **Server** tab.

6 If the route changes, do as follows to add a route. If the route does not change, you do not need to change the IP address or host name. Instead, skip this step.

- Right-click the server name and choose **Configure Route** from the shortcut menu.



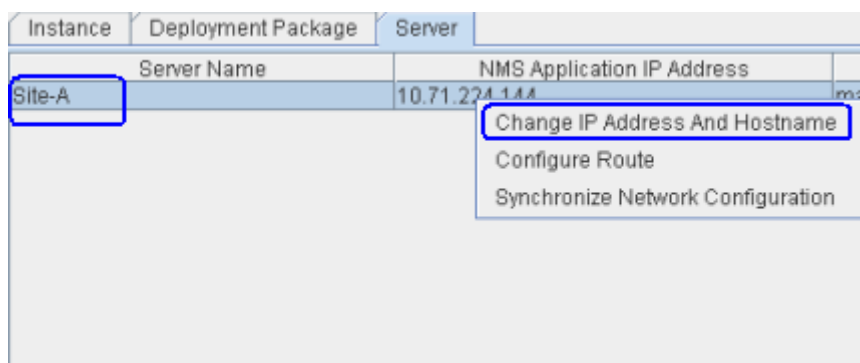
- In the dialog box that is displayed, click **Add** or **Delete** according to actual route conditions to re-configure the route.

Destination	Subnet Mask	Route
0.0.0.0	0.0.0.0	10.71.224.1
10.71.224.0	255.255.254.0	10.71.224.144
127.0.0.1	255.255.255.255	127.0.0.1

3. Click **OK**.

7 Do as follows to change the host name and IP address.

1. Right-click the server name and choose **Change IP Address And Hostname** from the shortcut menu.



2. In the **Change IP Address And Hostname** dialog box, enter the new host name, IP address, and subnet mask.

Local IP Address:

Interface	IP Address	Host Name	Subnet Mask	IP Type
e1000g0	10.71.210.31	T522021031	255.255.254.0	SYSIP

3. Click **OK**. The progress bar is displayed. Wait patiently.

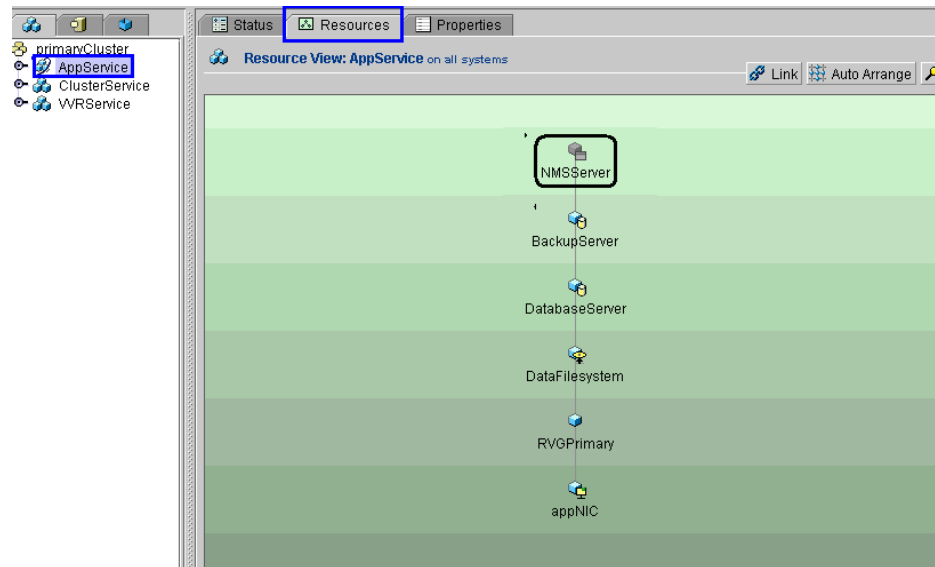
4. After the configuration is complete, the **Message** dialog box is displayed, asking you to restart the OS and back up the database in time. click **OK**.

8 Restart the OS of the server whose host name and IP address are changed for the settings to take effect.

```
# cd /opt/VRTSvcs/bin
# hastop -all -force
# sync;sync;sync;sync
# shutdown -y -g0 -i6
```


- 9 Log in to the VCS clients of the secondary site. For details, see [A.4.3.2 How to Log in and Exit the VCS \(Veritas Cluster Server\)](#).
- 10 On the VCS client, choose **AppService > Resources** and ensure that the **NMSServer** resource of the secondary site is in the **offline** state and other resources are in the **online** state.

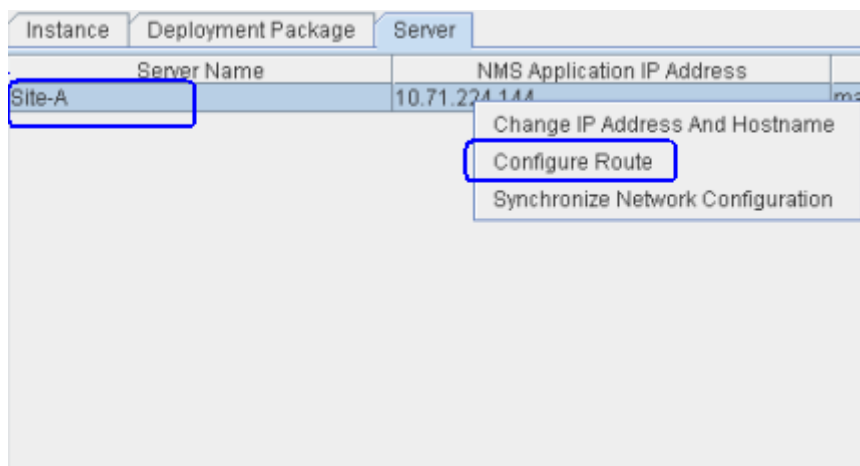
Figure D-5 High Availability System (Solaris) resources



NOTE

- Resources whose icons are grayed out are in the **offline** state. For example, the **NMSServer** resource in the preceding figure. Resources whose resource icons are not grayed out are in the **online** state. For example, the **BackupServer** resource in the preceding figure.
- Check the status of all resources and ensure that the **NMSServer** resource is in the **offline** state and other resources are in the **online** state.
- To make a resource online, right-click the resource and choose **online > hostname** from the shortcut menu. In the **Question** dialog box, click **Yes**.
- To make a resource offline, right-click the resource and choose **offline > hostname** from the shortcut menu. In the **Question** dialog box, click **Yes**.

- 11 [Log in to the MSuite of secondary site.](#)
- 12 On the MSuite client, click the **Server** tab.
- 13 If the route changes, do as follows to add a route. If the route does not change, you do not need to change the IP address or host name. Instead, skip this step.
 1. Right-click the server name and choose **Configure Route** from the shortcut menu.



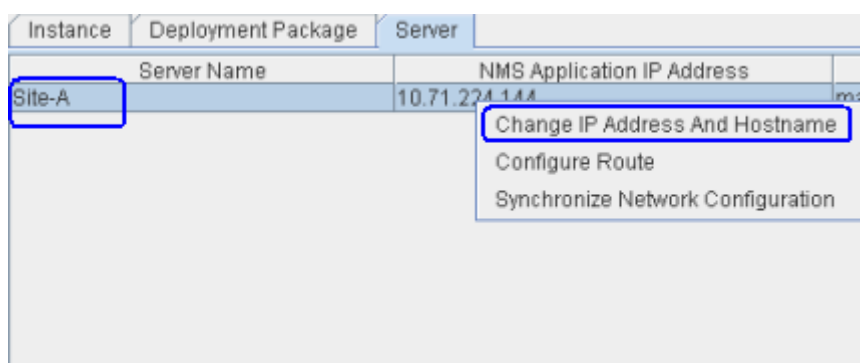
- In the dialog box that is displayed, click **Add** or **Delete** according to actual route conditions to re-configure the route.

Destination	Subnet Mask	Route
0.0.0.0	0.0.0.0	10.71.224.1
10.71.224.0	255.255.254.0	10.71.224.144
127.0.0.1	255.255.255.255	127.0.0.1

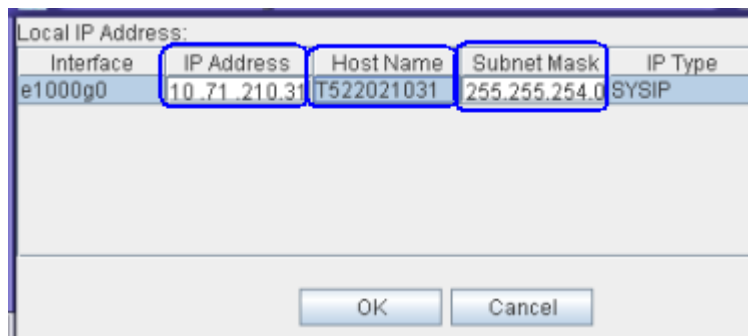
- Click **OK**.

14 Do as follows to change the host name and IP address.

- Right-click the server name and choose **Change IP Address And Hostname** from the shortcut menu.



- In the **Change IP Address And Hostname** dialog box, enter the new host name, IP address, and subnet mask.



3. Click **OK**. The progress bar is displayed. Wait patiently.
4. After the configuration is complete, the **Message** dialog box is displayed, asking you to restart the OS and back up the database in time. click **OK**.
- 15 Restart the OS of the server whose host name and IP address are changed for the settings to take effect.


```
# cd /opt/VRTSvcs/bin
# hstop -all -force
# sync;sync;sync;sync
# shutdown -y -g0 -i6
```
- 16 Log in to the OS of the primary site as the **root** user.
- 17 Connect the primary and secondary sites. For details, see [D.6.1 Establishing the HA Relationship Between the Primary and Secondary Sites](#).

 NOTE

If NBIs and instances are deployed and the xFtp monitor is configured before the host name and IP address are changed, you must configure NBIs on the MSuite client and re-configure the xFtp monitor on the U2000 client after changing the IP address and host name.

- For details about how to configure NBIs, see the related NBI user guide.
- For details about how to configure the xFtp monitor, see the U2000 Help.

----End

D.5.1.8 How to Change the IP Address and Host Name of the High Availability System (SUSE Linux-Distributed)

Question

How do I change the IP address and host name of the High Availability System (SUSE Linux-Distributed)?

Answer

NOTE

To change the IP address and host name for the single-server system (Solaris), do as follows:

1. Use the MSuite to separate the primary site from the secondary site.
2. Log in to a VCS client and ensure that the **NMSServer** resource is in **offline** state and other resources are in **online** state on the primary site.
3. Use the MSuite to change the IP address and host name for the primary site. If a route is changed, reconfigure the route.
4. Restart the OS to make the modifications take effect.
5. Log in to a VCS client and ensure that the **NMSServer** resource is in **offline** state and other resources are in **online** state on the secondary site.
6. Use the MSuite to change the IP address and host name for the secondary site. If a route is changed, reconfigure the route.
7. Restart the OS to make the modifications take effect.
8. Use the MSuite to reconnect the primary and secondary sites.

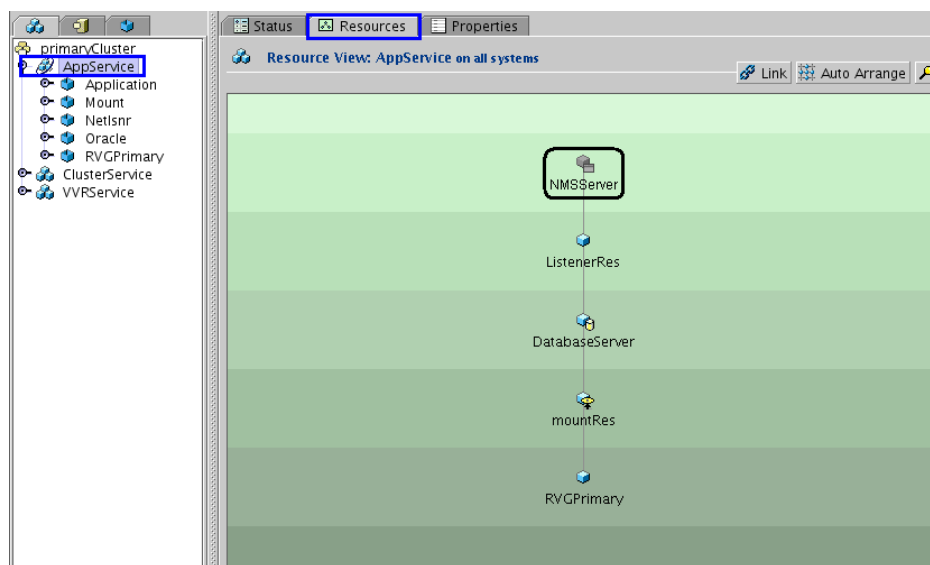
1 Log in to the MSuite client of the master server the primary site

NOTE

The IP address entered during login is the system IP address of the master server of the primary site.

- 2 Separate the primary site from the secondary site. For details, see [D.6.2 Deleting the HA Relationship Between the Primary and Secondary Sites](#).
- 3 Log in to the VCS clients of the primary site. For details, see [A.4.3.2 How to Log in and Exit the VCS \(Veritas Cluster Server\)](#).
- 4 On the VCS client, choose **AppService > Resources** and ensure that the **NMSServer** resource of the primary site is in the **offline** state and other resources are in the **online** state.

Figure D-6 High Availability System (SUSE Linux-Distributed) resources



 NOTE

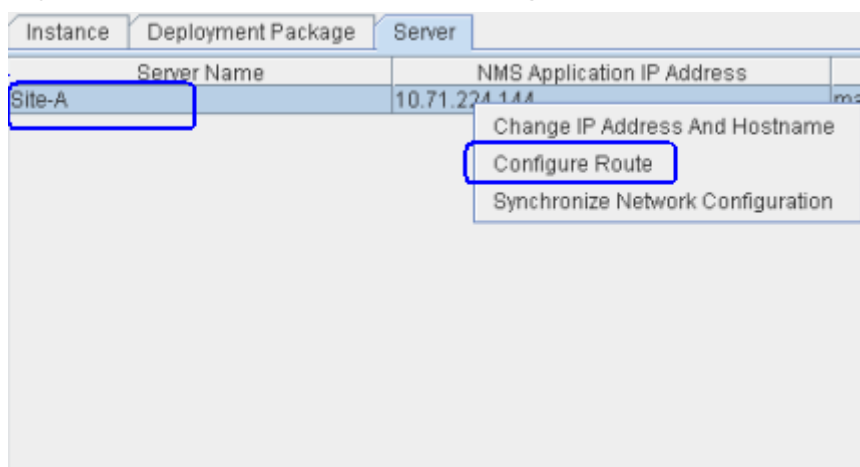
- Resources whose icons are grayed out are in the **offline** state. For example, the **NMSServer** resource in the preceding figure. Resources whose resource icons are not grayed out are in the **online** state. For example, the **BackupServer** resource in the preceding figure.
 - Check the status of all resources and ensure that the **NMSServer** resource is in the **offline** state and other resources are in the **online** state.
 - To make a resource online, right-click the resource and choose **online > hostname** from the shortcut menu. In the **Question** dialog box, click **Yes**.
 - To make a resource offline, right-click the resource and choose **offline > hostname** from the shortcut menu. In the **Question** dialog box, click **Yes**.
- 5 Log in to the slave server as user **root**. Open a terminal window and run the following command to end the **daem** process of the slave server:
- ```
/etc/init.d/u2kdaem stop
```



**CAUTION**

There must be a space between the dot (.) and **svc\_profile.sh**.

- 6 On the MSuite client, click the **Server** tab.
- 7 If the route changes, do as follows to add a route. If the route does not change, you do not need to change the IP address or host name. Instead, skip this step.
1. Right-click the server name and choose **Configure Route** from the shortcut menu.



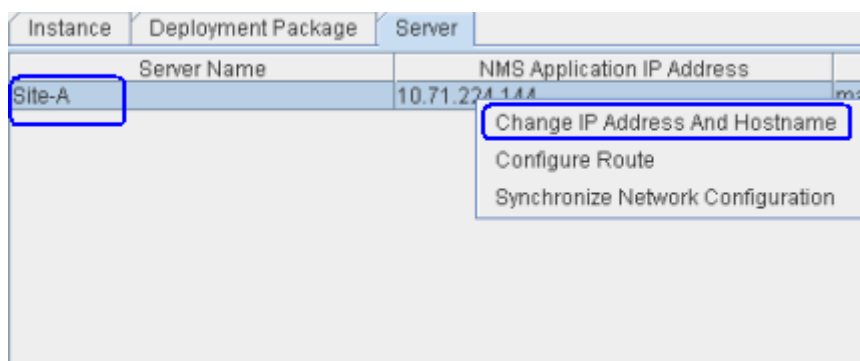
2. In the dialog box that is displayed, click **Add** or **Delete** according to actual route conditions to re-configure the route.

| Destination | Subnet Mask     | Route         |
|-------------|-----------------|---------------|
| 0.0.0.0     | 0.0.0.0         | 10.71.224.1   |
| 10.71.224.0 | 255.255.254.0   | 10.71.224.144 |
| 127.0.0.1   | 255.255.255.255 | 127.0.0.1     |

3. Click **OK**.

8 Do as follows to change the host name and IP address.

1. Right-click the server name and choose **Change IP Address And Hostname** from the shortcut menu.



2. In the **Change IP Address And Hostname** dialog box, enter the new host name, IP address, and subnet mask.

Local IP Address:

| Interface | IP Address   | Host Name  | Subnet Mask   | IP Type |
|-----------|--------------|------------|---------------|---------|
| e1000g0   | 10.71.210.31 | T522021031 | 255.255.254.0 | SYSIP   |

3. Click **OK**. The progress bar is displayed. Wait patiently.

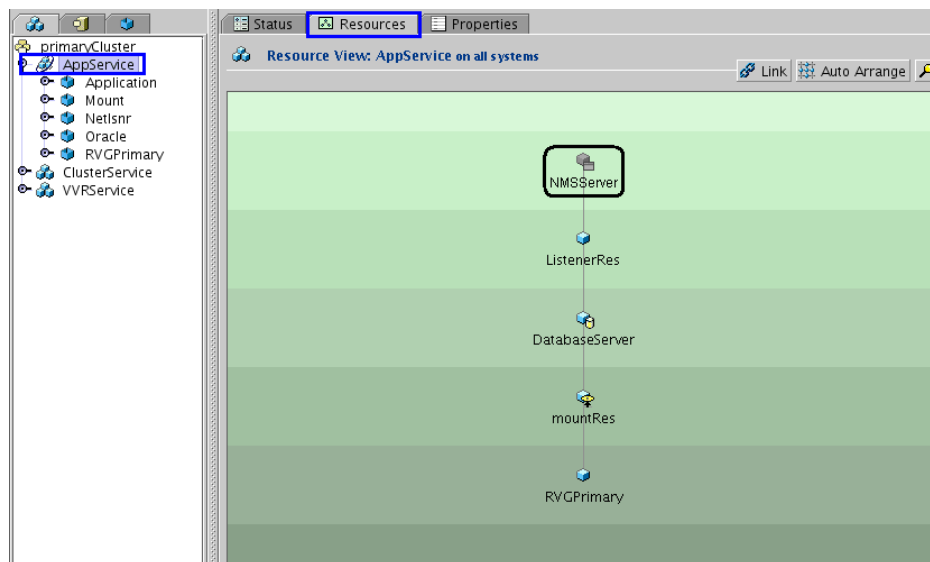
4. After the configuration is complete, the **Message** dialog box is displayed, asking you to restart the OS and back up the database in time. click **OK**.

9 Restart the OS of the server whose host name and IP address are changed for the settings to take effect.

```
cd /opt/VRTSvcs/bin
hastop -all -force
sync;sync;sync;sync
shutdown -r now
```

- 10 Log in to the VCS clients of the secondary site. For details, see [A.4.3.2 How to Log in and Exit the VCS \(Veritas Cluster Server\)](#).
- 11 On the VCS client, choose **AppService > Resources** and ensure that the **NMSServer** resource of the secondary site is in the **offline** state and other resources are in the **online** state.

**Figure D-7** High Availability System (SUSE Linux-Distributed) resources



**NOTE**

- Resources whose icons are grayed out are in the **offline** state. For example, the **NMSServer** resource in the preceding figure. Resources whose resource icons are not grayed out are in the **online** state. For example, the **BackupServer** resource in the preceding figure.
- Check the status of all resources and ensure that the **NMSServer** resource is in the **offline** state and other resources are in the **online** state.
- To make a resource online, right-click the resource and choose **online > hostname** from the shortcut menu. In the **Question** dialog box, click **Yes**.
- To make a resource offline, right-click the resource and choose **offline > hostname** from the shortcut menu. In the **Question** dialog box, click **Yes**.

- 12 Log in to the slave server as user **root**. Open a terminal window and run the following command to end the **daem** process of the slave server:

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



**CAUTION**

There must be a space between the dot (.) and **svc\_profile.sh**.

- 13 [Log in to the MSuite client of the master server the secondary site.](#)

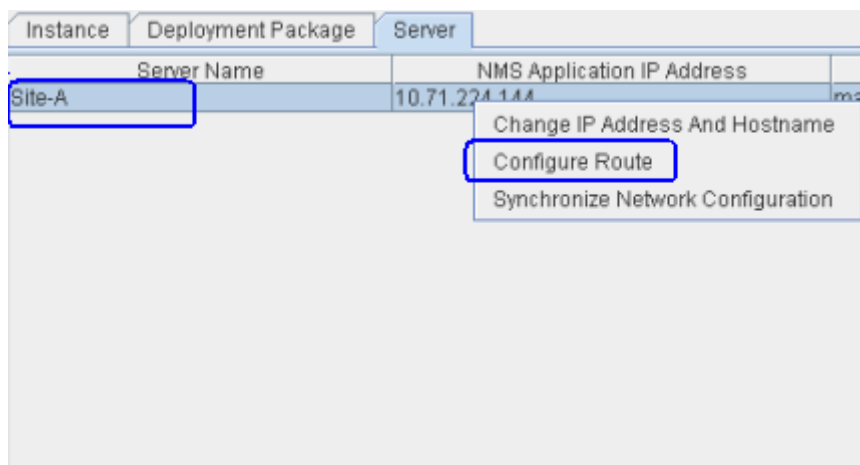
**NOTE**

The IP address entered during login is the system IP address of the master server of the primary site.

- 14 On the MSuite client, click the **Server** tab.

- 15** If the route changes, do as follows to add a route. If the route does not change, you do not need to change the IP address or host name. Instead, skip this step.

1. Right-click the server name and choose **Configure Route** from the shortcut menu.



2. In the dialog box that is displayed, click **Add** or **Delete** according to actual route conditions to re-configure the route.

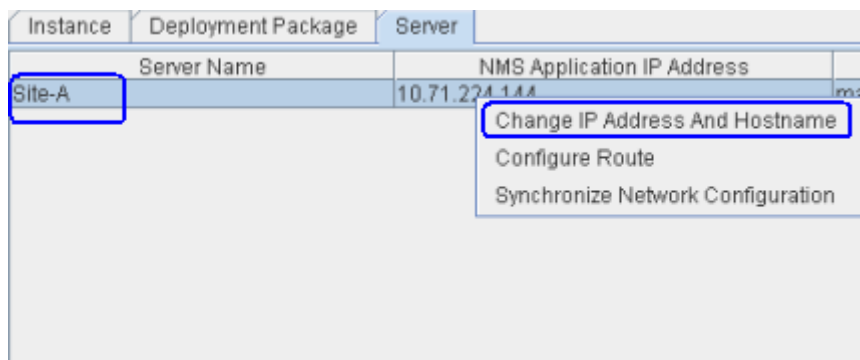
| Destination | Subnet Mask     | Route         |
|-------------|-----------------|---------------|
| 0.0.0.0     | 0.0.0.0         | 10.71.224.1   |
| 10.71.224.0 | 255.255.254.0   | 10.71.224.144 |
| 127.0.0.1   | 255.255.255.255 | 127.0.0.1     |

Buttons: Add, Delete

3. Click **OK**.

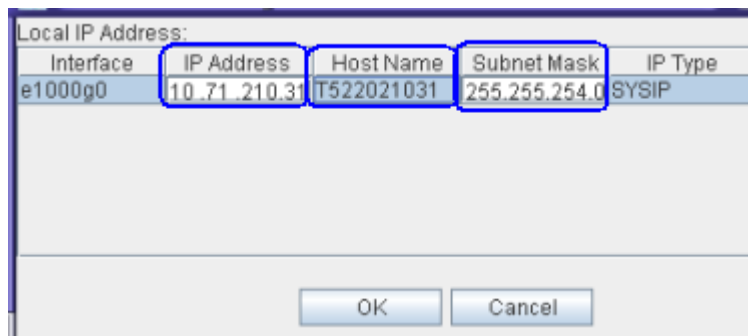
- 16** Do as follows to change the host name and IP address.

1. Right-click the server name and choose **Change IP Address And Hostname** from the shortcut menu.



2. In the **Change IP Address And Hostname** dialog box, enter the new host name, IP address, and subnet mask.





3. Click **OK**. The progress bar is displayed. Wait patiently.
  4. After the configuration is complete, the **Message** dialog box is displayed, asking you to restart the OS and back up the database in time. click **OK**.
- 17 Restart the OS of the server whose host name and IP address are changed for the settings to take effect.

```
cd /opt/VRTSvcs/bin
hstop -all -force
sync;sync;sync;sync
shutdown -r now
```

- 18 Log in to the OS of the master server of primary site as **root** user.

- 19 **Log in to the MSuite client of the master server the primary site**

**NOTE**

The IP address entered during login is the system IP address of the master server of the primary site.

- 20 Connect the primary and secondary sites. For details, see [D.6.1 Establishing the HA Relationship Between the Primary and Secondary Sites](#).

**NOTE**

1. If NAT networking was used, you must re-configure the **ipmap.cfg** file after the OS is restarted. For details, see [A.9.36 How to Configure the ipmap.cfg Mapping File](#).
2. If NBIs and instances are deployed and the xFtp monitor is configured before the host name and IP address are changed, you must configure NBIs on the MSuite client and re-configure the xFtp monitor on the U2000 client after changing the IP address and host name.
  - For details about how to configure NBIs, see the related NBI user guide.
  - For details about how to configure the xFtp monitor, see the U2000 Help.

----End

## D.5.2 Configuring Routes

This topic describes how to configure routes. After the U2000 is installed, if the network configurations of the server change, you can configure the routes of the server through the MSuite.

### Prerequisite

U2000 processes must have been stopped.

## Context

- In the high availability system (Veritas hot standby), if you need to modify the routes of the primary and secondary sites, you need to log in to the MSuite servers of the primary and secondary sites to perform the operation.
- In the Windows OS, using the MSuite to modify routes is unavailable.

## Procedure

- 1 Log in to the MSuite client. For details, see [D.2.2 Logging In to the MSuite Client](#).
- 2 On the MSuite client, click the **Server** tab.
- 3 Right-click the target server and choose **Configure Router** from the shortcut menu. The **Configure Router** dialog box is displayed.
- 4 Add or delete a route according to the new route plan.
- 5 Click **OK**.

----End

## D.5.3 Synchronizing Network Configurations

This topic describes how to synchronize network configurations. When a network configuration of the NMS server changes, you need to synchronize the network configuration so that the IP addresses of the MSuite and server are synchronized. Otherwise, the system displays a failure message during the login to the MSuite client.

## Prerequisite

- Ensure that the NMS server programs are already stop.
- Ensure that the database is running.
- In a high availability system, delete the high availability relationship between the primary and secondary sites. For details, see [D.6.2 Deleting the HA Relationship Between the Primary and Secondary Sites](#). Then, log in to both the primary and secondary sites to synchronize network configurations.

## Procedure

- 1 Log in to the MSuite client. For details, see [D.2.2 Logging In to the MSuite Client](#).
- 2 On the MSuite client, click the **Server** tab.
- 3 Right-click the server whose network configuration needs to be synchronized and choose **Synchronize Network Configuration** from the shortcut menu. A dialog box is displayed for you to confirm the operation.
- 4 Click **OK**. A progress bar showing the synchronization progress is displayed.
- 5 When the system displays "Synchronize network configuration success", click **OK**.

----End

## Follow-up Procedure

In a high availability system, reestablish the high availability relationship between the primary and secondary sites after synchronizing network configurations.

1. On the primary and secondary sites, do as follows to check whether the VCS service has been started:

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

The following information is displayed:

```
root 5852 1 0 07:14:51 ? 0:00 /opt/VRTSvcs/bin/hashadow
root 5842 1 0 07:14:45 ? 1:36 /opt/VRTSvcs/bin/had -onenode
```

### NOTE

If the displayed information contains `/opt/VRTSvcs/bin/hashadow` and `/opt/VRTSvcs/bin/had -onenode`, the VCS service has been started. If the VCS service has not been started, run the `hastart -onenode` command on the primary and secondary sites to start the VCS service.

2. Reestablish the high availability relationship between the primary and secondary sites. For details, see [D.6.1 Establishing the HA Relationship Between the Primary and Secondary Sites](#).

## D.6 Management of the High Availability System (Veritas hot standby)

This topic describes the frequently used operations of managing and maintaining the high availability system (Veritas hot standby) through the MSuite.

### [D.6.1 Establishing the HA Relationship Between the Primary and Secondary Sites](#)

This topic describes how to synchronize the primary and secondary sites. In a high availability system (Veritas hot standby), after installing the U2000 at the primary and secondary sites, synchronize the primary and secondary sites to configure the primary and secondary sites as an HA system.

### [D.6.2 Deleting the HA Relationship Between the Primary and Secondary Sites](#)

This topic describes how to delete the HA relationship between the primary and secondary sites. After the delete operation, the connection between the primary site and the secondary site is interrupted. In this manner, the HA system becomes two standalone sites. To delete the HA relationship between the primary and secondary sites, perform the following operations.

### [D.6.3 Deleting Replication Relations](#)

This topic describes how to delete replication relations. During the maintenance of the high availability system (Veritas hot standby), you can use the MSuite to delete the replication relations between the primary and secondary sites.

### [D.6.4 Configuring the Current Server as the Active Server Forcibly](#)

This topic describes how to forcibly configure the current server as the active server. When the replication relations between the primary and secondary sites become abnormal or the high availability system is in the dual-active state, you can perform this operation to specify the active site and data replication direction to restore data replication relations.

### [D.6.5 Performing the Dual-Active Operation](#)

This topic describes how to perform the dual-active operation. During the maintenance of the high availability system (Veritas hot standby), you can use the MSuite to configure the high availability system (Veritas hot standby) to enter the dual-active state from the normal state.

## D.6.1 Establishing the HA Relationship Between the Primary and Secondary Sites

This topic describes how to synchronize the primary and secondary sites. In a high availability system (Veritas hot standby), after installing the U2000 at the primary and secondary sites, synchronize the primary and secondary sites to configure the primary and secondary sites as an HA system.

### Prerequisite

- All the MSuite servers on the servers of the primary and secondary sites must be started.
- The subsystems, deployed instances, and passwords of the administrator and NMS user of the database on the primary and secondary sites must be consistent.
- In a distributed system, the slave servers at the primary and secondary sites must be of the same quantity and correspond to each other.

### Context

In a centralized system, log in to only the MSuite server at the primary site to perform the operation described in this topic. In a distributed system, log in to only the MSuite server of the master server at the primary site to perform the operation described in this topic.

### Procedure

- 1 Log in to the MSuite client.
- 2 Choose **Deploy > Synchronize Primary and Secondary Sites** from the main menu. The **Synchronize the primary and secondary sites** dialog box is displayed.
- 3 Enter the IP address of the remote server.

#### NOTE

**Remote IP** indicates the system IP address of the secondary site. In a distributed system, enter the system IP address of the secondary sitemaster server.

- 4 Click **OK**. A progress bar is displayed indicating the synchronization progress between the primary and secondary sites. Wait approximately 20 minutes until a dialog box is displayed indicating that the synchronization is completed.
- 5 Click **OK**. The synchronization between the primary and secondary sites is complete.
- 6 Run the following command repeatedly to check the status of data replication.

- In Solaris or SUSE Linux OS, run the following command:

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

A message similar to the following will be displayed:

```
Replicated Data Set: datarvg
Primary:
 Host name: 129.9.1.1
 RVG name: datarvg
 DG name: datadg
 RVG state: enabled for I/O
 Data volumes: 1
 VSets: 0
 SRL name: srl_vol
 SRL size: 1.00 G
 Total secondaries: 1
```

```
Secondary:
 Host name: 129.9.1.2
 RVG name: datarvg
 DG name: datadg
 Data status: inconsistent
 Replication status: resync in progress (autosync)
 Current mode: asynchronous
 Logging to: DCM (contains 28742784 Kbytes)
 (autosync)
 Timestamp Information: N/A
```

 **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-date**, 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.
- In Windows OS, run the following command:

```
C:\> vxrlink -g datadg -i2 status datarlk
```

A message similar to the following will be displayed:

```
2010-3-8 14:35:19
RLINK is up to date.
RLINK is up to date.
```

If **RLINK is up to date** is displayed, the replication is normal.

----End

## Operations Through the CLI

On Solaris or SUSE Linux OS, if you fail to log in to the GUI desktop system, establish the HA relationship between the primary and secondary sites.

The operations in CLI mode are as follows:

On Solaris OS, run the following command as user **nmsuser**. On SUSE Linux OS, run the following command as user **root**.

```
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
```

## D.6.2 Deleting the HA Relationship Between the Primary and Secondary Sites

This topic describes how to delete the HA relationship between the primary and secondary sites. After the delete operation, the connection between the primary site and the secondary site is interrupted. In this manner, the HA system becomes two standalone sites. To delete the HA relationship between the primary and secondary sites, perform the following operations.

### Prerequisite

The MSuite server on the primary and secondary sites must be started.

## Procedure

- 1 Log in to the MSuite client.
- 2 Choose **Deploy > Separate Primary Site from Secondary Site**. The **Separate Primary Site from Secondary Site** dialog box is displayed.
- 3 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.
- 4 Click **OK**.

----End

## Operations Through the CLI

On Solaris or SUSE Linux OS, if you fail to log in to the GUI desktop system, delete the HA relationship between the primary and secondary sites through the CLI.

The operations in CLI mode are as follows:

On Solaris OS, run the following command as user **nmsuser**. On SUSE Linux OS, run the following command as user **root**.

```
cd /opt/U2000/engineering
./startclient.sh deploy -ip 127.0.0.1 -port 12212 -username admin -password admin
splitHA
```

## 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. .

## D.6.3 Deleting Replication Relations

This topic describes how to delete replication relations. During the maintenance of the high availability system (Veritas hot standby), you can use the MSuite to delete the replication relations between the primary and secondary sites.

## Prerequisite

Ensure that the **/opt** directory has available space. You can run the **df -hk /opt** command to view the remaining space of the **/opt** directory.

## Context

If the high availability system is in the normal state, do not perform this operation. Otherwise, the high availability system becomes unavailable.

## Procedure

- 1 Log in to the MSuite client.
- 2 Choose **Deploy > Delete Replication**.  
The progress bar of deleting the replication relations is displayed. Five minutes later, a dialog box is displayed indicating that the replication relation is successfully deleted.

- 3 Click **OK**.

----End

## Follow-up Procedure

If you need to re-establish the replication relations, forcibly configure the local site as the primary site. For details, see [D.6.4 Configuring the Current Server as the Active Server Forcibly](#).

## D.6.4 Configuring the Current Server as the Active Server Forcibly

This topic describes how to forcibly configure the current server as the active server. When the replication relations between the primary and secondary sites become abnormal or the high availability system is in the dual-active state, you can perform this operation to specify the active site and data replication direction to restore data replication relations.

### Prerequisite

- The data replication relation between the primary and secondary sites must be abnormal.
- All the MSuite servers on the servers of the primary and secondary sites must be started.

### Context

- Do not perform this operation if the HA system works in the normal state. Otherwise, an exception may occur in the HA system.
- Do not perform this operation if the resource group **AppService** at the primary and secondary sites are in the online process. Otherwise, an exception may occur in the HA system.
- If you log in to the MSuite server of the primary site to perform this operation, the primary site becomes the active site after the operation. If you log in to the MSuite server of the secondary site to perform this operation, the secondary site becomes the active site after the operation.

### Procedure

- 1 Log in to the MSuite client.
- 2 Choose **Deploy > Force Active of Local Site**.
- 3 Click **OK**. Then, the current server is configured to function as the active server.

----End

## D.6.5 Performing the Dual-Active Operation

This topic describes how to perform the dual-active operation. During the maintenance of the high availability system (Veritas hot standby), you can use the MSuite to configure the high availability system (Veritas hot standby) to enter the dual-active state from the normal state.

### Prerequisite

Ensure that the **/opt** directory has available space. You can run the **df -hk /opt** command to view the remaining space of the **/opt** directory.

## Context

If the high availability system is in the normal state, do not perform this operation. Otherwise, the high availability system becomes unavailable.

## Procedure

- 1 Log in to the MSuite client.
- 2 On the MSuite client, choose **Deploy > Enable Dual Active Sites**.  
The progress bar of performing the dual-active operation is displayed. Five minutes later, a dialog box is displayed indicating that the dual-active operation is successfully performed.
- 3 Click **OK**.

----End

## Follow-up Procedure

If you need to change the state of the HA system from the dual-active state to the normal state, forcibly configure the local site as the primary site. For details, see [D.6.4 Configuring the Current Server as the Active Server Forcibly](#).

# D.7 Maintaining a Distributed System

This topic describes the daily operations used to maintain a distributed system through the MSuite. If you are using a centralized system, skip this topic.

### [D.7.1 Adding a Slave Server](#)

This topic describes how to connect the slave server to the master server to form a distributed system.

### [D.7.2 Deleting a Slave Server](#)

This topic describes how to delete a slave server.

### [D.7.3 Migrating an Instance](#)

This topic describes how to migrate an instance. To balance the load among each server in a distributed system, you can migrate an instance from the server with heavy load to another server with lighter load within a site.

## D.7.1 Adding a Slave Server

This topic describes how to connect the slave server to the master server to form a distributed system.

## Prerequisite

- The U2000 must be installed on the master server and the operating system (OS) must be installed and configured on the slave server. For details, see the *Software Installation Guide* of the related scheme.
- The master and slave servers must be connected to the public and private networks. For details, see the *Software Installation Guide* of the related scheme.



- The Network Management System Maintenance Suite server must be started on the master and slave servers.

## Context

The operations in this topic are performed on the NMS maintenance suite client of the master server.

## Procedure

- 1 On the NMS maintenance suite client, click the **Server** tab.
- 2 Choose **System > Add a Slave Server**. The **Add a Slave Server** dialog box is displayed.
- 3 Set the parameters of the slave server.  
 **NOTE**
  - **Server Name**: Enter the planned host name of the slave server.
  - **IP Address**: Enter the planned IP address of the slave server.
- 4 Click **OK**. A progress bar is displayed indicating the status of adding the slave server. Wait until a dialog box is displayed indicating that the slave server is added successfully.
- 5 Click **OK**. A progress bar is displayed indicating the progress of adding deployment packages. Wait patiently. A prompt is displayed indicating that components are successfully added.
- 6 Click **OK**.

----End

## Follow-up Procedure

After the preceding operations are performed, follow the GUI prompt to restart the OS of the slave server.

## D.7.2 Deleting a Slave Server

This topic describes how to delete a slave server.

## Prerequisite

- Make sure that all NMS maintenance suite servers are started.
- Make sure that no component and instances are deployed on the slave server. If a certain subsystem or instance is already deployed on the slave server, you need to delete the subsystem or instance, or migrate it to another server by using the MSuite.

## Context

The operations in this topic are performed on the MSuite client of the master server.

## Procedure

- 1 On the NMS maintenance suite client, click the **Server** tab.

- 2 Choose **System > Remove a Slave Server**. The **Remove a Slave Server** dialog box is displayed.
  - 3 Click **OK**. The **Remove a Slave Server** dialog box is displayed.
  - 4 Select the slave server to be deleted.
  - 5 Click **OK**. A progress bar is displayed showing the status of deleting the slave server.  
Wait until the message is displayed indicating that the slave server is deleted successfully.
  - 6 Click **OK**.
- End

## D.7.3 Migrating an Instance

This topic describes how to migrate an instance. To balance the load among each server in a distributed system, you can migrate an instance from the server with heavy load to another server with lighter load within a site.

### Prerequisite

The database must be in the running state.

### Procedure

- 1 Log in to the MSuite client. For details, see [D.2.2 Logging In to the MSuite Client](#).
- 2 On the MSuite client, click the **Instance** tab.
- 3 Right-click the instance that you want to migrate and choose **Move Instance** from the shortcut menu. The **Move Instance** dialog box is displayed.

#### NOTE

If the **Move Instance** option is unavailable, it indicates that this instance cannot be migrated. Only deployment packages in the transport domain support instance migration.

- 4 Select the target server and click **OK**.
- 5 Wait until the message "The instance is already moved" is displayed. Click **OK**.

#### NOTE

When you migrate an instance, the MSuite automatically checks the status of the instance. If the status of the instance is **All start**, the MSuite automatically stops the instance and then migrates it.

----End

## D.8 Configuring the Northbound Interface Instance

This topic describes how to configure the northbound interface (NBI) instance. When the U2000 needs to access the upper-layer NMS, the related NBI should be configured as required. The NBIs that are commonly used by the U2000 are CORBA, SNMP, XML and TEXT NBIs.

## D.9 Managing Databases

This topic describes how to manage databases. To ensure the security of system data, the MSuite provides the function of managing databases.

### [D.9.1 Backing Up the System Database](#)

This topic describes how to back up the U2000 database through the MSuite, including backing up the U2000 database to the local server and remote server. Backing up the U2000 data is the prerequisite to restoring the U2000 database in a fast and secure manner.

### [D.9.2 Restoring Data of a U2000 Single-Server System \(Windows\)](#)

If the U2000 database is faulty, you can restore data on the current U2000 by using the backup U2000 data.

### [D.9.3 Restoring U2000 Single-Server System \(Solaris\) Data](#)

If the U2000 database is faulty, you can restore data on the current U2000 by using the backup U2000 data.

### [D.9.4 Restoring U2000 Single-Server System \(SUSE Linux-Distributed\) Data](#)

If the U2000 database is faulty, you can restore data on the current U2000 by using the backup U2000 data.

### [D.9.5 Restoring U2000 High Availability System \(Windows\) Data](#)

If the U2000 database is faulty, you can restore data on the current U2000 by using the backup U2000 data.

### [D.9.6 Restoring U2000 High Availability System \(Solaris\) Data](#)

If the U2000 database is faulty, you can restore data on the current U2000 by using the backup U2000 data.

### [D.9.7 Restoring U2000 High Availability System \(SUSE Linux-Distributed\) Data](#)

If the U2000 database is faulty, you can restore data on the current U2000 by using the backup U2000 data.

### [D.9.8 Restoring Data of a U2000 High Availability System \(Cross-U2000\)](#)

If multiple sets of U2000s are available, and the components installed on the U2000s as well as the database versions and OS versions of the U2000s are the same, you can restore data cross these U2000s. That is, the backup data of U2000 A can be used to restore the data of U2000 B.

### [D.9.9 Initializing the U2000 Database](#)

This topic describes how to initialize the U2000 database. Initialize the U2000 database before it is in disorder or restored, or data is damaged.

## D.9.1 Backing Up the System Database

This topic describes how to back up the U2000 database through the MSuite, including backing up the U2000 database to the local server and remote server. Backing up the U2000 data is the prerequisite to restoring the U2000 database in a fast and secure manner.

### [D.9.1.1 Immediately Backing Up the U2000 Database to a Local Server Through the MSuite](#)

This topic describes how to immediately back up the U2000 database to a local server through the NMS maintenance suite (MSuite). After this configuration, the database can be safely and quickly restored after a fault occurs.

### [D.9.1.2 Immediately Backing Up the U2000 Database to a Remote Server Through the MSuite](#)

This topic describes how to immediately back up the U2000 database to a remote server by using the NMS maintenance suite (MSuite). After this configuration, the database can be safely and quickly restored after a fault occurs.

### D.9.1.1 Immediately Backing Up the U2000 Database to a Local Server Through the MSuite

This topic describes how to immediately back up the U2000 database to a local server through the NMS maintenance suite (MSuite). After this configuration, the database can be safely and quickly restored after a fault occurs.

#### Prerequisite

The database is running.

#### Context

The backup process cannot be canceled once it is started.

#### Procedure

- 1 Log in to the MSuite client. For details, see [D.2.2 Logging In to the MSuite Client](#).
- 2 On the MSuite client, choose **Backup and Restore** > **Backup system data** from the main menu.
- 3 Select **Data Backup-Binary Mode(Recommended)**, and then click **Next**.

#### NOTE

- **Data Backup-Text Mode** is only used to collect fault information when the U2000 fails to locate and rectify the fault. This mode is not recommended during routine database backup.
- **Data Backup-Text Mode** is not supported by the SUSE Linux OS and will not be displayed on this OS.

- 4 Set the related parameters. Then, click **Next**.
  1. Set the backup amount. The backup quantity indicates the number of data copies saved in the backup path. To save the disk space on the server, do not set the backup quantity to an inappropriately large value. If the number of data copies in the backup path exceeds the preset value, the system automatically deletes the earliest data copies. It is recommended that you use the default value.
  2. Set the backup path for storing the backup file. Select **Back up the data to the local server** and then set the **Local server backup path**.
    - It is recommended that you use the default backup path. For initial backup, no default backup path exists and the system will ask whether to create a default backup path. Click **Yes** to create the path.
    - If you want to use another backup path, click **Brows** to select it.



## CAUTION

If a non-default backup path is used, ensure that the path has read, write, and execute permissions. If the path does not have these permissions, run the following command as user **root** to grant these permissions.

```
chmod -R 775 Backup path
```

Please configure backup information

Backup count:

☒ Backup the data to the local server

Local server backup path:

☐ Backup the data to a remote server

Server IP address:  Transfer mode:

User name:  Password:

Remote server backup path:

- 5 The system starts the backup preprocessing and backup process. A progress bar is displayed showing the backup progress. Wait patiently.
- 6 After the backup is complete, click **Finish**.

----End

## Operations Through the CLI

On Solaris or SUSE Linux OS, if you fail to log in to the GUI desktop system,, back up the U2000 database through the CLI.



## CAUTION

The MSuite adopts single-user mode, so you must exit all MSuite client GUIs before performing the backup through the CLI.

The operations in CLI mode are as follows:

On Solaris OS, run the following command as user **nmsuser**. On SUSE Linux OS, run the following command as user **root**.

```
cd /opt/U2000/engineering
./startclient.sh storage -ip 127.0.0.1 -port 12212 -username admin -password MSuite
password -DumpDB -StoreMode local -FilePath Backup path
```

**NOTE**

The default user name and password are both **admin**. If the password has been changed, enter the new password.

**NOTE**

- *MSuite password*: The default password of the MSuite is **admin**. If the password has been changed, enter the new password.
- *Backup path*: The backup path must have read, write, and execute permissions. If the path does not have these permissions, run the following command as user **root** to grant these permissions.  
# `chmod -R 775 Backup path`

## D.9.1.2 Immediately Backing Up the U2000 Database to a Remote Server Through the MSuite

This topic describes how to immediately back up the U2000 database to a remote server by using the NMS maintenance suite (MSuite). After this configuration, the database can be safely and quickly restored after a fault occurs.

### Prerequisite

- The database is running.
- The FTP or SFTP server programs are running on the remote server, and the relevant ports are enabled. The port of FTP server is 21, and the port of SFTP server is 22.

**NOTE**

- For details on how to start the FTP or SFTP server programs on Solaris, see [A.3.3.1 How to Start/Stop the FTP, TFTP, SFTP, and Telnet Services](#).
- For details on how to start the FTP or SFTP server programs on SUSE Linux, see [A.2.1 How to Start/Stop the FTP, TFTP, SFTP, and Telnet Services](#).
- For details on how to configure FTP, SFTP or TFTP services on Windows, see [A.1.7 How to Configure the FTP, SFTP, or TFTP Service on Windows OS](#).
- The FTP or SFTP user must have write permissions for the remote FTP server.

### Context

- The backup process cannot be canceled once it is started.
- On the Solaris OS, the temporary directory *tmp* is created in the **/opt** path during the backup of the database. If the *tmp* directory exists in the **/opt** path, you need to ensure that the owner and group of the directory are both **sybase**. Run the following commands to change the owner and group of the */opt/tmp*.  
# `chown -R sybase /opt/tmp`  
# `chgrp -R sybase /opt/tmp`

### Procedure

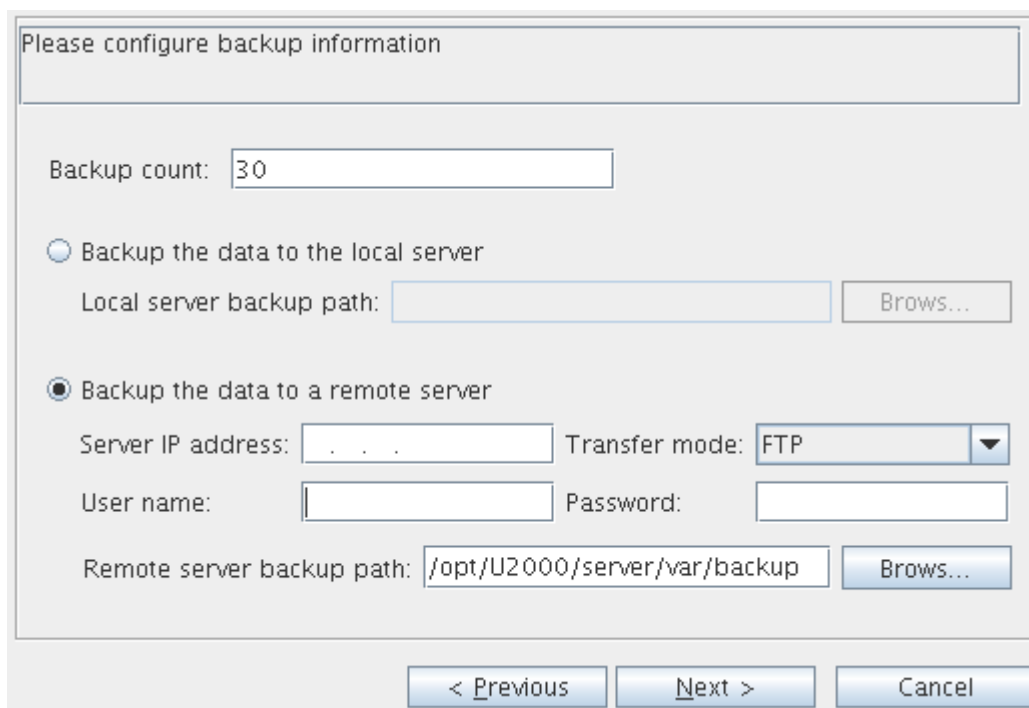
- 1 Log in to the MSuite client. For details, see [D.2.2 Logging In to the MSuite Client](#).
- 2 On the MSuite client, choose **Backup and Restore > Backup system data** from the main menu.
- 3 Select **Data Backup-Binary Mode(Recommended)**, and then click **Next**.

 **NOTE**

- **Data Backup-Text Mode** is only used to collect fault information when the U2000 fails to locate and rectify the fault. This mode is not recommended during routine database backup.
- **Data Backup-Text Mode** is not supported by the SUSE Linux OS and will not be displayed on this OS.

4 Set the related parameters. Then, click **Next**.

1. Set the backup amount. The backup quantity indicates the number of data copies saved in the backup path. To save the disk space on the server, do not set the backup quantity to an inappropriately large value. If the number of data copies in the backup path exceeds the preset value, the system automatically deletes the earliest data copies. It is recommended that you use the default value.
2. Set the path for storing the backup file. Select **Back up the data to a remote server** and then set the parameters associated with the remote server. The parameter description is as follows:
  - **Server IP address**: IP address of the server where the backup file is stored.
  - **Transfer mode**: FTP or SFTP mode.
  - **User name**: Name of the FTP user or SFTP user.
  - **Password**: Password of the FTP user or SFTP user.
  - **Remote server backup path**: Path for storing the backup file.



Please configure backup information

Backup count: 30

☐ Backup the data to the local server

Local server backup path:

☒ Backup the data to a remote server

Server IP address:  Transfer mode:

User name:  Password:

Remote server backup path:

- 5 The system starts the backup preprocessing and backup process. A progress bar is displayed showing the backup progress. Wait patiently.
- 6 After the backup is complete, click **Finish**.

----End

## Operations Through the CLI

On Solaris or SUSE Linux OS, if you fail to log in to the GUI desktop system,, back up the U2000 database through the CLI.



### CAUTION

The MSuite adopts single-user mode, so you must exit all MSuite client GUIs before performing the backup through the CLI.

---

The operations in CLI mode are as follows:

On Solaris OS, run the following command as user **nmsuser**. On SUSE Linux OS, run the following command as user **root**.

```
cd /opt/U2000/engineering
./startclient.sh storage -ip 127.0.0.1 -port 12212 -username admin -password Msuite
password -DumpDB -StoreMode remote -TransMode ftp -Server IP address of the remote
server -FTPUserName User name -Pwd FPassword -FilePath Backup path
```



### NOTE

- *MSuite password*: The default password of the MSuite is **admin**. If the password has been changed, enter the new password.
- *IP address of the remote server*: IP address of the remote server whether the backup file is stored.
- *User name*: Name of the FTP user or SFTP user.
- *Password*: Password of the FTP user or SFTP user.
- *Backup path*: Path for storing the backup file. Ensure that the FTP user or SFTP user have read permissions for this path.

## D.9.2 Restoring Data of a U2000 Single-Server System (Windows)

If the U2000 database is faulty, you can restore data on the current U2000 by using the backup U2000 data.

### [D.9.2.1 Restoring U2000 Single-Server System \(Windows\) Data from a Local Server](#)

If the backup U2000 data is stored on a local server, you can restore U2000 data from the local server.

### [D.9.2.2 Restoring U2000 Single-Server System \(Windows\) Data from a Remote Server](#)

If the backup U2000 data is stored on a remote server, you can restore U2000 data from the remote server.

### D.9.2.1 Restoring U2000 Single-Server System (Windows) Data from a Local Server

If the backup U2000 data is stored on a local server, you can restore U2000 data from the local server.

### Prerequisite

- U2000 processes must have been stopped. If U2000 processes are not stopped, see [A.9.18 How to End the Processes of the U2000 Single-Server System on Windows](#).
- The database must be running. If the database is not running, see [A.5.4 How to Start the SQL Server Database](#).



- If the database of U2000 A needs to be restored on U2000 B, paths for storing database files on the U2000 A and U2000 B must be the same.

## Procedure

- 1 Log in to the MSuite client. For details, see [D.2.2 Logging In to the MSuite Client](#).
- 2 On the MSuite client, choose **Backup and Restore > Restore system data** from the main menu.
- 3 Select **Data Restore-Binary Mode(Recommended)**, and then click **Next**.

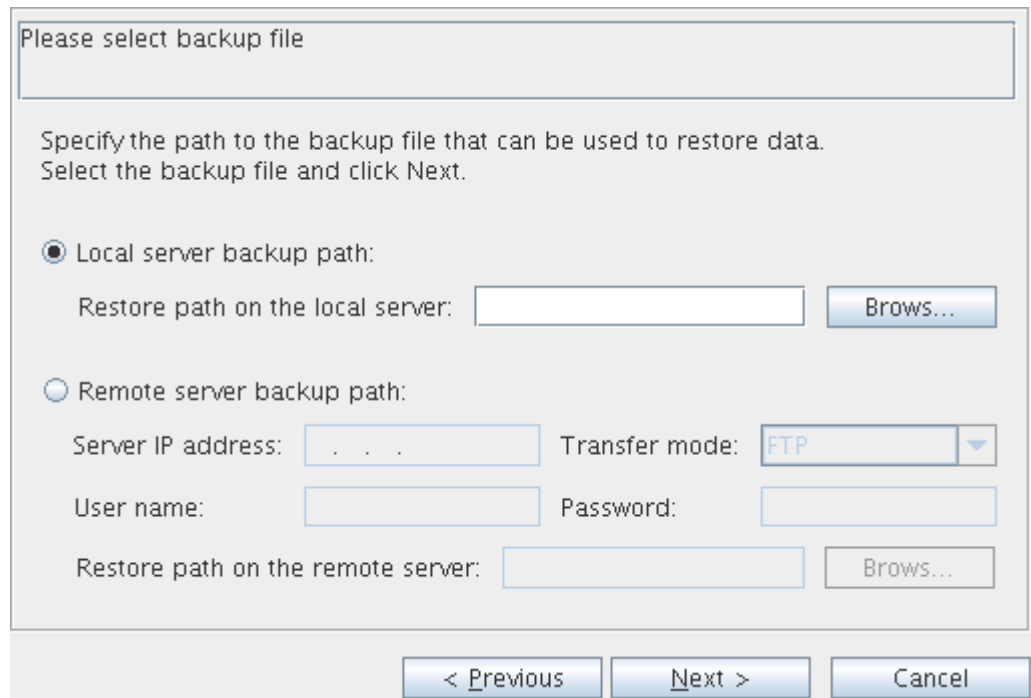
 **NOTE**

**Data Restore-Text Mode** is only used to locate and rectify the fault. This mode is not recommended during routine database restore.

- 4 Select **Local server backup path**, and then click **Browse** to select the data to be used for restoration.

 **NOTE**

During backup, the backed up data is generated in a folder named by time. For example, the path is /201009271646. You can enter the path of this folder to restore the backed up data.



- 5 Click **Next**, the system starts the restoration preprocessing and data restoration, and displays the restoration progress in a progress bar. Wait patiently.

**CAUTION**

If the system displays a message indicating component inconsistency and asking you whether to forcibly restore U2000 data, do as follows:

1. Read the message carefully and record involved components. Then, click **No** to choose not to continue restoring U2000 data.
2. Delete involved components. For details about how to delete involved components, see [D.4.2 Deleting a Component](#).
3. After involved components are deleted, restore U2000 data.

- 6 After U2000 data is restored, click **Finish**.
- 7 On the MSuite client, choose **System > Refresh NMS Information**. Alternatively, you can click the  icon on the toolbar.
- 8 In the scenario where the current database is SQL Server2000 SP4, check whether the database sorting mode is set to binary. For details, see [A.5.6 How to Check Whether the SQL Server Database Can Be Sorted in Binary Mode](#). If the database sorting mode is not set to binary, change it to binary. For details, see [A.5.7 How to Change the Database Sorting Mode to Binary](#).

----End

## Follow-up Procedure

After restoring U2000 data, start the NMS processes, for details, see [A.9.17 How to Start the Processes of the U2000 Single-Server System on Windows](#).

**NOTE**

- If the CORBA NBI, XML NBI, SNMP NBI, or text NBI is configured for the U2000, you need to reconfigure the NBI instance after successfully restoring the database. For details, see the related NBI user manual.
- After the preceding operations are complete, login passwords for the U2000 client, NE Software Management and U2000 System Monitor restore to be consistent with the U2000 data.

### D.9.2.2 Restoring U2000 Single-Server System (Windows) Data from a Remote Server

If the backup U2000 data is stored on a remote server, you can restore U2000 data from the remote server.

## Prerequisite

- U2000 processes must have been stopped. If U2000 processes are not stopped, see [A.9.18 How to End the Processes of the U2000 Single-Server System on Windows](#).
- The database must be running. If the database is not running, see [A.5.4 How to Start the SQL Server Database](#).
- The FTP or SFTP server programs are running on the remote server, and the relevant ports are enabled. The port of FTP server is 21, and the port of SFTP server is 22.

 **NOTE**

- For details on how to start the FTP or SFTP server programs on Solaris, see [A.3.3.1 How to Start/Stop the FTP, TFTP, SFTP, and Telnet Services](#).
- For details on how to start the FTP or SFTP server programs on SUSE Linux, see [A.2.1 How to Start/Stop the FTP, TFTP, SFTP, and Telnet Services](#).
- For details on how to configure FTP, SFTP or TFTP services on Windows, see [A.1.7 How to Configure the FTP, SFTP, or TFTP Service on Windows OS](#).
- If the database of U2000 A needs to be restored on U2000 B, paths for storing database files on the U2000 A and U2000 B must be the same.

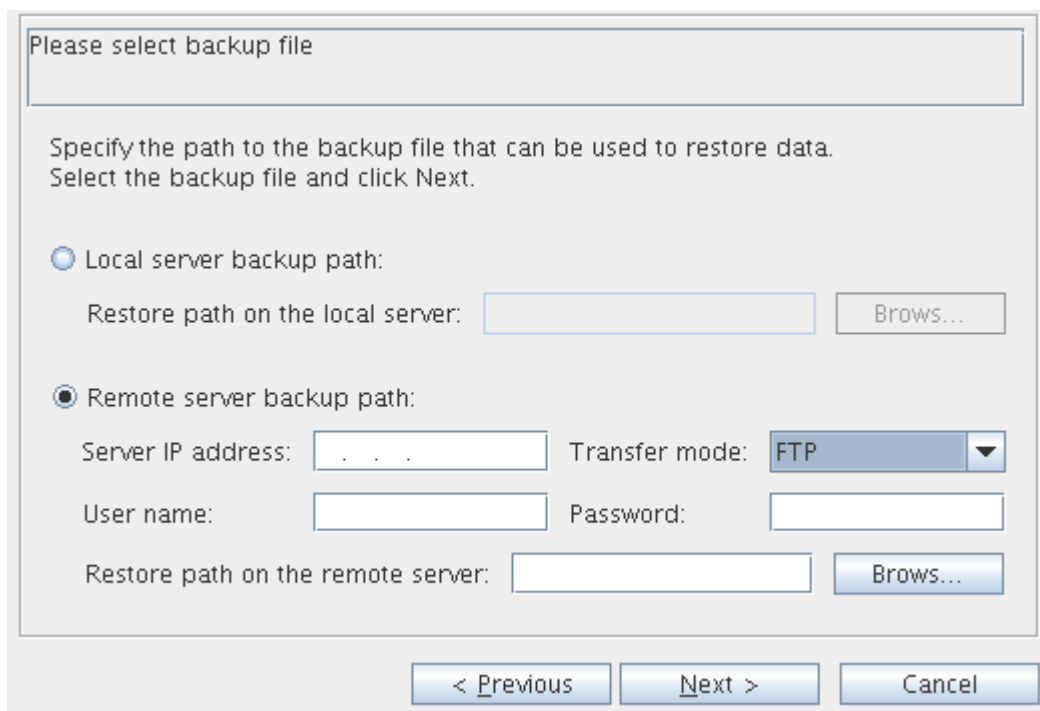
## Procedure

- 1 Log in to the MSuite client. For details, see [D.2.2 Logging In to the MSuite Client](#).
- 2 On the MSuite client, choose **Backup and Restore > Restore system data** from the main menu.
- 3 Select **Data Restore-Binary Mode(Recommended)**, and then click **Next**.

 **NOTE**

**Data Restore-Text Mode** is only used to locate and rectify the fault. This mode is not recommended during routine database restore.

- 4 Select **Remote server backup path** and set the associated parameters. Then, click **Next**.
  - **Server IP address**: indicates the IP address of the server where the restoration data is stored.
  - **Transfer mode**: The available options are FTP and SFTP.
  - **User name**: indicates the name of the FTP user or SFTP user.
  - **Password**: indicates the password of the FTP user or SFTP user.
  - **Remote server backup path**: indicates the path for storing the data used for restoration. During backup, the backed up data is generated in a folder named by time. You can enter the path of this folder to restore the backed up data.



- 5 Click **Next**, the system starts the restoration preprocessing and data restoration, and displays the restoration progress in a progress bar. Wait patiently.



### CAUTION

If the system displays a message indicating component inconsistency and asking you whether to forcibly restore U2000 data, do as follows:

1. Read the message carefully and record involved components. Then, click **No** to choose not to continue restoring U2000 data.
  2. Delete involved components. For details about how to delete involved components, see [D.4.2 Deleting a Component](#).
  3. After involved components are deleted, restore U2000 data.
- 

- 6 After U2000 data is restored, click **Finish**.
- 7 On the MSuite client, choose **System > Refresh NMS Information**. Alternatively, you can click the  icon on the toolbar.
- 8 In the scenario where the current database is SQL Server2000 SP4, check whether the database sorting mode is set to binary. For details, see [A.5.6 How to Check Whether the SQL Server Database Can Be Sorted in Binary Mode](#). If the database sorting mode is not set to binary, change it to binary. For details, see [A.5.7 How to Change the Database Sorting Mode to Binary](#).

----End

## Follow-up Procedure

After restoring U2000 data, start the NMS processes, for details, see [A.9.17 How to Start the Processes of the U2000 Single-Server System on Windows](#).



### NOTE

- If the CORBA NBI, XML NBI, SNMP NBI, or text NBI is configured for the U2000, you need to reconfigure the NBI instance after successfully restoring the database. For details, see the related NBI user manual.
- After the preceding operations are complete, login passwords for the U2000 client, NE Software Management and U2000 System Monitor restore to be consistent with the U2000 data.

## D.9.3 Restoring U2000 Single-Server System (Solaris) Data

If the U2000 database is faulty, you can restore data on the current U2000 by using the backup U2000 data.

### [D.9.3.1 Restoring U2000 Single-Server System \(Solaris\) Data from a Local Server](#)

If the backup U2000 data is stored on a local server, you can restore U2000 data from the local server.

### [D.9.3.2 Restoring U2000 Single-Server System \(Solaris\) Data from a Remote Server](#)

If the backup U2000 data is stored on a remote server, you can restore U2000 data from the remote server.

### D.9.3.1 Restoring U2000 Single-Server System (Solaris) Data from a Local Server

If the backup U2000 data is stored on a local server, you can restore U2000 data from the local server.

#### Prerequisite

- Database versions must be the same.
- U2000 processes must have been stopped. If U2000 processes are not stopped, see [A.9.21 How to End the Processes of the U2000 Single-Server System on Solaris](#).
- The database must be running. If the database is not running, see [A.6.1.2 How to Start the Sybase Database Service](#).
- In the Solaris OS, ensure that the owner and user group of the folder that stores backup data are both **sybase**. You can run the following commands to change the owner and user group of files:  

```
chown -R sybase backup path
chgrp -R sybase backup path
```

#### Procedure

- 1 Log in to the MSuite client. For details, see [D.2.2 Logging In to the MSuite Client](#).
- 2 On the MSuite client, choose **Backup and Restore > Restore system data** from the main menu.
- 3 Select **Data Restore-Binary Mode(Recommended)**, and then click **Next**.

 **NOTE**

**Data Restore-Text Mode** is only used to locate and rectify the fault. This mode is not recommended during routine database restore.

- 4 Select **Local server backup path**, and then click **Browse** to select the data to be used for restoration.

 **NOTE**

During backup, the backed up data is generated in a folder named by time. For example, the path is / 201009271646. You can enter the path of this folder to restore the backed up data.

- 5 Click **Next**, the system starts the restoration preprocessing and data restoration, and displays the restoration progress in a progress bar. Wait patiently.



## CAUTION

If the system displays a message indicating component inconsistency and asking you whether to forcibly restore U2000 data, do as follows:

1. Read the message carefully and record involved components. Then, click **No** to choose not to continue restoring U2000 data.
2. Delete involved components. For details about how to delete involved components, see [D. 4.2 Deleting a Component](#).
3. After involved components are deleted, restore U2000 data.

- 6 After U2000 data is restored, click **Finish**.
- 7 On the MSuite client, choose **System > Refresh NMS Information**. Alternatively, you can click the  icon on the toolbar.

----End

## Operations Through the CLI

On Solaris or SUSE Linux OS, if you fail to log in to the GUI desktop system, restore the U2000 data through the CLI.



## CAUTION

The MSuite adopts single-user mode, so you must exit all MSuite client GUIs before performing the backup through the CLI.

The operations in CLI mode are as follows:

On Solaris OS, run the following command as user **nmsuser**. On SUSE Linux OS, run the following command as user **root**.

```
cd /opt/U2000/engineering
./startclient.sh storage -ip 127.0.0.1 -port 12212 -username admin -password admin
-RestoreDB -StoreMode local -FilePath /opt/nmsBackup/200811211230
```



### NOTE

The default user name and password are both **admin**. If the password has been changed, enter the changed password.

## Follow-up Procedure

After restoring U2000 data, start the NMS processes, for details, see [A.9.20 How to Start the Processes of the U2000 Single-Server System on Solaris](#).



### NOTE

- If the CORBA NBI, XML NBI, SNMP NBI, or text NBI is configured for the U2000, you need to reconfigure the NBI instance after successfully restoring the database. For details, see the related NBI user manual.
- After the preceding operations are complete, login passwords for the U2000 client, NE Software Management and U2000 System Monitor restore to be consistent with the U2000 data.

## D.9.3.2 Restoring U2000 Single-Server System (Solaris) Data from a Remote Server

If the backup U2000 data is stored on a remote server, you can restore U2000 data from the remote server.

## Prerequisite

- Database versions must be the same.
- U2000 processes must have been stopped. If U2000 processes are not stopped, see [A.9.21 How to End the Processes of the U2000 Single-Server System on Solaris](#).
- The database must be running. If the database is not running, see [A.6.1.2 How to Start the Sybase Database Service](#).
- The FTP or SFTP server programs are running on the remote server, and the relevant ports are enabled. The port of FTP server is 21, and the port of SFTP server is 22.



### NOTE

- For details on how to start the FTP or SFTP server programs on Solaris, see [A.3.3.1 How to Start/Stop the FTP, TFTP, SFTP, and Telnet Services](#).
- For details on how to start the FTP or SFTP server programs on SUSE Linux, see [A.2.1 How to Start/Stop the FTP, TFTP, SFTP, and Telnet Services](#).
- For details on how to configure FTP, SFTP or TFTP services on Windows, see [A.1.7 How to Configure the FTP, SFTP, or TFTP Service on Windows OS](#).

## Context

- The temporary directory *tmp* is created in the **/opt** path during the restore of the database. If the *tmp* directory exists in the **/opt** path, you need to ensure that the owner and group of the directory are both **sybase**. Run the following commands to change the owner and group of the **/opt/tmp**.

```
chown -R sybase /opt/tmp
chgrp -R sybase /opt/tmp
```

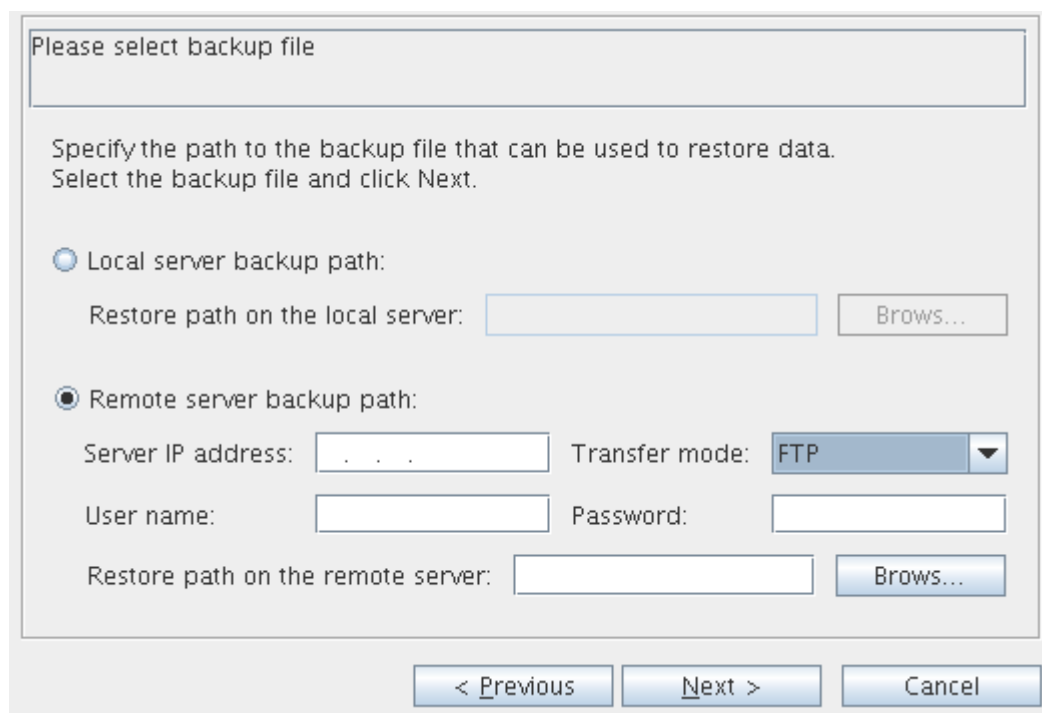
## Procedure

- 1 Log in to the MSuite client. For details, see [D.2.2 Logging In to the MSuite Client](#).
- 2 On the MSuite client, choose **Backup and Restore > Restore system data** from the main menu.
- 3 Select **Data Restore-Binary Mode(Recommended)**, and then click **Next**.

### NOTE

**Data Restore-Text Mode** is only used to locate and rectify the fault. This mode is not recommended during routine database restore.

- 4 Select **Remote server backup path** and set the associated parameters. Then, click **Next**.
  - **Server IP address**: indicates the IP address of the server where the restoration data is stored.
  - **Transfer mode**: The available options are FTP and SFTP.
  - **User name**: indicates the name of the FTP user or SFTP user.
  - **Password**: indicates the password of the FTP user or SFTP user.
  - **Remote server backup patch**: indicates the path for storing the data used for restoration. During backup, the backed up data is generated in a folder named by time. You can enter the path of this folder to restore the backed up data.



- 5 Click **Next**, the system starts the restoration preprocessing and data restoration, and displays the restoration progress in a progress bar. Wait patiently.





## CAUTION

If the system displays a message indicating component inconsistency and asking you whether to forcibly restore U2000 data, do as follows:

1. Read the message carefully and record involved components. Then, click **No** to choose not to continue restoring U2000 data.
2. Delete involved components. For details about how to delete involved components, see [D.4.2 Deleting a Component](#).
3. After involved components are deleted, restore U2000 data.

---

6 After U2000 data is restored, click **Finish**.

7 On the MSuite client, choose **System > Refresh NMS Information**. Alternatively, you can click the  icon on the toolbar.

----End

## Operations Through the CLI

On Solaris or SUSE Linux OS, if you fail to log in to the GUI desktop system, restore the U2000 data through the CLI.



## CAUTION

The MSuite adopts single-user mode, so you must exit all MSuite client GUIs before performing the backup through the CLI.

The operations in CLI mode are as follows:

On Solaris OS, run the following command as user **nmsuser**. On SUSE Linux OS, run the following command as user **root**.

```
cd /opt/U2000/engineering
./startclient.sh storage -ip 127.0.0.1 -port 12212 -username admin -password admin
-RestoreDB -StoreMode remote -TransMode ftp -Server 127.0.0.1 -FTPUserName abcde -
Pwd 12345 -FilePath /opt/nmsBackup/200811211230
```



### NOTE

The default user name and password are both **admin**. If the password has been changed, enter the changed password.

## Follow-up Procedure

After restoring U2000 data, start the NMS processes, for details, see [A.9.20 How to Start the Processes of the U2000 Single-Server System on Solaris](#).



### NOTE

- If the CORBA NBI, XML NBI, SNMP NBI, or text NBI is configured for the U2000, you need to reconfigure the NBI instance after successfully restoring the database. For details, see the related NBI user manual.
- After the preceding operations are complete, login passwords for the U2000 client, NE Software Management and U2000 System Monitor restore to be consistent with the U2000 data.

## D.9.4 Restoring U2000 Single-Server System (SUSE Linux-Distributed) Data

If the U2000 database is faulty, you can restore data on the current U2000 by using the backup U2000 data.

### D.9.4.1 Restoring U2000 Single-Server System (SUSE Linux-Distributed) Data from a Local Server

If the backup U2000 data is stored on a local server, you can restore U2000 data from the local server.

### D.9.4.2 Restoring U2000 Single-Server System (SUSE Linux-Distributed) Data from a Remote Server

If the backup U2000 data is stored on a remote server, you can restore U2000 data from the remote server.

### D.9.4.1 Restoring U2000 Single-Server System (SUSE Linux-Distributed) Data from a Local Server

If the backup U2000 data is stored on a local server, you can restore U2000 data from the local server.

#### Prerequisite

- U2000 processes must have been stopped. If U2000 processes are not stopped, see [A.9.24 How to End the Processes of the U2000 Single-Server System \(SUSE Linux-Distributed\)](#).
- The daem processes of each slaver server has been stopped. If the daem processes are not stopped, log in to the slave server as the root user and run the following command to stop the daem process of the slave server:  

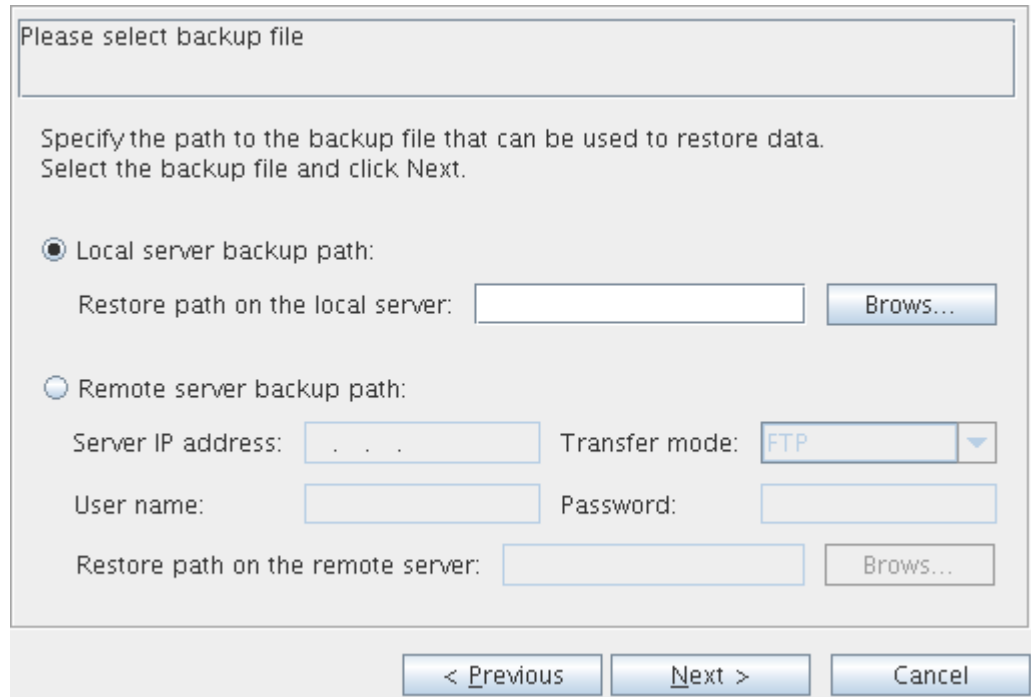
```
/etc/init.d/u2kdaem stop
```
- The database must be running. If the database is not running, see [A.7.5 How Can I Start the Oracle Database \(Single-Server System\)?](#).

#### Procedure

- 1 Log in to the MSuite client on the master server of active site. For details, see [D.2.2 Logging In to the MSuite Client](#).
- 2 On the MSuite client, choose **Backup and Restore > Restore system data** from the main menu.
- 3 Select **Local server backup path**, and then click **Browse** to select the data to be used for restoration.

#### NOTE

During backup, the backed up data is generated in a folder named by time. For example, the path is /201009271646. You can enter the path of this folder to restore the backed up data.



- 4 Click **Next**, the system starts the restoration preprocessing and data restoration, and displays the restoration progress in a progress bar. Wait patiently.



## CAUTION

If the system displays a message indicating component inconsistency and asking you whether to forcibly restore U2000 data, do as follows:

1. Read the message carefully and record involved components. Then, click **No** to choose not to continue restoring U2000 data.
2. Delete involved components. For details about how to delete involved components, see [D. 4.2 Deleting a Component](#).
3. After involved components are deleted, restore U2000 data.

- 
- 5 After U2000 data is restored, click **Finish**.
  - 6 On the MSuite client, choose **System > Refresh NMS Information**. Alternatively, you can click the  icon on the toolbar.

----End

## Operations Through the CLI

On Solaris or SUSE Linux OS, if you fail to log in to the GUI desktop system, restore the U2000 data through the CLI.

**CAUTION**

The MSuite adopts single-user mode, so you must exit all MSuite client GUIs before performing the backup through the CLI.

The operations in CLI mode are as follows:

On Solaris OS, run the following command as user **nmsuser**. On SUSE Linux OS, run the following command as user **root**.

```
cd /opt/U2000/engineering
./startclient.sh storage -ip 127.0.0.1 -port 12212 -username admin -password admin
-RestoreDB -StoreMode local -FilePath /opt/nmsBackup/200811211230
```

**NOTE**

The default user name and password are both **admin**. If the password has been changed, enter the changed password.

## Follow-up Procedure

1. After restoring U2000 data, log in to the each slave server start the daem processes, for details, see [A.9.39 How to Start the daem Process](#).
2. Log in to the master server of active site to start the NMS processes, for details, see [A.9.23 How to Start the Processes of the U2000 Single-Server System \(SUSE Linux-Distributed\)](#).

**NOTE**

- If the CORBA NBI, XML NBI, SNMP NBI, or text NBI is configured for the U2000, you need to reconfigure the NBI instance after successfully restoring the database. For details, see the related NBI user manual.
- After the preceding operations are complete, login passwords for the U2000 client, NE Software Management and U2000 System Monitor restore to be consistent with the U2000 data.

### D.9.4.2 Restoring U2000 Single-Server System (SUSE Linux-Distributed) Data from a Remote Server

If the backup U2000 data is stored on a remote server, you can restore U2000 data from the remote server.

#### Prerequisite

- U2000 processes must have been stopped. If U2000 processes are not stopped, see [A.9.24 How to End the Processes of the U2000 Single-Server System \(SUSE Linux-Distributed\)](#).
- The daem processes of each slaver server has been stopped. If the daem processes are not stopped, log in to the slave server as the root user and run the following command to stop the daem process of the slave server:  

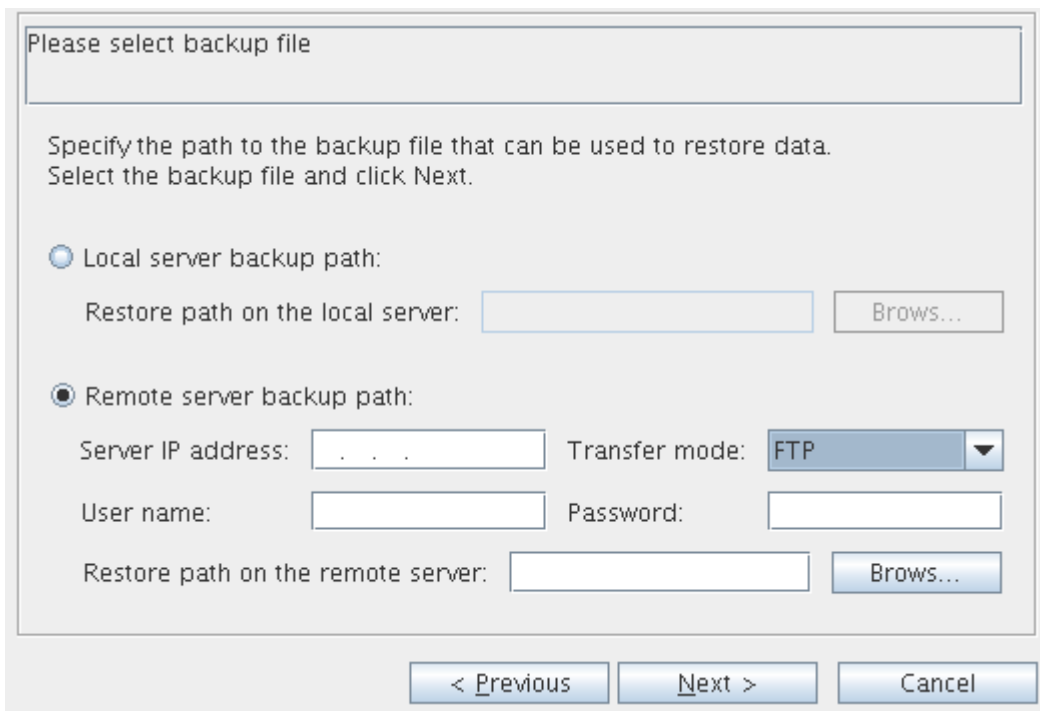
```
/etc/init.d/u2kdaem stop
```
- The database must be running. If the database is not running, see [A.7.5 How Can I Start the Oracle Database \(Single-Server System\)?](#).
- The FTP or SFTP server programs are running on the remote server, and the relevant ports are enabled. The port of FTP server is 21, and the port of SFTP server is 22.

 **NOTE**

- For details on how to start the FTP or SFTP server programs on Solaris, see [A.3.3.1 How to Start/Stop the FTP, TFTP, SFTP, and Telnet Services](#).
- For details on how to start the FTP or SFTP server programs on SUSE Linux, see [A.2.1 How to Start/Stop the FTP, TFTP, SFTP, and Telnet Services](#).
- For details on how to configure FTP, SFTP or TFTP services on Windows, see [A.1.7 How to Configure the FTP, SFTP, or TFTP Service on Windows OS](#).

## Procedure

- 1 Log in to the MSuite client on the master server of active site. For details, see [D.2.2 Logging In to the MSuite Client](#).
- 2 On the MSuite client, choose **Backup and Restore > Restore system data** from the main menu.
- 3 Select **Remote server backup path** and set the associated parameters. Then, click **Next**.
  - **Server IP address**: indicates the IP address of the server where the restoration data is stored.
  - **Transfer mode**: The available options are FTP and SFTP.
  - **User name**: indicates the name of the FTP user or SFTP user.
  - **Password**: indicates the password of the FTP user or SFTP user.
  - **Remote server backup patch**: indicates the path for storing the data used for restoration. During backup, the backed up data is generated in a folder named by time. You can enter the path of this folder to restore the backed up data.



- 4 Click **Next**, the system starts the restoration preprocessing and data restoration, and displays the restoration progress in a progress bar. Wait patiently.

**CAUTION**

If the system displays a message indicating component inconsistency and asking you whether to forcibly restore U2000 data, do as follows:

1. Read the message carefully and record involved components. Then, click **No** to choose not to continue restoring U2000 data.
  2. Delete involved components. For details about how to delete involved components, see [D.4.2 Deleting a Component](#).
  3. After involved components are deleted, restore U2000 data.
- 

- 5 After U2000 data is restored, click **Finish**.
- 6 On the MSuite client, choose **System > Refresh NMS Information**. Alternatively, you can click the  icon on the toolbar.

----End

## Operations Through the CLI

On Solaris or SUSE Linux OS, if you fail to log in to the GUI desktop system, restore the U2000 data through the CLI.

**CAUTION**

The MSuite adopts single-user mode, so you must exit all MSuite client GUIs before performing the backup through the CLI.

---

The operations in CLI mode are as follows:

On Solaris OS, run the following command as user **nmsuser**. On SUSE Linux OS, run the following command as user **root**.

```
cd /opt/U2000/engineering
./startclient.sh storage -ip 127.0.0.1 -port 12212 -username admin -password admin
-RestoreDB -StoreMode remote -TransMode ftp -Server 127.0.0.1 -FTPUserName abcde -
Pwd 12345 -FilePath /opt/nmsBackup/200811211230
```

**NOTE**

The default user name and password are both **admin**. If the password has been changed, enter the changed password.

## Follow-up Procedure

1. After restoring U2000 data, log in to the each slave server start the daem processes, for details, see [A.9.39 How to Start the daem Process](#).
2. Log in to the master server of active site to start the NMS processes, for details, see [A.9.23 How to Start the Processes of the U2000 Single-Server System \(SUSE Linux-Distributed\)](#).

 **NOTE**

- If the CORBA NBI, XML NBI, SNMP NBI, or text NBI is configured for the U2000, you need to reconfigure the NBI instance after successfully restoring the database. For details, see the related NBI user manual.
- After the preceding operations are complete, login passwords for the U2000 client, NE Software Management and U2000 System Monitor restore to be consistent with the U2000 data.

## D.9.5 Restoring U2000 High Availability System (Windows) Data

If the U2000 database is faulty, you can restore data on the current U2000 by using the backup U2000 data.

### D.9.5.1 Restoring U2000 High Availability System (Windows) Data from a Local Server

If the backup U2000 data is stored on a local server, you can restore U2000 data from the local server.

### D.9.5.2 Restoring U2000 High Availability System (Windows) Data from a Remote Server

If the backup U2000 data is stored on a remote server, you can restore U2000 data from the remote server.

### D.9.5.1 Restoring U2000 High Availability System (Windows) Data from a Local Server

If the backup U2000 data is stored on a local server, you can restore U2000 data from the local server.

## Prerequisite

- U2000 processes must have been stopped. If U2000 processes are not stopped, see [A.9.27 How to End the U2000 Processes of the High Availability System \(Windows\)](#).
- The database of the active site must be running. If the database is not running, see [A.5.4 How to Start the SQL Server Database](#).
- If the database of U2000 A needs to be restored on U2000 B, paths for storing database files on the U2000 A and U2000 B must be the same.

## Context



### CAUTION

The operations mentioned in this topic are applicable only to the case where the components and instance information among the backup U2000 data are consistent with the counterparts deployed on the current U2000. For details about how to restore U2000 data in other cases, see [D.9.8 Restoring Data of a U2000 High Availability System \(Cross-U2000\)](#).

## Procedure

- 1 Log in to the MSuite client on the active site. For details, see [D.2.2 Logging In to the MSuite Client](#).
- 2 On the MSuite client, choose **Backup and Restore > Restore system data** from the main menu.

- 3 Select **Data Restore-Binary Mode(Recommended)**, and then click **Next**.

**NOTE**

**Data Restore-Text Mode** is only used to locate and rectify the fault. This mode is not recommended during routine database restore.

- 4 Select **Local server backup path**, and then click **Browse** to select the data to be used for restoration.

**NOTE**

During backup, the backed up data is generated in a folder named by time. For example, the path is /201009271646. You can enter the path of this folder to restore the backed up data.

Please select backup file

Specify the path to the backup file that can be used to restore data.  
Select the backup file and click Next.

☒ Local server backup path:

Restore path on the local server:

☐ Remote server backup path:

Server IP address:  Transfer mode:

User name:  Password:

Restore path on the remote server:

- 5 Click **Next**, the system starts the restoration preprocessing and data restoration, and displays the restoration progress in a progress bar. Wait patiently.

**CAUTION**

If the system displays a message indicating component inconsistency and asking you whether to forcibly restore U2000 data, do as follows:

1. Read the message carefully and record involved components. Then, click **No** to choose not to continue restoring U2000 data.
2. Delete involved components. For details about how to delete involved components, see [D. 4.2 Deleting a Component](#).
3. After involved components are deleted, restore U2000 data.

- 6 After U2000 data is restored, click **Finish**.



- 7 On the MSuite client, choose **System > Refresh NMS Information**. Alternatively, you can click the  icon on the toolbar.

- 8 After U2000 data is restored, the U2000 automatically synchronizes data between the primary and secondary sites. To view data synchronization status, run the following command on the active site:

```
C:\> vxrlink -g datadg -i2 status datarlk
```

- If **RLINK is up to date** is displayed, it indicates that data replication is normal.
  - If **RLINK is up to date** is not displayed, it indicates that data synchronization has not been finished. Running the preceding command to check data replication status every half an hour is recommended. You must check data replication status on a regular basis until **RLINK is up to date** is displayed.
- 9 In the scenario where the current database is SQL Server2000 SP4, check whether the database sorting mode is set to binary. For details, see [A.5.6 How to Check Whether the SQL Server Database Can Be Sorted in Binary Mode](#). If the database sorting mode is not set to binary, change it to binary. For details, see [A.5.7 How to Change the Database Sorting Mode to Binary](#).

----End

## Follow-up Procedure

After restoring U2000 data, start the NMS processes, for details, see [A.9.26 How to Start the U2000 Processes of the High Availability System \(Windows\)](#).

### NOTE

- If the CORBA NBI, XML NBI, SNMP NBI, or text NBI is configured for the U2000, you need to reconfigure the NBI instance after successfully restoring the database. For details, see the related NBI user manual.
- After the preceding operations are complete, login passwords for the U2000 client, NE Software Management and U2000 System Monitor restore to be consistent with the U2000 data.

## D.9.5.2 Restoring U2000 High Availability System (Windows) Data from a Remote Server

If the backup U2000 data is stored on a remote server, you can restore U2000 data from the remote server.

## Prerequisite

- U2000 processes must have been stopped. If U2000 processes are not stopped, see [A.9.27 How to End the U2000 Processes of the High Availability System \(Windows\)](#).
- The database of the active site must be running. If the database is not running, see [A.5.4 How to Start the SQL Server Database](#).
- The FTP or SFTP server programs are running on the remote server, and the relevant ports are enabled. The port of FTP server is 21, and the port of SFTP server is 22.

 **NOTE**

- For details on how to start the FTP or SFTP server programs on Solaris, see [A.3.3.1 How to Start/Stop the FTP, TFTP, SFTP, and Telnet Services](#).
- For details on how to start the FTP or SFTP server programs on SUSE Linux, see [A.2.1 How to Start/Stop the FTP, TFTP, SFTP, and Telnet Services](#).
- For details on how to configure FTP, SFTP or TFTP services on Windows, see [A.1.7 How to Configure the FTP, SFTP, or TFTP Service on Windows OS](#).
- If the database of U2000 A needs to be restored on U2000 B, paths for storing database files on the U2000 A and U2000 B must be the same.

## Context

**CAUTION**

The operations mentioned in this topic are applicable only to the case where the components and instance information among the backup U2000 data are consistent with the counterparts deployed on the current U2000. For details about how to restore U2000 data in other cases, see [D.9.8 Restoring Data of a U2000 High Availability System \(Cross-U2000\)](#).

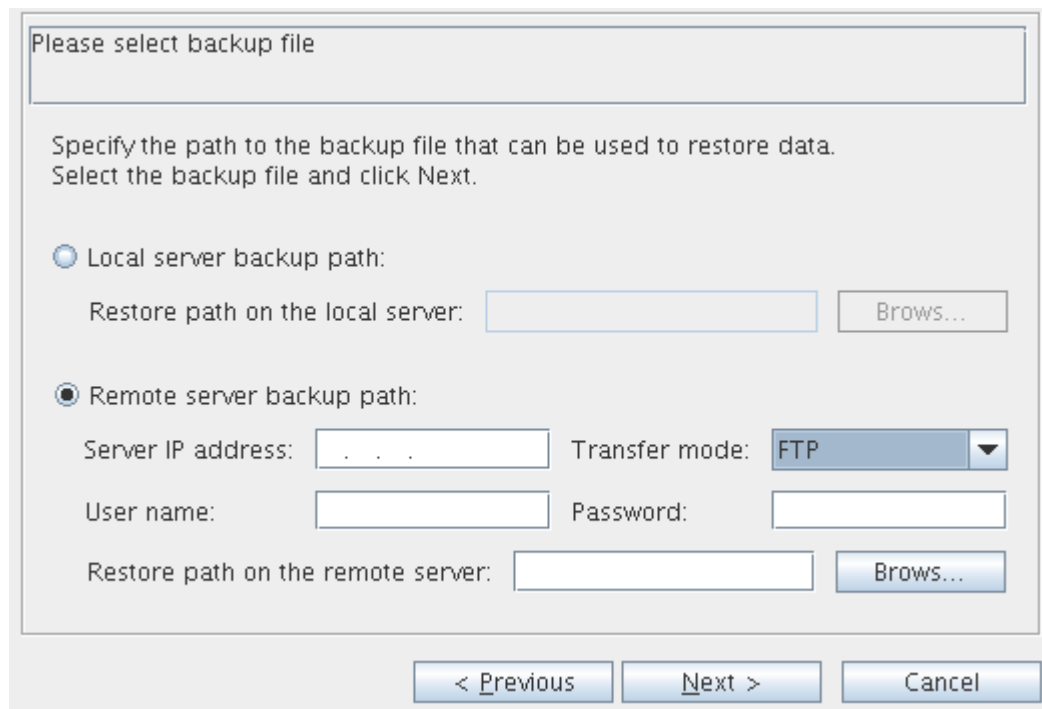
## Procedure

- 1 Log in to the MSuite client on the active site. For details, see [D.2.2 Logging In to the MSuite Client](#).
- 2 On the MSuite client, choose **Backup and Restore > Restore system data** from the main menu.
- 3 Select **Data Restore-Binary Mode(Recommended)**, and then click **Next**.

 **NOTE**

**Data Restore-Text Mode** is only used to locate and rectify the fault. This mode is not recommended during routine database restore.

- 4 Select **Remote server backup path** and set the associated parameters. Then, click **Next**.
  - **Server IP address**: indicates the IP address of the server where the restoration data is stored.
  - **Transfer mode**: The available options are FTP and SFTP.
  - **User name**: indicates the name of the FTP user or SFTP user.
  - **Password**: indicates the password of the FTP user or SFTP user.
  - **Remote server backup path**: indicates the path for storing the data used for restoration. During backup, the backed up data is generated in a folder named by time. You can enter the path of this folder to restore the backed up data.



- 5 Click **Next**, the system starts the restoration preprocessing and data restoration, and displays the restoration progress in a progress bar. Wait patiently.



## CAUTION

If the system displays a message indicating component inconsistency and asking you whether to forcibly restore U2000 data, do as follows:

1. Read the message carefully and record involved components. Then, click **No** to choose not to continue restoring U2000 data.
2. Delete involved components. For details about how to delete involved components, see [D. 4.2 Deleting a Component](#).
3. After involved components are deleted, restore U2000 data.

- 6 After U2000 data is restored, click **Finish**.
- 7 On the MSuite client, choose **System > Refresh NMS Information**. Alternatively, you can click the  icon on the toolbar.
- 8 After U2000 data is restored, the U2000 automatically synchronizes data between the primary and secondary sites. To view data synchronization status, run the following command on the active site:

```
C:\> vxrlink -g datadg -i2 status datarlk
```

- If **RLINK is up to date** is displayed, it indicates that data replication is normal.
- If **RLINK is up to date** is not displayed, it indicates that data synchronization has not been finished. Running the preceding command to check data replication status every half an hour

is recommended. You must check data replication status on a regular basis until **RLINK is up to date** is displayed.

- 9 In the scenario where the current database is SQL Server2000 SP4, check whether the database sorting mode is set to binary. For details, see [A.5.6 How to Check Whether the SQL Server Database Can Be Sorted in Binary Mode](#). If the database sorting mode is not set to binary, change it to binary. For details, see [A.5.7 How to Change the Database Sorting Mode to Binary](#).

----End

## Follow-up Procedure

After restoring U2000 data, start the NMS processes, for details, see [A.9.26 How to Start the U2000 Processes of the High Availability System \(Windows\)](#).

### NOTE

- If the CORBA NBI, XML NBI, SNMP NBI, or text NBI is configured for the U2000, you need to reconfigure the NBI instance after successfully restoring the database. For details, see the related NBI user manual.
- After the preceding operations are complete, login passwords for the U2000 client, NE Software Management and U2000 System Monitor restore to be consistent with the U2000 data.

## D.9.6 Restoring U2000 High Availability System (Solaris) Data

If the U2000 database is faulty, you can restore data on the current U2000 by using the backup U2000 data.

### [D.9.6.1 Restoring U2000 High Availability System \(Solaris\) Data from a Local Server](#)

If the backup U2000 data is stored on a local server, you can restore U2000 data from the local server.

### [D.9.6.2 Restoring U2000 High Availability System \(Solaris\) Data from a Remote Server](#)

If the backup U2000 data is stored on a remote server, you can restore U2000 data from the remote server.

### D.9.6.1 Restoring U2000 High Availability System (Solaris) Data from a Local Server

If the backup U2000 data is stored on a local server, you can restore U2000 data from the local server.

## Prerequisite

- Database versions must be the same.
- U2000 processes must have been stopped. If U2000 processes are not stopped, see [A.9.30 How to End the U2000 Processes of the High Availability System \(Solaris\)](#).
- The database of the active site must be running. If the database is not running, see [A.6.1.2 How to Start the Sybase Database Service](#).
- In the Solaris OS, ensure that the owner and user group of the folder that stores backup data are both **sybase**. You can run the following commands to change the owner and user group of files:  

```
chown -R sybase backup path
chgrp -R sybase backup path
```

## Context



### CAUTION

The operations mentioned in this topic are applicable only to the case where the components and instance information among the backup U2000 data are consistent with the counterparts deployed on the current U2000. For details about how to restore U2000 data in other cases, see [D.9.8 Restoring Data of a U2000 High Availability System \(Cross-U2000\)](#).

## Procedure

- 1 Log in to the MSuite client on the active site. For details, see [D.2.2 Logging In to the MSuite Client](#).
- 2 On the MSuite client, choose **Backup and Restore > Restore system data** from the main menu.
- 3 Select **Data Restore-Binary Mode(Recommended)**, and then click **Next**.



#### NOTE

**Data Restore-Text Mode** is only used to locate and rectify the fault. This mode is not recommended during routine database restore.

- 4 Select **Local server backup path**, and then click **Browse** to select the data to be used for restoration.



#### NOTE

During backup, the backed up data is generated in a folder named by time. For example, the path is /201009271646. You can enter the path of this folder to restore the backed up data.

- 5 Click **Next**, the system starts the restoration preprocessing and data restoration, and displays the restoration progress in a progress bar. Wait patiently.

**CAUTION**

If the system displays a message indicating component inconsistency and asking you whether to forcibly restore U2000 data, do as follows:

1. Read the message carefully and record involved components. Then, click **No** to choose not to continue restoring U2000 data.
  2. Delete involved components. For details about how to delete involved components, see [D. 4.2 Deleting a Component](#).
  3. After involved components are deleted, restore U2000 data.
- 

- 6 After U2000 data is restored, click **Finish**.
- 7 On the MSuite client, choose **System > Refresh NMS Information**. Alternatively, you can click the  icon on the toolbar.
- 8 After U2000 data is restored, the U2000 automatically synchronizes data between the primary and secondary sites. To view data synchronization status, run the following command on the active site:

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

If the displayed information contains "needs dcm resynchronization", it indicates that the status is abnormal. Then, run the following command to synchronize data:

```
vradmin -g datadg resync datarvg
```

----End

## Operations Through the CLI

On Solaris or SUSE Linux OS, if you fail to log in to the GUI desktop system, restore the U2000 data through the CLI.

**CAUTION**

The MSuite adopts single-user mode, so you must exit all MSuite client GUIs before performing the backup through the CLI.

---

The operations in CLI mode are as follows:

On Solaris OS, run the following command as user **nmsuser**. On SUSE Linux OS, run the following command as user **root**.

```
cd /opt/U2000/engineering
./startclient.sh storage -ip 127.0.0.1 -port 12212 -username admin -password admin
-RestoreDB -StoreMode local -FilePath /opt/nmsBackup/200811211230
```

**NOTE**

The default user name and password are both **admin**. If the password has been changed, enter the changed password.

## Follow-up Procedure

After restoring U2000 data, start the NMS processes, for details, see [A.9.29 How to Start the U2000 Processes of the High Availability System \(Solaris\)](#).

### NOTE

- If the CORBA NBI, XML NBI, SNMP NBI, or text NBI is configured for the U2000, you need to reconfigure the NBI instance after successfully restoring the database. For details, see the related NBI user manual.
- After the preceding operations are complete, login passwords for the U2000 client, NE Software Management and U2000 System Monitor restore to be consistent with the U2000 data.

## D.9.6.2 Restoring U2000 High Availability System (Solaris) Data from a Remote Server

If the backup U2000 data is stored on a remote server, you can restore U2000 data from the remote server.

## Prerequisite

- Database versions must be the same.
- U2000 processes must have been stopped. If U2000 processes are not stopped, see [A.9.30 How to End the U2000 Processes of the High Availability System \(Solaris\)](#).
- The database of the active site must be running. If the database is not running, see [A.6.1.2 How to Start the Sybase Database Service](#).
- The FTP or SFTP server programs are running on the remote server, and the relevant ports are enabled. The port of FTP server is 21, and the port of SFTP server is 22.

### NOTE

- For details on how to start the FTP or SFTP server programs on Solaris, see [A.3.3.1 How to Start/Stop the FTP, TFTP, SFTP, and Telnet Services](#).
- For details on how to start the FTP or SFTP server programs on SUSE Linux, see [A.2.1 How to Start/Stop the FTP, TFTP, SFTP, and Telnet Services](#).
- For details on how to configure FTP, SFTP or TFTP services on Windows, see [A.1.7 How to Configure the FTP, SFTP, or TFTP Service on Windows OS](#).

## Context



### CAUTION

The operations mentioned in this topic are applicable only to the case where the components and instance information among the backup U2000 data are consistent with the counterparts deployed on the current U2000. For details about how to restore U2000 data in other cases, see [D.9.8 Restoring Data of a U2000 High Availability System \(Cross-U2000\)](#).

- The temporary directory *tmp* is created in the */opt* path during the restore of the database. If the *tmp* directory exists in the */opt* path, you need to ensure that the owner and group of the directory are both **sybase**. Run the following commands to change the owner and group of the */opt/tmp*.  
# `chown -R sybase /opt/tmp`  
# `chgrp -R sybase /opt/tmp`

## Procedure

- 1 Log in to the MSuite client on the active site. For details, see [D.2.2 Logging In to the MSuite Client](#).
- 2 Select **Remote server backup path** and set the associated parameters. Then, click **Next**.
  - **Server IP address**: indicates the IP address of the server where the restoration data is stored.
  - **Transfer mode**: The available options are FTP and SFTP.
  - **User name**: indicates the name of the FTP user or SFTP user.
  - **Password**: indicates the password of the FTP user or SFTP user.
  - **Remote server backup patch**: indicates the path for storing the data used for restoration. During backup, the backed up data is generated in a folder named by time. You can enter the path of this folder to restore the backed up data.

Please select backup file

Specify the path to the backup file that can be used to restore data.  
Select the backup file and click Next.

☐ Local server backup path:

Restore path on the local server:

☒ Remote server backup path:

Server IP address:  Transfer mode:

User name:  Password:

Restore path on the remote server:

- 3 Click **Next**, the system starts the restoration preprocessing and data restoration, and displays the restoration progress in a progress bar. Wait patiently.



### CAUTION

If the system displays a message indicating component inconsistency and asking you whether to forcibly restore U2000 data, do as follows:

1. Read the message carefully and record involved components. Then, click **No** to choose not to continue restoring U2000 data.
2. Delete involved components. For details about how to delete involved components, see [D.4.2 Deleting a Component](#).
3. After involved components are deleted, restore U2000 data.



- 4 On the MSuite client, choose **System > Refresh NMS Information**. Alternatively, you can click the  icon on the toolbar.

- 5 After U2000 data is restored, the U2000 automatically synchronizes data between the primary and secondary sites. To view data synchronization status, run the following command on the active site:

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

If the displayed information contains "needs dcm resynchronization", it indicates that the status is abnormal. Then, run the following command to synchronize data:

```
vradmin -g datadg resync datarvg
```

----End

## Operations Through the CLI

On Solaris or SUSE Linux OS, if you fail to log in to the GUI desktop system, restore the U2000 data through the CLI.



### CAUTION

The MSuite adopts single-user mode, so you must exit all MSuite client GUIs before performing the backup through the CLI.

---

The operations in CLI mode are as follows:

On Solaris OS, run the following command as user **nmsuser**. On SUSE Linux OS, run the following command as user **root**.

```
cd /opt/U2000/engineering
./startclient.sh storage -ip 127.0.0.1 -port 12212 -username admin -password admin
-RestoreDB -StoreMode remote -TransMode ftp -Server 127.0.0.1 -FTPUserName abcde -
Pwd 12345 -FilePath /opt/nmsBackup/200811211230
```



### NOTE

The default user name and password are both **admin**. If the password has been changed, enter the changed password.

## Follow-up Procedure

After restoring U2000 data, start the NMS processes, for details, see [A.9.29 How to Start the U2000 Processes of the High Availability System \(Solaris\)](#).



### NOTE

- If the CORBA NBI, XML NBI, SNMP NBI, or text NBI is configured for the U2000, you need to reconfigure the NBI instance after successfully restoring the database. For details, see the related NBI user manual.
- After the preceding operations are complete, login passwords for the U2000 client, NE Software Management and U2000 System Monitor restore to be consistent with the U2000 data.

## D.9.7 Restoring U2000 High Availability System (SUSE Linux-Distributed) Data

If the U2000 database is faulty, you can restore data on the current U2000 by using the backup U2000 data.

### D.9.7.1 Restoring U2000 High Availability System (SUSE Linux-Distributed) Data from a Local Server

If the backup U2000 data is stored on a local server, you can restore U2000 data from the local server.

### D.9.7.2 Restoring U2000 High Availability System (SUSE Linux-Distributed) Data from a Remote Server

If the backup U2000 data is stored on a remote server, you can restore U2000 data from the remote server.

### D.9.7.1 Restoring U2000 High Availability System (SUSE Linux-Distributed) Data from a Local Server

If the backup U2000 data is stored on a local server, you can restore U2000 data from the local server.

#### Prerequisite

- U2000 processes must have been stopped. If U2000 processes are not stopped, see [A.9.33 How to End the U2000 Processes of the High Availability System \(SUSE Linux-Distributed\)](#).
- The daem processes of each slaver server has been stopped. If the daem processes are not stopped, log in to the slave server as the root user and run the following command to stop the daem process of the slave server:  

```
/etc/init.d/u2kdaem stop
```
- The database of the active site must be running. If the database is not running, see [A.7.5 How Can I Start the Oracle Database \(Single-Server System\)?](#).

#### Context



#### CAUTION

The operations mentioned in this topic are applicable only to the case where the components and instance information among the backup U2000 data are consistent with the counterparts deployed on the current U2000. For details about how to restore U2000 data in other cases, see [D.9.8 Restoring Data of a U2000 High Availability System \(Cross-U2000\)](#).

---

#### Procedure

- 1 Log in to the MSuite client on the master server of the active site. For details, see [D.2.2 Logging In to the MSuite Client](#).
- 2 On the MSuite client, choose **Backup and Restore > Restore system data** from the main menu.

- 3 Select **Local server backup path**, and then click **Browse** to select the data to be used for restoration.



**NOTE**

During backup, the backed up data is generated in a folder named by time. For example, the path is / 201009271646. You can enter the path of this folder to restore the backed up data.

Please select backup file

Specify the path to the backup file that can be used to restore data.  
Select the backup file and click Next.

☒ Local server backup path:

Restore path on the local server:

☐ Remote server backup path:

Server IP address:  Transfer mode:

User name:  Password:

Restore path on the remote server:

- 4 Click **Next**, the system starts the restoration preprocessing and data restoration, and displays the restoration progress in a progress bar. Wait patiently.



**CAUTION**

If the system displays a message indicating component inconsistency and asking you whether to forcibly restore U2000 data, do as follows:

1. Read the message carefully and record involved components. Then, click **No** to choose not to continue restoring U2000 data.
2. Delete involved components. For details about how to delete involved components, see [D.4.2 Deleting a Component](#).
3. After involved components are deleted, restore U2000 data.

- 5 After U2000 data is restored, click **Finish**.
- 6 On the MSuite client, choose **System > Refresh NMS Information**. Alternatively, you can click the  icon on the toolbar.
- 7 After U2000 data is restored, the U2000 automatically synchronizes data between the primary and secondary sites. To view data synchronization status, run the following command on the active site:

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

If the displayed information contains "needs dcm resynchronization", it indicates that the status is abnormal. Then, run the following command to synchronize data:

```
vradmin -g datadg resync datarvg
```

----End

## Operations Through the CLI

On Solaris or SUSE Linux OS, if you fail to log in to the GUI desktop system, restore the U2000 data through the CLI.



### CAUTION

The MSuite adopts single-user mode, so you must exit all MSuite client GUIs before performing the backup through the CLI.

---

The operations in CLI mode are as follows:

On Solaris OS, run the following command as user **nmsuser**. On SUSE Linux OS, run the following command as user **root**.

```
cd /opt/U2000/engineering
./startclient.sh storage -ip 127.0.0.1 -port 12212 -username admin -password admin
-RestoreDB -StoreMode local -FilePath /opt/nmsBackup/200811211230
```



### NOTE

The default user name and password are both **admin**. If the password has been changed, enter the changed password.

## Follow-up Procedure

1. After restoring U2000 data, log in to the each slave server start the daem processes, for details, see [A.9.39 How to Start the daem Process](#).
2. Log in to the master server of active site to start the NMS processes, for details, see [A.9.32 How to Start the U2000 Processes of the High Availability System \(SUSE Linux-Distributed\)](#).



### NOTE

- If the CORBA NBI, XML NBI, SNMP NBI, or text NBI is configured for the U2000, you need to reconfigure the NBI instance after successfully restoring the database. For details, see the related NBI user manual.
- After the preceding operations are complete, login passwords for the U2000 client, NE Software Management and U2000 System Monitor restore to be consistent with the U2000 data.

### D.9.7.2 Restoring U2000 High Availability System (SUSE Linux-Distributed) Data from a Remote Server

If the backup U2000 data is stored on a remote server, you can restore U2000 data from the remote server.

## Prerequisite

- U2000 processes must have been stopped. If U2000 processes are not stopped, see [A.9.33 How to End the U2000 Processes of the High Availability System \(SUSE Linux-Distributed\)](#).
- The daem processes of each slaver server has been stopped. If the daem processes are not stopped, log in to the slave server as the root user and run the following command to stop the daem process of the slave server:  

```
/etc/init.d/u2kdaem stop
```
- The database of the active site must be running. If the database is not running, see [A.7.5 How Can I Start the Oracle Database \(Single-Server System\)?](#).
- The FTP or SFTP server programs are running on the remote server, and the relevant ports are enabled. The port of FTP server is 21, and the port of SFTP server is 22.

### NOTE

- For details on how to start the FTP or SFTP server programs on Solaris, see [A.3.3.1 How to Start/Stop the FTP, TFTP, SFTP, and Telnet Services](#).
- For details on how to start the FTP or SFTP server programs on SUSE Linux, see [A.2.1 How to Start/Stop the FTP, TFTP, SFTP, and Telnet Services](#).
- For details on how to configure FTP, SFTP or TFTP services on Windows, see [A.1.7 How to Configure the FTP, SFTP, or TFTP Service on Windows OS](#).

## Context



### CAUTION

The operations mentioned in this topic are applicable only to the case where the components and instance information among the backup U2000 data are consistent with the counterparts deployed on the current U2000. For details about how to restore U2000 data in other cases, see [D.9.8 Restoring Data of a U2000 High Availability System \(Cross-U2000\)](#).

## Procedure

- 1 Log in to the MSuite client on the master server of the active site. For details, see [D.2.2 Logging In to the MSuite Client](#).
- 2 On the MSuite client, choose **Backup and Restore > Restore system data** from the main menu.
- 3 Select **Remote server backup path** and set the associated parameters. Then, click **Next**.
  - **Server IP address**: indicates the IP address of the server where the restoration data is stored.
  - **Transfer mode**: The available options are FTP and SFTP.
  - **User name**: indicates the name of the FTP user or SFTP user.
  - **Password**: indicates the password of the FTP user or SFTP user.
  - **Remote server backup patch**: indicates the path for storing the data used for restoration. During backup, the backed up data is generated in a folder named by time. You can enter the path of this folder to restore the backed up data.

- 4 Click **Next**, the system starts the restoration preprocessing and data restoration, and displays the restoration progress in a progress bar. Wait patiently.



## CAUTION

If the system displays a message indicating component inconsistency and asking you whether to forcibly restore U2000 data, do as follows:

1. Read the message carefully and record involved components. Then, click **No** to choose not to continue restoring U2000 data.
2. Delete involved components. For details about how to delete involved components, see [D. 4.2 Deleting a Component](#).
3. After involved components are deleted, restore U2000 data.

- 5 After U2000 data is restored, click **Finish**.
- 6 On the MSuite client, choose **System > Refresh NMS Information**. Alternatively, you can click the  icon on the toolbar.
- 7 After U2000 data is restored, the U2000 automatically synchronizes data between the primary and secondary sites. To view data synchronization status, run the following command on the active site:

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

If the displayed information contains "needs dcm resynchronization", it indicates that the status is abnormal. Then, run the following command to synchronize data:

```
vradmin -g datadg resync datarvg
```

----End

## Operations Through the CLI

On Solaris or SUSE Linux OS, if you fail to log in to the GUI desktop system, restore the U2000 data through the CLI.



### CAUTION

The MSuite adopts single-user mode, so you must exit all MSuite client GUIs before performing the backup through the CLI.

---

The operations in CLI mode are as follows:

On Solaris OS, run the following command as user **nmsuser**. On SUSE Linux OS, run the following command as user **root**.

```
cd /opt/U2000/engineering
./startclient.sh storage -ip 127.0.0.1 -port 12212 -username admin -password admin
-RestoreDB -StoreMode remote -TransMode ftp -Server 127.0.0.1 -FTPUserName abcde -
Pwd 12345 -FilePath /opt/nmsBackup/200811211230
```



### NOTE

The default user name and password are both **admin**. If the password has been changed, enter the changed password.

## Follow-up Procedure

1. After restoring U2000 data, log in to the each slave server start the daem processes, for details, see [A.9.39 How to Start the daem Process](#).
2. Log in to the master server of active site to start the NMS processes, for details, see [A.9.32 How to Start the U2000 Processes of the High Availability System \(SUSE Linux-Distributed\)](#).



### NOTE

- If the CORBA NBI, XML NBI, SNMP NBI, or text NBI is configured for the U2000, you need to reconfigure the NBI instance after successfully restoring the database. For details, see the related NBI user manual.
- After the preceding operations are complete, login passwords for the U2000 client, NE Software Management and U2000 System Monitor restore to be consistent with the U2000 data.

## D.9.8 Restoring Data of a U2000 High Availability System (Cross-U2000)

If multiple sets of U2000s are available, and the components installed on the U2000s as well as the database versions and OS versions of the U2000s are the same, you can restore data cross these U2000s. That is, the backup data of U2000 A can be used to restore the data of U2000 B.

### Prerequisite

- U2000 versions must be the same.
- Database versions must be the same.
- Installed components must be the same.

## Procedure

- 1 Separate the primary site and secondary site. For details, see [D.6.2 Deleting the HA Relationship Between the Primary and Secondary Sites](#).
- 2 Restore databases of the primary and secondary sites.



### CAUTION

Perform this step on both the primary and secondary sites.

---

- For details about how to restore data for the High Availability System (Windows), see [D.9.5 Restoring U2000 High Availability System \(Windows\) Data](#).
  - For details about restoring data for the High Availability System (Solaris), see [D.9.6 Restoring U2000 High Availability System \(Solaris\) Data](#).
  - For details about restoring data for the High Availability System (SUSE Linux-Distributed), see [D.9.7 Restoring U2000 High Availability System \(SUSE Linux-Distributed\) Data](#).
- 3 Connect the primary and secondary sites. For details, see [D.6.1 Establishing the HA Relationship Between the Primary and Secondary Sites](#).

----End

## Follow-up Procedure



### NOTE

- If the CORBA NBI, XML NBI, SNMP NBI, or text NBI is configured for the U2000, you need to reconfigure the NBI instance after successfully restoring the database. For details, see the related NBI user manual.
- After the preceding operations are complete, login passwords for the U2000 client, NE Software Management and U2000 System Monitor restore to be consistent with the U2000 data.

## D.9.9 Initializing the U2000 Database

This topic describes how to initialize the U2000 database. Initialize the U2000 database before it is in disorder or restored, or data is damaged.

### Prerequisite

- The NMS processes are ended. Perform the following operations to end the NMS processes if they are running:
  - For the Single-Server System (Windows), see [A.9.18 How to End the Processes of the U2000 Single-Server System on Windows](#).
  - For the Single-Server System (Solaris), see [A.9.21 How to End the Processes of the U2000 Single-Server System on Solaris](#).
  - For the Single-Server System (SUSE Linux-Distributed), see [A.9.24 How to End the Processes of the U2000 Single-Server System \(SUSE Linux-Distributed\)](#).
  - For the High Availability System (Windows), see [A.9.27 How to End the U2000 Processes of the High Availability System \(Windows\)](#).



- For the High Availability System (Solaris), see [A.9.30 How to End the U2000 Processes of the High Availability System \(Solaris\)](#).
  - For the High Availability System (SUSE Linux-Distributed), see [A.9.33 How to End the U2000 Processes of the High Availability System \(SUSE Linux-Distributed\)](#).
- The database is running. Perform the following operations to start the database if it is not running:
  - For the Single-Server System (Windows), see [A.5.4 How to Start the SQL Server Database](#).
  - For the Single-Server System (Solaris), see [A.6.1.2 How to Start the Sybase Database Service](#).
  - For the Single-Server System (SUSE Linux-Distributed), see [A.7.5 How Can I Start the Oracle Database \(Single-Server System\)?](#).
  - For the High Availability System (Windows), see [A.5.4 How to Start the SQL Server Database](#).
  - For the High Availability System (Solaris), see [A.6.1.2 How to Start the Sybase Database Service](#).
  - For the High Availability System (SUSE Linux-Distributed), see [A.7.4 How to Start the Oracle Database in the High Availability System](#).
- In a distributed system, the daem processes of the slave servers are ended. Log in to each slave server and run the following command to stop the daem processes:  
`# /etc/init.d/u2kdaem stop`
- In a high availability (HA) system, freeze the entire resource group.

## Context



### CAUTION

This operation will delete all U2000 data from the database and restore all U2000 information to default settings. Therefore, back up the U2000 database and NMS deployment information before performing initialization.

This operation will:

- Restore the login passwords for the U2000 client, NE Software Management and the U2000 System Monitor client to the default passwords (the default passwords are blank).
  - Delete all service data that users configured on the U2000 client.
- 

## Procedure

- 1 Log in to the MSuite client. For details, see [D.2.2 Logging In to the MSuite Client](#).
- 2 On the MSuite client, choose **System > Initialize Database** from the main menu. The initialization wizard and a prompt will be displayed.
- 3 Read the initialization information carefully and click **Next**.
- 4 Click **Yes**. The system starts initializing the database and displays a progress bar. Wait patiently.
- 5 After the initialization is complete, click **Finish**.

- 6 On the MSuite client, choose **System > Refresh NMS Information**. Alternatively, you can click the  icon on the toolbar.
- 7 **Optional:** In the HA system, run the **hagui&** command to log in to the VCS client, unfreeze the entire resource group by using the **UnFreeze** menu item, and then make the NMS resources online by using the **Online** menu item.

----End

## Operations Through the CLI

On Solaris or SUSE Linux OS, if you fail to log in to the GUI desktop system, initialize the database through the CLI.

The operations in CLI mode are as follows:

On Solaris OS, run the following command as user **nmsuser**. On SUSE Linux OS, run the following command as user **root**.

```
cd /opt/u2000/engineering
./startclient.sh storage -ip 127.0.0.1 -port 12212 -username admin -password admin
-InitDatabase
```

### NOTE

The default user name and password are both **admin**. If the password has been changed, enter the new password.

## Follow-up Procedure

The U2000 server will not automatically restart after all the preceding operations are completed. You need to start the U2000 server manually.

---

# E Shutting Down the U2000

---

This topic describes how to shut down the U2000 server and client. The shutdown procedure varies according to the deployment scheme.

## [E.1 Shutting Down the U2000 Client](#)

This topic describes how to shut down the U2000 client. You need to shut down the U2000 client before the U2000 server.

## [E.2 Shutting Down the Single-Server System \(Windows\)](#)

In any situation, you must follow the correct procedure for powering off the server as required, ensuring that the server is shut down in a secure manner.

## [E.3 Shutting Down the Single-Server System \(Solaris\)](#)

This topic describes how to shut down 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).

## [E.4 Shutting Down the Single-Server System \(SUSE Linux-Distributed\)](#)

This topic describes how to shut down the U2000 Single-Server System (SUSE Linux-Distributed).

## [E.5 Shutting Down the High Availability System \(Windows\)](#)

This topic describes how to shut down 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).

## [E.6 Shutting Down the High Availability System \(Solaris\)](#)

This topic describes how to shut down 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).

## [E.7 Shutting Down the High Availability System \(SUSE Linux-Distributed\)](#)

This topic describes how to shut down 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).

## E.1 Shutting Down the U2000 Client

This topic describes how to shut down the U2000 client. You need to shut down the U2000 client before the U2000 server.

### Prerequisite

The U2000 client must start normally.

### Procedure

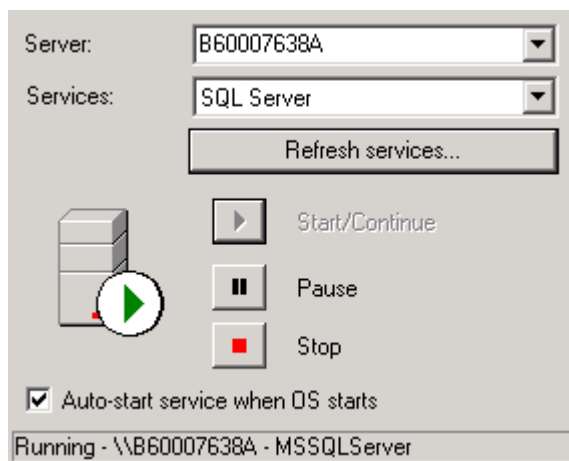
- 1 Choose **File > Exit** from the main menu.
- 2 In the **Confirm** dialog box, click **OK**.  
If certain operations on the system topology are performed but not saved, a prompt is displayed, asking you whether to save the operations.  
  
----End

## E.2 Shutting Down the Single-Server System (Windows)

In any situation, you must follow the correct procedure for powering off the server as required, ensuring that the server is shut down in a secure manner.

### Procedure

- 1 Exit all running U2000 clients.
- 2 Stop U2000 services and processes.
  1. Run the **stopserver.bat** file in the U2000 path, that is, **C:\HWENGR\engineering**, to end the U2000 MSuite processes.
  2. Run the **stopnms.bat** file in the U2000 path, for example, **D:\U2000\server\bin**, to end U2000 processes.
- 3 Stop the SQL Server database service.
  1. Choose **Start > Programs > Microsoft SQL Server > Service Manager**.
  2. In the dialog box shown in the following figure, click .



3. In the dialog box that is displayed, click **Yes**.
- 4 Shut down the Windows OS.

----End

## E.3 Shutting Down the Single-Server System (Solaris)

This topic describes how to shut down 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 Log in to the OS of the server as the **nmsuser** user.
- 3 Ensure that the U2000 is not running:

To check the running status of the U2000 process, run the following command:

```
$ daem_ps
```

Information similar to the following is displayed:

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

#### NOTE

The U2000 is running if the displayed information contains **imap\_sysmonitor -cmd start**.

Run the following commands to stop U2000 if it is running:

```
$ cd /opt/U2000/server/bin
$./stopnms.sh
```

#### 4 Ensure that the Sybase database is not running.

Run the following command to check whether the Sybase database is running:

```
$ ps -ef | grep sybase
```

Information similar to the following is displayed:

```
sybase 4848 4847 0 May 18 ? 167:11 /opt/sybase/ASE-15_0/bin/data
server -sDBSVR -d/opt/sybase/data/lv_master -e/opt
sybase 5250 5248 0 May 18 ? 0:00 /opt/sybase/ASE-15_0/bin/back
upserver -sDBSVR_back -e/opt/sybase/ASE-15_0/insta
sybase 4847 1 0 May 18 ? 0:00 /usr/bin/sh /opt/sybase/ASE-1
5_0/install/RUN_DBSVR
sybase 5248 1 0 May 18 ? 0:00 /usr/bin/sh /opt/sybase/ASE-1
5_0/install/RUN_DBSVR_back
...
```

#### NOTE

The database is running if the displayed information contains **/opt/sybase/ASE-15\_0/install/RUN\_DBSVR** and **/opt/sybase/ASE-15\_0/install/RUN\_DBSVR\_back**.

Run the following commands to stop the Sybase database if it is running:

```
$ su - sybase
$. /opt/sybase/SYBASE.sh
$ cd /opt/sybase/OCS-15_0/bin
$./isql -sDBSVR -Usa -Pchangeme
1> shutdown SYB_BACKUP
2> go
1> shutdown
2> go
$ exit
```

#### NOTE

- Leave a space between the dot (.) and the command **/opt/sybase/SYBASE.sh**.
- In the **./isql -sDBSVR -Usa -Pchangeme** command, *changeme* is the password of user **sa** of the Sybase database.

#### 5 Run the following commands to switch to user **root**:

```
$ su
password: password_of_root_user
```

#### 6 Run the following commands to shut down the OS:

```
sync;sync;sync;sync
shutdown -y -g0 -i5
```

----End

## E.4 Shutting Down the Single-Server System (SUSE Linux-Distributed)

This topic describes how to shut down the U2000 Single-Server System (SUSE Linux-Distributed).

## Context

Shutting down the Single-Server System (SUSE Linux-Distributed) includes stopping the U2000 server processes and database.

## Procedure

- 1 Exit all running U2000 clients.
- 2 Log in to the OS of the master server as the **root** user.
- 3 Run the following commands to stop the U2000:

```
cd /opt/U2000/server/bin
./stopnms.sh
```

- 4 Run the following commands to stop the Oracle process.

```
> su - oracle
> sqlplus / as sysdba
SQL> shutdown immediate
SQL> exit
> exit
```

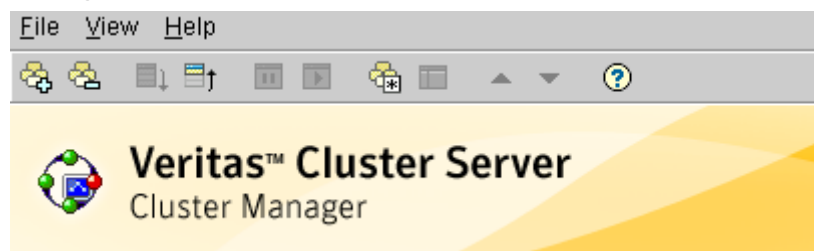
----End

## E.5 Shutting Down the High Availability System (Windows)

This topic describes how to shut down 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).

## Procedure

- 1 Exit all running U2000 clients.
- 2 On the primary site, do as follows to stop the U2000 processes:
  1. Choose **Start > Programs > Symantec > Veritas Cluster Server > Veritas Cluster Manager - Java Console** to start the VCS client.



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

3. Enter the IP address of the system of the primary site. Then, click **OK**.

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

Wait patiently. If all the resources on the **Resources** tab page turn grey, it indicates that the NMS processes are stopped.

- 3 Log in to the server of the active site and run the following commands to stop the VCS service:

```
C : \> hastop -all -force
```

In the Task Manager, check whether the **had.exe** process exists. If yes, right-click the process and stop it.

- 4 Log in to the server of the standby site and perform the preceding step to stop the VCS service on the server of the standby site.
- 5 Shut down the OS of the standby site.
  1. Choose **Start** > **Shut Down**.
  2. In the dialog box that is displayed, select **Shut Down**. Then, click **OK**.
- 6 Shut down the OS of the active site.
  1. Choose **Start** > **Shut Down**.
  2. In the dialog box that is displayed, select **Shut Down**. Then, click **OK**.

----End

## E.6 Shutting Down the High Availability System (Solaris)

This topic describes how to shut down 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).



## Procedure

- 1 Exit all running U2000 clients.

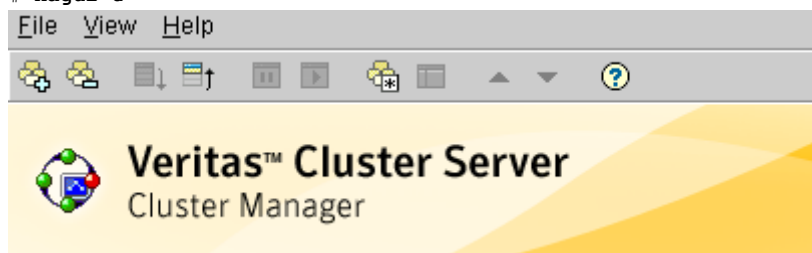
- 2 Stop the U2000 processes.

The U2000 processes consist of the U2000 server process and the Sybase process.

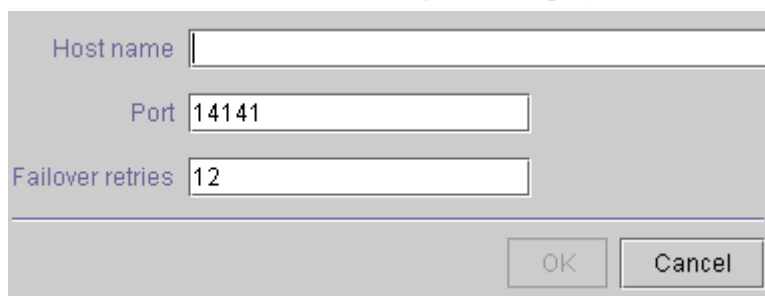
Check whether the U2000 processes are stopped and perform the following operations:

1. Access the **Java Desktop System, Release 3** session of the OS of the server of the active site as the **root** user.
2. Run the following command to start the VCS client:

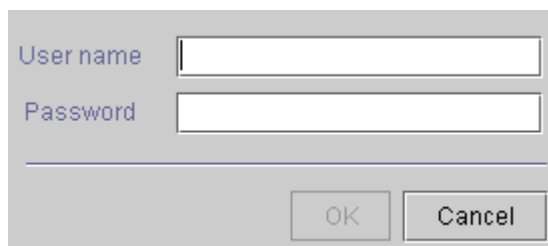
```
haguai &
```



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



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



5. Enter the default user name **admin** and the default password **password** of the VCS client. Then, click **OK**.
6. Select the **AppService** resource group from the navigation tree, click the **Status** tab, and then view the status of the U2000 processes.
  - If **Group Status on Member Systems** is displayed as **Offline**, it indicates that the U2000 processes are stopped.
  - If **Group Status on Member Systems** is displayed as **Online**, it indicates that the U2000 processes are started. Do as follows to stop the U2000 processes:  
Right-click **AppService** and choose **Offline > host\_name** from the shortcut menu.
- 3 Log in to the server of the active site as user **root** and run the following commands to stop the VCS service:

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

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

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

A message similar to the following will be displayed:

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

 **NOTE**

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

- 5 Log in to the server of the standby site as the **root** user and perform the preceding two steps to stop the VCS service on the server of the standby site.

- 6 Shut down the OS of the standby site.

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

```
sync;sync;sync;sync
shutdown -y -g0 -i5
```

- 7 Run the following command to shut down the OS of the active site:

```
sync;sync;sync;sync
shutdown -y -g0 -i5
```

----End

## E.7 Shutting Down the High Availability System (SUSE Linux-Distributed)

This topic describes how to shut down 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).

### 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:

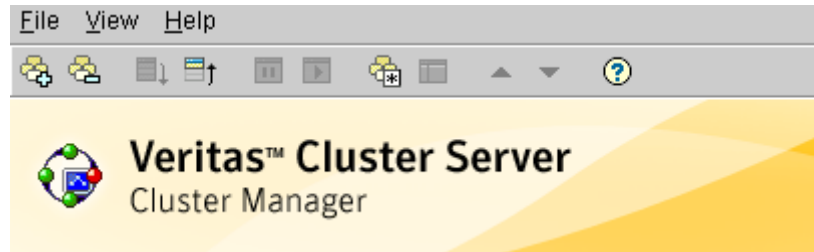
1. Access the **GNOME** session process of the OS of the master server of the active site as the **root** user.

 **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
hstop -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 U2000 Port List

---

This topic describes the service ports used by the U2000.

## [F.1 U2000 Service Port Overview](#)

This topic describes the U2000, service ports to be filtered and the method to query service ports.

## [F.2 Ports Between the U2000 Server and the NEs](#)

This topic describes the ports used between the U2000 server and the NEs.

## [F.3 Ports Between the U2000 Server and the Clients](#)

This topic describes the ports used between the U2000 server and the clients.

## [F.4 Ports Between the U2000 Server and the OSS](#)

This topic describes the ports used between the U2000 server and the operation support system (OSS).

## [F.5 Ports on Primary and Secondary Sites of the Veritas HA System](#)

This topic describes the ports required when the U2000 uses the Veritas HA system.

## [F.6 Ports for Internal Processes of the U2000 Server](#)

This topic describes the ports for internal processes of the U2000 server.

## [F.7 Ports for Remote Maintenance](#)

This topic describes the ports for remote maintenance.

## [F.8 Ports for Other Connections](#)

This topic describes the ports for communication between the U2000 server and other applications.

## F.1 U2000 Service Port Overview

This topic describes the U2000, service ports to be filtered and the method to query service ports.

### Overview of U2000 service ports

In the security policy of the firewall, you must filter the traffic according to the IP address and the Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) port number.

The TCP/UDP port number is used to split a datagram, and transfer the datagram to the proper applications.

The TCP/UDP port range is 0~65535, which is divided into three segments:

- 0~1023: Identifies some standard services, such as FTP, Telnet, and Trivial File Transfer Protocol (TFTP).
- 1024~49151: Assigned by Internet Assigned Number Authority (IANA) to the registered applications.
- 32768~65535: Private port numbers, which are dynamically assigned to any applications.

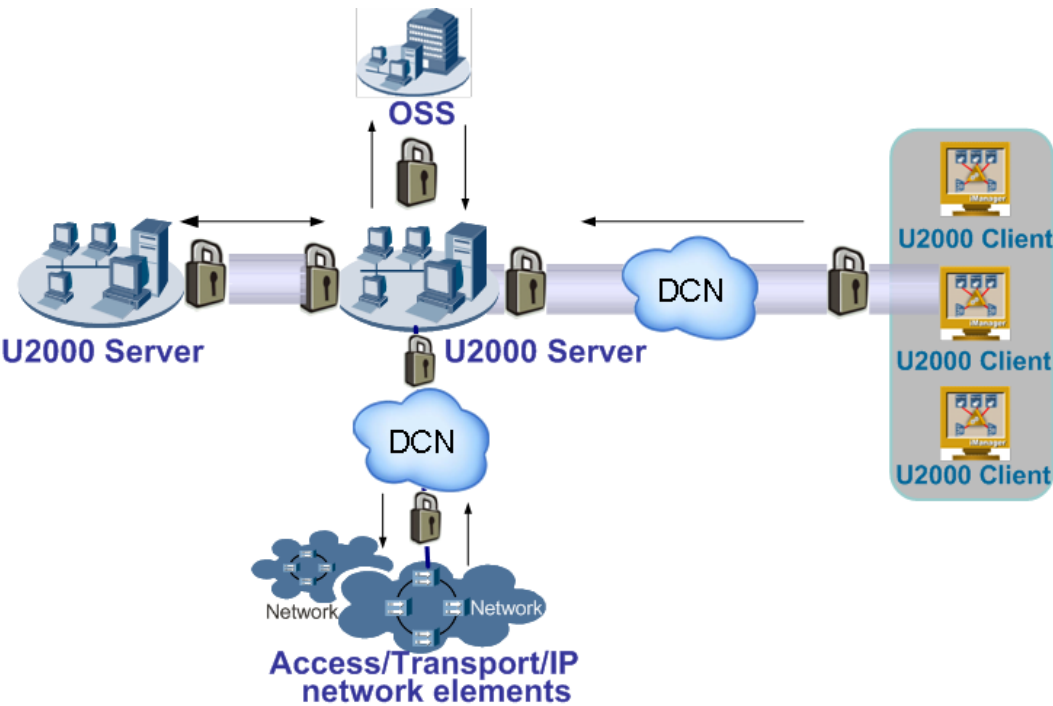
U2000 service ports are classified into the following types:

- Ports on the U2000 server for connecting the OSS
- Ports on the OSS for Connecting the U2000 Server
- Ports on the U2000 server for connecting clients
- Ports on the U2000 server for connecting NEs
- Ports on NEs for connecting the U2000 server
- Ports on primary and secondary sites of the Veritas HA system
- Ports for internal processes of the U2000 server
- Ports for other connections
- Ports for remote maintenance

### Diagram of U2000 service ports

The diagram of U2000 service ports shows the relationships between the U2000 server and peripherals, and the position and direction of firewalls.

Figure F-1 Relationship between the U2000 server and peripherals



Method to query service ports

The method to query service ports is as follows:

● Solaris OS

# `/usr/bin/netstat -an -P tcp`

Information similar to the following is displayed:

| TCP: IPv4     |                |       |        |        |        |        |  |
|---------------|----------------|-------|--------|--------|--------|--------|--|
| Local Address | Remote Address | Swind | Send-Q | Rwind  | Recv-Q | State  |  |
| -----         | -----          | ----- | -----  | -----  | -----  | -----  |  |
| *.*           | *.*            | 0     | 0      | 49152  | 0      | IDLE   |  |
| *.4145        | *.*            | 0     | 0      | 49152  | 0      | LISTEN |  |
| *.8989        | *.*            | 0     | 0      | 131760 | 0      | LISTEN |  |
| *.8199        | *.*            | 0     | 0      | 49152  | 0      | LISTEN |  |
| *.14150       | *.*            | 0     | 0      | 49152  | 0      | LISTEN |  |
| *.111         | *.*            | 0     | 0      | 49152  | 0      | LISTEN |  |
| ...           |                |       |        |        |        |        |  |

● Windows OS

# `netstat -ano`

Information similar to the following is displayed:

Active Connections

| Proto | Local Address     | Foreign Address | State     | PID  |
|-------|-------------------|-----------------|-----------|------|
| TCP   | 0.0.0.0:135       | 0.0.0.0:0       | LISTENING | 900  |
| TCP   | 0.0.0.0:371       | 0.0.0.0:0       | LISTENING | 1892 |
| TCP   | 0.0.0.0:445       | 0.0.0.0:0       | LISTENING | 4    |
| TCP   | 0.0.0.0:2401      | 0.0.0.0:0       | LISTENING | 2032 |
| TCP   | 0.0.0.0:2967      | 0.0.0.0:0       | LISTENING | 1284 |
| TCP   | 0.0.0.0:3389      | 0.0.0.0:0       | LISTENING | 852  |
| TCP   | 0.0.0.0:20100     | 0.0.0.0:0       | LISTENING | 2556 |
| TCP   | 10.112.38.168:139 | 0.0.0.0:0       | LISTENING | 4    |

```

TCP 10.112.38.168:1204 10.72.18.62:445 ESTABLISHED 4
TCP 10.112.38.168:1248 10.82.20.114:80 CLOSE_WAIT 2380
TCP 10.112.38.168:1320 10.72.112.73:1352 ESTABLISHED 3644
TCP 10.112.38.168:1333 10.82.20.135:80 CLOSE_WAIT 2380
TCP 10.112.38.168:1351 10.110.0.27:135 ESTABLISHED 648
...

```

- SUSE Linux OS

```
/bin/netstat -ant
```

Information similar to the following is displayed:

```

TCP: IPv4
 Local Address Remote Address Swind Send-Q Rwind Recv-Q State

 . *.* 0 0 49152 0 IDLE
 *.4145 *.* 0 0 49152 0 LISTEN
 *.8989 *.* 0 0 131760 0 LISTEN
 *.8199 *.* 0 0 49152 0 LISTEN
 *.14150 *.* 0 0 49152 0 LISTEN
 *.111 *.* 0 0 49152 0 LISTEN
 ...

```

## F.2 Ports Between the U2000 Server and the NEs

This topic describes the ports used between the U2000 server and the NEs.

While setting up a firewall between the U2000 server and the NEs, you must enable ports as follows:

- Any port on the U2000 server can connect to the ports listed in [Table F-1](#).
- Any port on the NEs can connect to the ports listed in [Table F-2](#).

**Table F-1** Ports on the NEs for connecting the U2000

| Source End   | Destination End | Protocol Type | Source Port | Destination Port | Description                                                                                |
|--------------|-----------------|---------------|-------------|------------------|--------------------------------------------------------------------------------------------|
| U2000 Server | NEs             | UDP           | Any port    | 161              | Port for NEs to receive SNMP requests. NEs and other processes send messages to this port. |



| Source End   | Destination End | Protocol Type | Source Port    | Destination Port | Description                                                                                                                                                          |
|--------------|-----------------|---------------|----------------|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| U2000 Server | NEs             | TCP           | Any port       | 21               | FTP-based port. The NE functions as the FTP server and the bulk collector periodically obtains PW performance files from NEs over the FTP protocol through this port |
| U2000 Server | NEs             | TCP           | Any port       | 1400             | Port for transport GNEs. This port is used for the NMS server to communicate with and manage NEs.                                                                    |
| U2000 Server | NEs             | UDP           | 35600 to 35654 | 1500             | Port for transport NEs. This port is used for the NMS server to communicate with NEs, and automatic discovery of equipment.                                          |
| U2000 Server | NEs             | TCP           | Any port       | 3081             | For the TL1 NE, port on the NE side whose ID is 3081. This port is used for the communication between the NMS and NEs.                                               |

| Source End   | Destination End | Protocol Type | Source Port | Destination Port | Description                                                                                                                                                         |
|--------------|-----------------|---------------|-------------|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| U2000 Server | NEs             | TCP           | Any port    | 5432             | Port on the NE side whose ID is 5432. This port is used for the communication between the NMS and NEs.                                                              |
| U2000 Server | NEs             | TCP           | Any port    | 23               | Telnet protocol port which network management processes use to configure and synchronize the resources                                                              |
| U2000 Server | NEs             | UDP           | Any port    | 68               | Port for the PnPMgrDM process. This is the destination port for DHCP responses. NEs listen to this port. The PnP process sends DHCP responses to such ports of NEs. |
| U2000 Server | NEs             | TCP           | Any port    | 22               | NetConf protocol port. This port is used for the interaction between the U2000 and NEs.                                                                             |

**Table F-2** Ports on the U2000server for connecting NEs

| Source End | Destination End | Protocol Type | Source Port | Destination Port | Description                                                                                                                                                                                                                |
|------------|-----------------|---------------|-------------|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NEs        | U2000 Server    | TCP           | Any port    | 21               | FTP-based port. The NMS functions as the FTP server and NEs periodically upload performance files to the NMS server through this port                                                                                      |
| NEs        | U2000 Server    | TCP           | Any port    | 21               | Port for the FTP server process to provide file transfer services. Some NEs of the access, datacom, and transport domains that are managed by the data center (DC) rely on FTP services to back up data and load software. |

| Source End | Destination End | Protocol Type | Source Port | Destination Port | Description                                                                                                                                                                                                                     |
|------------|-----------------|---------------|-------------|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NEs        | U2000 Server    | TCP           | Any port    | 22               | Port for the SFTP server process. This port is used for SFTP services. Some NEs of the access, datacom, and transport domains that are managed by the data center (DC) rely on SFTP services to back up data and load software. |
| NEs        | U2000 Server    | TCP           | Any port    | 69               | Port for the TFTP server process. This port is used for TFTP services. The DC uses TFTP services to back up data for and load software on NEs in the access domain.                                                             |
| NEs        | U2000 Server    | UDP           | Any port    | 4999             | Port for the secdevregdm process. This port is used for security NEs to proactively register with the NMS server.                                                                                                               |

| Source End | Destination End | Protocol Type | Source Port | Destination Port | Description                                                                                                                                                                                                                                                            |
|------------|-----------------|---------------|-------------|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NEs        | U2000 Server    | UDP           | Any port    | 13005            | Port for the UniteUtilDM process. This port is used for automatic discovery of PTN NEs. NEs regularly send NE data in UDP packets through this port to the NMS.                                                                                                        |
| NEs        | U2000 Server    | UDP           | Any port    | 514              | Port for the SyslogCollectorDM process. This is a general Syslog port. This port is used for the OSS to receive operation logs and running logs from NEs. Operation logs and running logs are sent in UDP packets through this port after NEs are properly configured. |
| NEs        | U2000 Server    | UDP           | Any port    | 162              | Port for the trapdispatcher process. It is used by the NMS to receive alarms and events of NEs by means of SNMP trap packets.                                                                                                                                          |

| Source End | Destination End | Protocol Type | Source Port | Destination Port | Description                                                                                                                                                                  |
|------------|-----------------|---------------|-------------|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NEs        | U2000 Server    | UDP           | Any port    | 67               | Port for the PnpMgrDM process. This is the destination port for DHCP requests. The plug and play (PnP) process listens to this port and receives the DHCP requests from NEs. |
| NEs        | U2000 Server    | TCP           | Any port    | 13029            | Port for the U2560TR069 Dm process. The NMS server communicates with TR069-compliant access NEs through this port in HTTP mode by using the TR069 protocol stack.            |
| NEs        | U2000 Server    | TCP           | Any port    | 13030            | Port for the U2560TR069 Dm process. The NMS server communicates with TR069-compliant access NEs through this port in HTTPS mode by using the TR069 protocol stack.           |

| Source End | Destination End | Protocol Type | Source Port | Destination Port | Description                                                                                                                                   |
|------------|-----------------|---------------|-------------|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| NEs        | U2000 Server    | TCP           | Any port    | 13033            | Port for the U2560TR069 Dm process. The NMS server communicates with TR069-compliant access NEs through this TR069 protocol stack-based port. |

## F.3 Ports Between the U2000 Server and the Clients

This topic describes the ports used between the U2000 server and the clients.

While setting up a firewall between the U2000 server and the clients, you must enable the ports on the U2000 server. Any port on the U2000 server can connect to the ports listed in [Table F-3](#).

**Table F-3** Ports on the U2000 server for connecting the clients

| Source End    | Destination End | Protocol Type | Source Port | Destination Port | Description                                                        |
|---------------|-----------------|---------------|-------------|------------------|--------------------------------------------------------------------|
| U2000 Clients | U2000 Server    | TCP           | Any port    | 12200            | Port used to perform operations on the QuickStep in command lines. |
| U2000 Clients | U2000 Server    | TCP           | Any port    | 12201            | Port used by the QuickStep client to send HTTP requests.           |

| Source End    | Destination End | Protocol Type | Source Port | Destination Port | Description                                                                                                                                                                                                                    |
|---------------|-----------------|---------------|-------------|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| U2000 Clients | U2000 Server    | TCP           | Any port    | 12204            | Port for the Quickstep commissioning. It is recommended that this port is enabled for only the maintenance of the server.                                                                                                      |
| U2000 Clients | U2000 Server    | TCP           | Any port    | 13006            | SSL-based port for the toolkit process on the server and this port is open to Toolkit clients. The Toolkit is an upgrade tool for board-level NEs in the transport domain, which is part of the NE Software Management System. |
| U2000 Clients | U2000 Server    | TCP           | Any port    | 21               | General port for FTP services for NE software management. FTP files (such as NE software packages and NE configuration files) can be delivered between the NMS server and clients through this port.                           |



| Source End    | Destination End | Protocol Type | Source Port | Destination Port | Description                                                                                                                                                                                                                                                      |
|---------------|-----------------|---------------|-------------|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| U2000 Clients | U2000 Server    | TCP           | Any port    | 22               | Port for the SFTP server process. The NMS client and server transfer files to each other through this port. The DC uses the SFTP service to configure data on NEs and transfer NE software between clients and the server of the NMS.                            |
| U2000 Clients | U2000 Server    | TCP           | Any port    | 8999             | Port for the toolkit process on the server. This port can be used by the Toolkit client. This port is based on the SSL protocol. The Toolkit is an upgrade tool for board-level NEs in the transport domain, which is part of the NE Software Management System. |
| U2000 Clients | U2000 Server    | TCP           | Any port    | 443              | Port for the xmlagent process in SSL mode. This port is used for the NMS to listen to HTTPs requests from the OSS.                                                                                                                                               |

| Source End    | Destination End | Protocol Type | Source Port | Destination Port | Description                                                                                                                                                              |
|---------------|-----------------|---------------|-------------|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| U2000 Clients | U2000 Server    | TCP           | Any port    | 11080            | Web service port for the standalone Web LCT.                                                                                                                             |
| U2000 Clients | U2000 Server    | TCP           | Any port    | 13003            | Port for the gcli process. This port is an HTTP-based port. Service processes of the intelligent configuration tool listen to this port and receive operation requests.  |
| U2000 Clients | U2000 Server    | TCP           | Any port    | 13004            | Port for the gcli process. This port is an HTTPS-based port. Service processes of the intelligent configuration tool listen to this port and receive operation requests. |
| U2000 Clients | U2000 Server    | TCP           | Any port    | 12212            | Port for the msserver process. This port is used to for MSuite clients to communicate with the MSuite server.                                                            |

| Source End    | Destination End | Protocol Type | Source Port | Destination Port | Description                                                                                                                           |
|---------------|-----------------|---------------|-------------|------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| U2000 Clients | U2000 Server    | TCP           | Any port    | 12213            | Port for the msserver process in SSL mode. This port is used to for MSuite clients to communicate with the MSuite server.             |
| U2000 Clients | U2000 Server    | TCP           | Any port    | 12214            | Port for the msserver process. This port is used for file transfer between the MSuite server and clients.                             |
| U2000 Clients | U2000 Server    | TCP           | Any port    | 12215            | Port for the msserver process in SSL mode. This port is used to for MSuite clients to communicate with the MSuite server.             |
| U2000 Clients | U2000 Server    | TCP           | Any port    | 14150            | Port for the VCS Command process on the Veritas HA system. This port is used for the NMS server to issue VCS commands to NMS clients. |

| Source End    | Destination End | Protocol Type | Source Port | Destination Port | Description                                                                                                                                                                                   |
|---------------|-----------------|---------------|-------------|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| U2000 Clients | U2000 Server    | TCP           | Any port    | 8080             | Universal port for the HTTP service. This port is provided by the NMS server for clients to use HTTP services. This port is used by client auto update (CAU), HedEx online help, and Web LCT. |
| U2000 Clients | U2000 Server    | TCP           | Any port    | 8181             | Port for VCS Web service in a Veritas-based HA system. By default, the NMS server does not use the VCS web service.                                                                           |
| U2000 Clients | U2000 Server    | TCP           | Any port    | 8443             | Service port provided by the NMS server for clients to use HTTPS services. This port is used for the online help and Web LCT.                                                                 |

| Source End    | Destination End | Protocol Type | Source Port | Destination Port | Description                                                                                                                                    |
|---------------|-----------------|---------------|-------------|------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| U2000 Clients | U2000 Server    | TCP           | Any port    | 12216            | Web proxy port for managing the SRG equipment. This port is used by processes of the server to manage the SRG equipment by means of Web proxy. |
| U2000 Clients | U2000 Server    | TCP           | Any port    | 31030            | Port for the imapmrb process. The MDP process sends messages through this port.                                                                |
| U2000 Clients | U2000 Server    | TCP           | Any port    | 31032            | Port for the EventService process. This port is used when events are sent.                                                                     |
| U2000 Clients | U2000 Server    | TCP           | Any port    | 31035            | Port for the porttrunk_agent process. This port is used for the porttunk process.                                                              |
| U2000 Clients | U2000 Server    | TCP           | Any port    | 31037            | Port for the DesktopService process. Java clients communicate with the server through this port.                                               |

| Source End    | Destination End | Protocol Type | Source Port | Destination Port | Description                                                                                                       |
|---------------|-----------------|---------------|-------------|------------------|-------------------------------------------------------------------------------------------------------------------|
| U2000 Clients | U2000 Server    | TCP           | Any port    | 31038            | Port for the DesktopService process. A Web client connects with the server through this port.                     |
| U2000 Clients | U2000 Server    | TCP           | Any port    | 31039            | Port for the DesktopService process (in SSL mode). Java clients communicate with the server through this port.    |
| U2000 Clients | U2000 Server    | TCP           | Any port    | 31040            | Port for the DesktopService0101 process (in HTTPS mode). A Web client connects with the server through this port. |
| U2000 Clients | U2000 Server    | TCP           | Any port    | 31041 to 31050   | process. When multiple instances are deployed for the DesktopService, port IDs range from 31041 to 31050.         |
| U2000 Clients | U2000 Server    | TCP           | Any port    | 31080            | Port for the imapmrb process (in SSL mode). This port is used when the MDP process sends messages.                |

| Source End    | Destination End | Protocol Type | Source Port | Destination Port | Description                                                                                              |
|---------------|-----------------|---------------|-------------|------------------|----------------------------------------------------------------------------------------------------------|
| U2000 Clients | U2000 Server    | TCP           | Any port    | 31082            | Port for the EventService process (in SSL mode). This port is used for sending events.                   |
| U2000 Clients | U2000 Server    | TCP           | Any port    | 13001            | Port for the Nemgr_vmf process. This port is used for the interaction between the client and the server. |

## F.4 Ports Between the U2000 Server and the OSS

This topic describes the ports used between the U2000 server and the operation support system (OSS).

While setting up a firewall between the U2000 server and the OSS, make sure that any port on the U2000 server can connect to the ports listed in [Table F-4](#).

**Table F-4** Ports on the U2000 server for connecting the OSS

| Source End | Destination End | Protocol Type | Source Port | Destination Port | Description                                                                                                                                |
|------------|-----------------|---------------|-------------|------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| OSS        | U2000 Server    | TCP           | Any port    | 21               | FTP protocol port. The performance text NBI process transfers performance files to the OSS through this port by means of the FTP protocol. |

| Source End | Destination End | Protocol Type | Source Port | Destination Port | Description                                                                                                                                                                                                |
|------------|-----------------|---------------|-------------|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| OSS        | U2000 Server    | TCP           | Any port    | 12001            | Port for the Naming_Service process in non-SSL mode. The Naming_Service process, an ACE/TAO-based open-source naming service process of the CORBA NBI, is used to register CORBA service objects.          |
| OSS        | U2000 Server    | TCP           | Any port    | 12002            | Port for the itnotify process in non-SSL mode. The Notify_Service process, an ACE/TAO-based open-source notification service of the CORBA NBI, is used to forward events to the OSS through the CORBA NBI. |



| Source End | Destination End | Protocol Type | Source Port | Destination Port | Description                                                                                                                                                                                   |
|------------|-----------------|---------------|-------------|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| OSS        | U2000 Server    | TCP           | Any port    | 12002            | Port for the itnotify process. The itnotify is a notify process developed by Progress Software. This port is used for the NMS to forward CORBA events to the OSS.                             |
| OSS        | U2000 Server    | TCP           | Any port    | 12003            | Port for the Agent_CORBA process. This port is used for the NMS to listen to CORBA requests from the OSS through the CORBA NBI.                                                               |
| OSS        | U2000 Server    | TCP           | Any port    | 22001            | Port for the Naming_Service process in SSL mode. The Naming_Service process, an ACE/TAO-based open-source naming service process of the CORBA NBI, is used to register CORBA service objects. |

| Source End | Destination End | Protocol Type | Source Port | Destination Port | Description                                                                                                                                                                                    |
|------------|-----------------|---------------|-------------|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| OSS        | U2000 Server    | TCP           | Any port    | 22002            | Port for the Notify_Service in SSL mode. The Notify_Service process, an ACE/TAO open-source notification service of the CORBA NBI, is used to forward events to the OSS through the CORBA NBI. |
| OSS        | U2000 Server    | TCP           | Any port    | 22002            | Port for the itnotify process in SSL mode. The itnotify is a notify process developed by Progress Software. This port is used for the NMS to forward CORBA events to the OSS.                  |
| OSS        | U2000 Server    | TCP           | Any port    | 22003            | Port for the Agent_CROBA process in SSL mode. This port is used for the NMS to listen to CORBA requests from the OSS through the CORBA NBI.                                                    |

| Source End | Destination End | Protocol Type | Source Port | Destination Port | Description                                                                                                                              |
|------------|-----------------|---------------|-------------|------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| OSS        | U2000 Server    | TCP           | Any port    | 61616            | Port for the JMSServer process (service port in non-SSL mode). This port is used by the JMS message server to interconnect with the OSS. |
| OSS        | U2000 Server    | TCP           | Any port    | 61617            | Port for the JMSServer process (service port in SSL mode). This port is used by the JMS server to interconnect with the OSS.             |
| OSS        | U2000 Server    | TCP           | Any port    | 8161             | Port for the JMSServer process. This port is used for monitoring and maintenance.                                                        |
| OSS        | U2000 Server    | UDP           | Any port    | 9812             | Port for the snmp_agent process. This is an SNMP listening port for the NMS to receive requests from the OSS.                            |
| OSS        | U2000 Server    | TCP           | Any port    | 9997             | Port for the xmlagent process in SSL mode. This port is used for the NMS to listen to HTTP requests from the OSS.                        |

| Source End | Destination End | Protocol Type | Source Port | Destination Port | Description                                                                                                                                                 |
|------------|-----------------|---------------|-------------|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| OSS        | U2000 Server    | TCP           | Any port    | 15000            | Port for the Eml_mml process. This port is used for the NMS to communicate with the OSS through the MML interface.                                          |
| OSS        | U2000 Server    | TCP           | Any port    | 15001            | Port for the Eml_mml process in SSL mode. This port is used for the NMS server to communicate with the OSS through the MML interface.                       |
| OSS        | U2000 Server    | TCP           | Any port    | 10501            | Port for the iNBXMLSoap Agent process. This port interconnects with the XML1.1 NBI and is used to provision services for access NEs through the XML1.1 NBI. |
| OSS        | U2000 Server    | TCP           | Any port    | 8001             | Port for the CFMSiDm process. This port is used to dynamically adjust the process commissioning switch.                                                     |

| Source End | Destination End | Protocol Type | Source Port | Destination Port | Description                                                                                                                   |
|------------|-----------------|---------------|-------------|------------------|-------------------------------------------------------------------------------------------------------------------------------|
| OSS        | U2000 Server    | TCP           | Any port    | 9000             | Port for the cltsi process. This port interconnects with NBIs and is used to conduct narrowband line tests on access NEs.     |
| OSS        | U2000 Server    | TCP           | Any port    | 9001             | Port for the CFMSiDm process. This port interconnects with the CFMSi NBI and is used to set telephone numbers for access NEs. |

**Table F-5** lists the ports on the OSS for connecting the U2000 server.

**Table F-5** Ports on the OSS for connecting the U2000 server

| Source End   | Destination End | Protocol Type | Source Port | Destination Port | Description                                                                                      |
|--------------|-----------------|---------------|-------------|------------------|--------------------------------------------------------------------------------------------------|
| U2000 Server | OSS             | TCP           | Any port    | 982              | Port for the snmp_agent process. It is an SNMP forwarding port for the delivery of trap packets. |

## F.5 Ports on Primary and Secondary Sites of the Veritas HA System

This topic describes the ports required when the U2000 uses the Veritas HA system.

When the U2000 uses the Veritas HA system, you need to configure the ports required by the Veritas HA system. See **Table F-6**.

 **NOTE**

When configuring the firewall between the primary and secondary sites, you need to set only the protocol type, source IP address, and destination IP address, but not the source port and destination port.

**Table F-6** Veritas on primary and secondary sites of the HA system ports

| Source End   | Destination End | Protocol Type | Source Port | Destination Port | Description                                                                                                                                                                                                                                                 |
|--------------|-----------------|---------------|-------------|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| U2000 Server | U2000 Server    | TCP           | Any port    | 12212            | Port for the msserver process. This port is used for MSuite clients to communicate with the MSuite server. On the high availability (HA) system, this port is used for servers at the primary site to notify the secondary site for cooperative deployment. |
| U2000 Server | U2000 Server    | TCP           | Any port    | 12213            | Port for the msserver process. This port is used for MSuite clients to communicate with the MSuite server. On the HA system, this port is used for the primary site to notify the secondary site for cooperative deployment.                                |

| Source End   | Destination End | Protocol Type | Source Port | Destination Port | Description                                                                                                                                                                                                           |
|--------------|-----------------|---------------|-------------|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| U2000 Server | U2000 Server    | TCP           | Any port    | 12214            | Port for the msserver process. This port is used to for MSuite clients to communicate with the MSuite server. On the HA system, this port is used for file transfer between the primary and secondary.                |
| U2000 Server | U2000 Server    | TCP           | Any port    | 12215            | Port for the msserver process in SSL mode. This port is used for MSuite clients to communicate with the MSuite server. On the HA system, this port is used for file transfer between the primary and secondary sites. |

| Source End   | Destination End | Protocol Type | Source Port | Destination Port | Description                                                                                                                                                                              |
|--------------|-----------------|---------------|-------------|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| U2000 Server | U2000 Server    | TCP           | Any port    | 14145            | Port for the VCS global cluster on the Veritas HA system. This port is used for the WAC (Wide-Area connector) process on the local cluster to listen to connection from remote clusters. |
| U2000 Server | U2000 Server    | TCP           | Any port    | 14155            | Port for the GCO WAC process on the Veritas HA system. This port is used for the WAC (Wide-Area connector) process on the local cluster to listen to connection from remote clusters.    |
| U2000 Server | U2000 Server    | TCP,UDP       | Any port    | 4145             | Port for Veritas volume replicator (VVR) heartbeat communication between the active and standby servers. This port listens to the transport layer of the system.                         |



| Source End   | Destination End | Protocol Type | Source Port | Destination Port | Description                                                                                                                                                           |
|--------------|-----------------|---------------|-------------|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| U2000 Server | U2000 Server    | TCP           | Any port    | 8199             | Port for the vradmind process of the VVR in a Veritas-based HA system. The active and standby servers communicate by means of the vradmind process through this port. |
| U2000 Server | U2000 Server    | TCP           | Any port    | 8989             | Port for the in.vxrsyncd process of the VVR in a Veritas HA system. The active and standby servers communicate by means of the vradmind process through this port.    |

## F.6 Ports for Internal Processes of the U2000 Server

This topic describes the ports for internal processes of the U2000 server.

The ports for internal processes of the U2000 server are used only for communication between internal processes of the U2000, but not external communication. You can view these ports by using the port scanning tool and do not need to configure them on firewalls.

U2000 internal processes of the server listed in [Table F-7](#).

**Table F-7** Ports for internal processes of the U2000 server

| Source End   | Destination End | Protocol Type | Source Port | Destination Port | Description                                                                                                                                                |
|--------------|-----------------|---------------|-------------|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| U2000 Server | U2000 Server    | TCP           | Any port    | 12202            | Port used by the Quickstep Tomcat to send shutdown requests.                                                                                               |
| U2000 Server | U2000 Server    | TCP           | Any port    | 12203            | Port used by the Quickstep tomcat AJP.                                                                                                                     |
| U2000 Server | U2000 Server    | TCP           | Any port    | 11000 to 11100   | Port for transport NE management processes. This port is used for communication between NEs and the Web LCT and ASON management process.                   |
| U2000 Server | U2000 Server    | TCP           | Any port    | 135              | RPC port for the Windows OS. This port contains the endpoint mapper and other RPC services. Most services of the Windows-based sever depends on this port. |

| Source End   | Destination End | Protocol Type | Source Port | Destination Port | Description                                                                                                                                                                                      |
|--------------|-----------------|---------------|-------------|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| U2000 Server | U2000 Server    | TCP           | Any port    | 14141            | Port for the VCS process on the Veritas HA system. This port is used for connection between the VCS server and clients. The VCS clients can be deployed either on the NMS server or on other PC. |
| U2000 Server | U2000 Server    | TCP           | Any port    | 14144            | Port for the VCS process on the Veritas HA system. This is a VCS Notifier listening port. This port is used for the NMS to listen to the VCS server.                                             |
| U2000 Server | U2000 Server    | TCP           | Any port    | 1433             | Service port of the Microsoft SQL Server for connecting a remote database.                                                                                                                       |
| U2000 Server | U2000 Server    | UDP           | Any port    | 1434             | Service port of the Microsoft SQL Monitor for monitoring a database.                                                                                                                             |
| U2000 Server | U2000 Server    | TCP           | Any port    | 1521             | Service port of the Oracle database.                                                                                                                                                             |

| Source End   | Destination End | Protocol Type | Source Port | Destination Port | Description                                                                                                                                              |
|--------------|-----------------|---------------|-------------|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| U2000 Server | U2000 Server    | TCP           | Any port    | 2994             | Port for internal database management. This port is blocked by the firewall.                                                                             |
| U2000 Server | U2000 Server    | TCP,UDP       | Any port    | 4045             | Port for network file system (NFS) services of SUSE Linux. In a distributed system, the active and standby servers share files by using the NFS service. |
| U2000 Server | U2000 Server    | TCP           | Any port    | 4100             | Service port for Sybase database.                                                                                                                        |
| U2000 Server | U2000 Server    | TCP           | Any port    | 4200             | Service port for backing up the Sybase database.                                                                                                         |
| U2000 Server | U2000 Server    | TCP           | Any port    | 587              | SMTP service port provided by the OS. This port is not used by the NMS server.                                                                           |
| U2000 Server | U2000 Server    | TCP           | Any port    | 9819             | Port for the TL1NBI process. This port interconnects with the TL1 NBI and is used to provision services for access NEs through the TL1 NBI.              |

| Source End   | Destination End | Protocol Type | Source Port | Destination Port | Description                                                                                                            |
|--------------|-----------------|---------------|-------------|------------------|------------------------------------------------------------------------------------------------------------------------|
| U2000 Server | U2000 Server    | TCP           | Any port    | 11101 to 11104   | TCP port for forwarding traps internally. Traps are forwarded to NEs through this port.                                |
| U2000 Server | U2000 Server    | TCP           | Any port    | 31000            | Port for the imapsysd process. It is used to call the CORBA NBI of the sysd.                                           |
| U2000 Server | U2000 Server    | TCP           | Any port    | 31001            | Port for the lic_agent process. It is used to call the CORBA NBI of the lic.                                           |
| U2000 Server | U2000 Server    | TCP           | Any port    | 31005            | Port for the log_agent process. This port is used when the CORBA NBI of the log is called.                             |
| U2000 Server | U2000 Server    | TCP           | Any port    | 31006            | Port for listening to logs. This port is used when services call the log of the log_client.                            |
| U2000 Server | U2000 Server    | TCP           | Any port    | 31007            | Port for the SettingService process. This port is used when services call the setting_client to obtain configurations. |

| Source End   | Destination End | Protocol Type | Source Port | Destination Port | Description                                                                                        |
|--------------|-----------------|---------------|-------------|------------------|----------------------------------------------------------------------------------------------------|
| U2000 Server | U2000 Server    | TCP           | Any port    | 31008            | Port for the sm_agent process. This port is used when the corba NBI of the sm is called.           |
| U2000 Server | U2000 Server    | TCP           | Any port    | 31010            | Port for the tm_agent process. This port is used when the CORBA NBI of the tm is called.           |
| U2000 Server | U2000 Server    | TCP           | Any port    | 31011            | Port for the ifms_agent process. This port is used when the CORBA NBI of the fm is called.         |
| U2000 Server | U2000 Server    | TCP           | Any port    | 31013            | Port for the manager_agent process. This port is used when the CORBA NBI of the manager is called. |
| U2000 Server | U2000 Server    | TCP           | Any port    | 31015            | Port for the itm_agent process. This port is used when the CORBA NBI of the itm is called.         |

| Source End   | Destination End | Protocol Type | Source Port | Destination Port | Description                                                                                              |
|--------------|-----------------|---------------|-------------|------------------|----------------------------------------------------------------------------------------------------------|
| U2000 Server | U2000 Server    | TCP           | Any port    | 31033            | Port for the lte_agent process. This port is used when the CORBA NBI of the lte is called.               |
| U2000 Server | U2000 Server    | TCP           | Any port    | 31036            | Port for the eam_agent process. This port is used when the CORBA NBI of the eam is called.               |
| U2000 Server | U2000 Server    | TCP           | Any port    | 31050            | Port for the imapsysd process (in SSL mode). This port is used when the CORBA NBI of the sysd is called. |
| U2000 Server | U2000 Server    | TCP           | Any port    | 31051            | Port for the lic_agent process (in SSL mode). This port is used when the CORBA NBI of the lic is called. |
| U2000 Server | U2000 Server    | TCP           | Any port    | 31055            | Port for the log_agent process (in SSL mode). This port is used when the CORBA NBI of the log is called. |

| Source End   | Destination End | Protocol Type | Source Port | Destination Port | Description                                                                                                                          |
|--------------|-----------------|---------------|-------------|------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| U2000 Server | U2000 Server    | TCP           | Any port    | 31057            | Port for the SettingService process (in SSL mode). This port is used when services call the setting_client to obtain configurations. |
| U2000 Server | U2000 Server    | TCP           | Any port    | 31058            | Port for the sm_agent process (SSL). This port is used when the CORBA NBI of the sm is called.                                       |
| U2000 Server | U2000 Server    | TCP           | Any port    | 31060            | Port for the tm_agent process. This port is used when the CORBA NBI of the tm is called.                                             |
| U2000 Server | U2000 Server    | TCP           | Any port    | 31061            | Port for the ifms_agent process (SSL). This port is used when the CORBA NBI of the fm is called.                                     |
| U2000 Server | U2000 Server    | TCP           | Any port    | 31063            | Port for the manager_agent process (in SSL mode). This port is used for calling the CORBA NBI of the manager.                        |



| Source End   | Destination End | Protocol Type | Source Port | Destination Port | Description                                                                                                                                         |
|--------------|-----------------|---------------|-------------|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| U2000 Server | U2000 Server    | TCP           | Any port    | 31065            | Port for the itm_agent process (SSL). This port is used when the CORBA NBI of the itm is called.                                                    |
| U2000 Server | U2000 Server    | TCP           | Any port    | 31083            | Port for the lte_agent process (in SSL mode). This port is used when the CORBA NBI of the lte is called.                                            |
| U2000 Server | U2000 Server    | TCP           | Any port    | 31099            | Port for the eam_agent process (in SSL mode). This port is used when the CORBA NBI of the eam is called.                                            |
| U2000 Server | U2000 Server    | TCP           | Any port    | 8250             | Port listened to by the CAU. This port is used by the Cau service part of the Tomcat to partly check whether Cau services are available at present. |

## F.7 Ports for Remote Maintenance

This topic describes the ports for remote maintenance.

**Table F-8** lists the ports for remote maintenance.

**Table F-8** Ports for remote maintenance

| Source End | Destination End | Protocol Type | Source Port | Destination Port | Description                                                                                                                                                                                                                             |
|------------|-----------------|---------------|-------------|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Any port   | U2000 Server    | UDP           | Any port    | 177              | Standard XDMCP-based service port for Solaris and SUSE Linux OSs. X terminals, such as the XManager, operate Solaris and Linux OSs remotely through this port. It is recommended that you enable this port only for server maintenance. |
| Any port   | U2000 Server    | TCP           | Any port    | 2148             | Port for the VXSVC server on the Veritas-based HA system. Port for a customer Veritas Enterprise Administrator (VEA) client to connect to the VXSVC server to view and configure volumes.                                               |
| Any port   | U2000 Server    | TCP           | Any port    | 23               | Standard Telnet-based service port. It is recommended that you enable this port only for server maintenance.                                                                                                                            |

| Source End | Destination End | Protocol Type | Source Port | Destination Port | Description                                                                                                                                                                                    |
|------------|-----------------|---------------|-------------|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Any port   | U2000 Server    | TCP           | Any port    | 3389             | Port for Windows to provide remote desktop services over the Remote Desktop Protocol (RDP).                                                                                                    |
| Any port   | U2000 Server    | TCP           | Any port    | 445              | Port for sharing services on Window OS. It is recommended that this you enable this port only for server maintenance.                                                                          |
| Any port   | U2000 Server    | TCP           | Any port    | 6112             | Port for the Solaris OS. This port is applicable to the CDE Subprocess Controls Server daemon (dtspcd). Through this port, you can log in to the Solaris-based server remotely from a CDE GUI. |
| Any port   | U2000 Server    | TCP           | Any port    | 7100             | Port for X Font services of Solaris. It is recommended that you enable this port only for server maintenance.                                                                                  |

| Source End | Destination End | Protocol Type | Source Port | Destination Port | Description                                                                                                |
|------------|-----------------|---------------|-------------|------------------|------------------------------------------------------------------------------------------------------------|
| Any port   | U2000 Server    | TCP           | Any port    | 8005             | Service port provided by the Tomcat for disabling Tomcat services.                                         |
| Any port   | U2000 Server    | TCP           | Any port    | 9003             | Port for the StdCltsiDm process. This port is used to dynamically adjust the process commissioning switch. |

## F.8 Ports for Other Connections

This topic describes the ports for communication between the U2000 server and other applications.

**Table F-9** lists the ports for communication between the U2000 server and other applications.

**Table F-9** Ports for other connections

| Source End | Destination End | Protocol Type | Source Port | Destination Port | Description                                                                                                                          |
|------------|-----------------|---------------|-------------|------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| Any port   | U2000 Server    | TCP,UDP       | Any port    | 111              | RPC port for the Solaris-based server. This port is used to provide services such as NFS service. This port is not used for the NMS. |

| Source End | Destination End | Protocol Type | Source Port | Destination Port | Description                                                                                                                                                            |
|------------|-----------------|---------------|-------------|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Any port   | U2000 Server    | UDP           | Any port    | 123              | General port for the NTP process. This port is used for time synchronization in a network. The NMS server that does not run on Windows can function as the NTP server. |
| Any port   | U2000 Server    | TCP           | Any port    | 513              | Port for Rlogin services of Solaris. This port is not used by the NMS server.                                                                                          |
| Any port   | U2000 Server    | TCP           | Any port    | 6481             | Port for Tag services of Solaris. This port is not used by the NMS server.                                                                                             |
| Any port   | U2000 Server    | TCP           | Any port    | 8009             | Port provided by the Tomcat for AJP services. This port is not used by the NMS.                                                                                        |



---

# G Abbreviations

---

|               |                                            |
|---------------|--------------------------------------------|
| <b>ACL</b>    | Access Control List                        |
| <b>ADSL</b>   | Asymmetrical Digital Subscriber Line       |
| <b>C</b>      |                                            |
| <b>CD-ROM</b> | Compact Disc-Read Only Memory              |
| <b>D</b>      |                                            |
| <b>DC</b>     | Data Center                                |
| <b>DCM</b>    | Digital Communication Multiplex            |
| <b>DSL</b>    | Digital Subscriber Line                    |
| <b>DSLAM</b>  | Digital Subscriber Line Access Multiplexer |
| <b>DSN</b>    | Data Source Name                           |
| <b>E</b>      |                                            |
| <b>ESD</b>    | electrostatic discharge                    |
| <b>ESR</b>    | Edge Services Router                       |
| <b>F</b>      |                                            |
| <b>FTP</b>    | File Transfer Protocol                     |
| <b>I</b>      |                                            |
| <b>IANA</b>   | Internet Assigned Number Authority         |
| <b>ID</b>     | Identity                                   |

|             |                                                        |
|-------------|--------------------------------------------------------|
| <b>iMAP</b> | Integrated Management Application Platform             |
| <b>IP</b>   | Internet Protocol                                      |
| <b>ISU</b>  | Integrated System Control Unit                         |
| <b>L</b>    |                                                        |
| <b>LCT</b>  | Local Craft Terminal                                   |
| <b>LOG</b>  | Call Logging                                           |
| <b>LAN</b>  | Local Area Network                                     |
| <b>M</b>    |                                                        |
| <b>MC</b>   | Message Center                                         |
| <b>MML</b>  | Human-Machine Language (formerly Man-Machine Language) |
| <b>MPLS</b> | MultiProtocol Label Switching                          |
| <b>MA</b>   | Media Service Access                                   |
| <b>MAC</b>  | Media Access Control                                   |
| <b>MAN</b>  | Metropolitan Area Network                              |
| <b>N</b>    |                                                        |
| <b>NE</b>   | Network Element                                        |
| <b>NIC</b>  | Network Information Center                             |
| <b>NTP</b>  | Network Time Protocol                                  |
| <b>O</b>    |                                                        |
| <b>ODBC</b> | Open Database Connectivity                             |
| <b>OEM</b>  | Original Equipment Manufacturer                        |
| <b>OSCT</b> | On Site Configuration Tool                             |
| <b>OSS</b>  | Operation Support System                               |
| <b>P</b>    |                                                        |
| <b>PC</b>   | Personal Computer                                      |
| <b>PPP</b>  | Peer-Peer Protocol                                     |



|             |                                    |
|-------------|------------------------------------|
| <b>PSTN</b> | Public Switched Telephone Network  |
| <b>PVC</b>  | Permanent Virtual Circuit          |
| <b>R</b>    |                                    |
| <b>RVG</b>  | Replicated Volume Group            |
| <b>S</b>    |                                    |
| <b>SCU</b>  | Simple Combiner Unit               |
| <b>SCSI</b> | Small Computer Systems Interface   |
| <b>SNMP</b> | Simple Network Management Protocol |
| <b>SQL</b>  | Structured Query Language          |
| <b>SSH</b>  | Secure Shell                       |
| <b>T</b>    |                                    |
| <b>TCP</b>  | Transport Control Protocol         |
| <b>TFTP</b> | Trivial File Transfer Protocol     |
| <b>U</b>    |                                    |
| <b>UDP</b>  | User Datagram Protocol             |
| <b>UPS</b>  | Uninterrupted Power Supply         |
| <b>V</b>    |                                    |
| <b>VCS</b>  | VERITAS Cluster Server             |
| <b>VEA</b>  | VERITAS Enterprise Administrator   |
| <b>VoIP</b> | Voice over IP                      |
| <b>VVR</b>  | VERITAS Volume Replicator          |
| <b>VxVM</b> | VERITAS Volume Manager             |
| <b>X</b>    |                                    |
| <b>XML</b>  | Extensible Markup Language         |