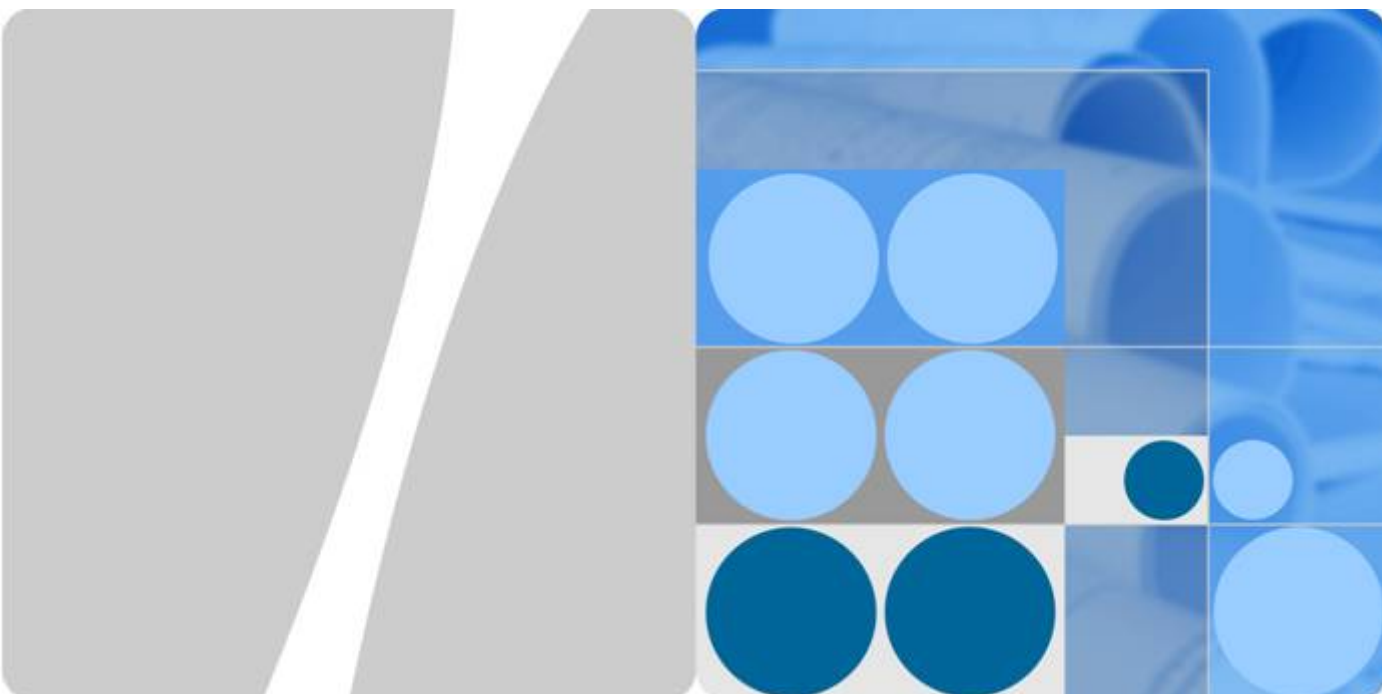




iManager U2000 Unified Network Management System

V100R002C01

Administrator 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 the operations that are performed by the network management system (NMS) administrators on the U2000. This document describes the processes of and methods for the operations and maintenance in various aspects, including user management, log management, database management, process management, and file management.

This document is intended for:

- U2000 system administrators
- Technical support 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.

Contents

About This Document.....	iii
1 Starting the U2000 System.....	1-1
1.1 Starting a Single-Server System (Windows).....	1-2
1.2 Starting a Single-Server System (Solaris).....	1-3
1.3 Starting the Single-Server System (SUSE Linux-Distributed).....	1-6
1.4 Starting the High Availability System (Windows).....	1-9
1.5 Starting a High Availability System (Solaris).....	1-11
1.6 Starting the High Availability System (SUSE Linux-Distributed).....	1-13
1.7 Logging In to the U2000 Client.....	1-15
2 Shutting Down the U2000.....	2-1
2.1 Shutting Down the U2000 Client.....	2-2
2.2 Shutting Down the Single-Server System (Windows).....	2-2
2.3 Shutting Down the Single-Server System (Solaris).....	2-3
2.4 Shutting Down the Single-Server System (SUSE Linux-Distributed).....	2-4
2.5 Shutting Down the High Availability System (Windows).....	2-5
2.6 Shutting Down the High Availability System (Solaris).....	2-6
2.7 Shutting Down the High Availability System (SUSE Linux-Distributed).....	2-8
3 Applying for and Updating the License.....	3-1
3.1 U2000 License Precautions.....	3-2
3.2 Applying for the U2000 License.....	3-2
3.3 Updating the U2000 License.....	3-4
3.4 Checking the Status of the U2000 License.....	3-9
3.5 Setting the Threshold of the Accessing NEs.....	3-9
3.6 Verifying the U2000 License.....	3-10
4 Security Management.....	4-1
4.1 Security Management Strategy.....	4-3
4.1.1 User Security Policy.....	4-4
4.1.2 Log Management Policy.....	4-6
4.1.3 Database Security Policy.....	4-7
4.1.4 NE Security Management.....	4-7
4.2 Setting Security Policies of U2000 Users.....	4-9
4.2.1 Setting the U2000 Login Mode.....	4-9

4.2.2 Setting the Access Control List.....	4-10
4.2.3 Setting the Password Policy.....	4-12
4.2.4 Setting the Account Policy.....	4-13
4.3 Creating U2000 Users and Assigning Permissions.....	4-14
4.3.1 Procedure for Creating U2000 Users.....	4-14
4.3.2 Creating an Object Set.....	4-15
4.3.3 Creating an Operation Set.....	4-16
4.3.4 Creating a U2000 User Group.....	4-18
4.3.5 Creating a U2000 User Account.....	4-20
4.3.6 Example for Creating User Accounts and Assigning Rights in the Authority- and Domain-based Management Scenario.....	4-21
4.4 Comparing the U2000 User Rights.....	4-25
4.5 Querying the Authorization.....	4-25
4.6 Modifying a U2000 User.....	4-26
4.6.1 Resetting the Password of a U2000 User.....	4-27
4.6.2 Modifying an Object Set.....	4-27
4.6.3 Modifying an Operation Set.....	4-29
4.6.4 Modifying a User Group.....	4-30
4.6.5 Modifying the Information About a U2000 User.....	4-31
4.7 Managing U2000 Object Sets.....	4-32
4.7.1 U2000 Object Set.....	4-33
4.7.2 Creating an Object Set.....	4-33
4.7.3 Modifying an Object Set.....	4-34
4.7.4 Deleting an Object Set.....	4-36
4.8 Managing U2000 Operation Sets.....	4-36
4.8.1 U2000 Operation Set.....	4-37
4.8.2 Creating an Operation Set.....	4-37
4.8.3 Modifying an Operation Set.....	4-38
4.8.4 Deleting an Operation Set.....	4-40
4.8.5 Exporting or Importing Operation Sets.....	4-41
4.9 Monitoring a U2000 User.....	4-43
4.9.1 Monitoring the U2000 User Sessions.....	4-44
4.9.2 Monitoring the U2000 User Operations.....	4-44
4.9.3 Forcing a U2000 User to Quit.....	4-45
4.9.4 Unlocking a User Account.....	4-45
4.9.5 Sending Messages to Online Users.....	4-46
4.10 Managing the Remote Maintenance User.....	4-47
4.10.1 Enabling a Remote Maintenance User.....	4-49
4.10.2 Setting the Remote Maintenance User Authority.....	4-50
4.10.3 Setting the Remote Maintenance User Validity.....	4-51
4.11 Managing NE Users.....	4-52
4.11.1 Querying the NE User Information.....	4-52
4.11.2 Creating an NE User.....	4-53

4.11.3 Modifying NE Users.....	4-55
4.11.4 Changing the NE User Password.....	4-55
4.11.5 Querying NE Security Parameters.....	4-56
4.11.6 Querying NE User Groups.....	4-57
4.11.7 Deleting NE Users.....	4-57
4.12 Managing NE Login.....	4-58
4.12.1 Locking Out NE Login.....	4-58
4.12.2 Locking Out NE Settings.....	4-59
4.12.3 Querying the Information About an Online NE User.....	4-59
4.12.4 Switching a Logged-In NE User.....	4-60
4.12.5 Forcing an NE User to Log Out of the U2000.....	4-61
4.12.6 Setting NE Login Prompt Message.....	4-61
4.13 Setting the Security Access of an NE.....	4-62
4.13.1 Controlling Communication Between NE and U2000 Through Ethernet Port.....	4-62
4.13.2 Controlling Communication Between NE and U2000 Through a Serial Port.....	4-63
4.13.3 Setting the NE OAM Access.....	4-64
4.13.4 Setting the NE COM Access.....	4-64
4.13.5 Controlling Communication Between NE and LCT.....	4-65
4.14 Setting the NE ACL.....	4-66
4.14.1 Overview of ACL.....	4-67
4.14.2 Setting Basic ACL Rules.....	4-67
4.14.3 Setting the Advanced ACL Rules.....	4-68
4.15 Auditing Changes.....	4-68
4.15.1 Viewing Information About Change Auditing.....	4-69
4.15.2 Dumping Information About Change Audit.....	4-69
4.15.3 Deleting Information About Change Audit.....	4-70
4.16 NE License Management.....	4-71
4.16.1 Getting to Know NE License Management.....	4-71
4.16.2 Querying the NE License Information.....	4-72
4.16.3 Applying for an NE License.....	4-73
4.16.4 Installing an NE License.....	4-74
4.16.5 Synchronize NE Information.....	4-75
4.16.6 Adjusting the NE License Capacity.....	4-75
4.16.7 Changing an NE License.....	4-76
5 Backing Up and Restoring the U2000 Database.....	5-1
5.1 Basic Concepts and Application Scenarios.....	5-3
5.2 Methods of Backing Up and Restoring the U2000 Data.....	5-4
5.3 Suggestions on Data Backup and Restoration.....	5-6
5.4 Backing Up U2000 Data to a Local Server.....	5-6
5.4.1 Periodically Backing Up the U2000 Data to a Local Server Through the U2000 Client.....	5-7
5.4.2 Immediately Backing Up the U2000 Database to a Local Server Through the U2000 Client.....	5-8
5.4.3 Immediately Backing Up the U2000 Database to a Local Server Through the MSuite.....	5-9

6 Managing U2000 Files and Disks.....6-1

6.2 Single-Server System (Windows).....	6-5
6.2.1 Checking the Usage of the Server Disk.....	6-5
6.2.2 Cleaning Up the U2000 Server Disk Space.....	6-6
6.2.3 Cleaning Up the U2000 Client Disk Space.....	6-7
6.3 Single-Server System (Solaris).....	6-7
6.3.1 Checking the Usage of the Server Disk.....	6-7
6.3.2 Cleaning Up the U2000 Server Disk Space.....	6-8
6.3.3 Cleaning Up the U2000 Client Disk Space.....	6-9
6.4 Single-Server System (SUSE Linux-Distributed).....	6-9
6.4.1 Checking the Usage of Server Disks.....	6-9
6.4.2 Cleaning Up the U2000 Server Disk Space.....	6-10
6.4.3 Cleaning Up the U2000 Client Disk Space.....	6-11
6.5 High Availability System (Windows).....	6-11
6.5.1 Checking Server Disks.....	6-11
6.5.1.1 Checking the Disk Usage of the U2000 Server.....	6-12
6.5.1.2 Checking the Status of Server Disks.....	6-15
6.5.1.3 Checking the Disk Group Status of the U2000 Server.....	6-17
6.5.1.4 Checking the Disk Volume Status of the U2000 Server.....	6-20
6.5.2 Clearing Disk Space.....	6-23
6.5.2.1 Cleaning Up the U2000 Server Disk Space.....	6-24
6.5.2.2 Cleaning Up the U2000 Client Disk Space.....	6-24
6.6 High Availability System (Solaris).....	6-25
6.6.1 Checking Server Disks.....	6-25
6.6.1.1 Checking the Disk Usage of the U2000 Server.....	6-25
6.6.1.2 Checking the Disk Status of the U2000 Server.....	6-26
6.6.1.3 Checking the Disk Group Status of the U2000 Server.....	6-28
6.6.1.4 Checking the Disk Volume Status of the U2000 Server.....	6-28
6.6.1.5 Viewing the Disk Mirroring Status.....	6-31
6.6.1.6 Monitoring the Mounting Status of File Systems.....	6-34
6.6.2 Clearing Disk Space.....	6-35
6.6.2.1 Cleaning Up the U2000 Server Disk Space.....	6-35
6.6.2.2 Cleaning Up the U2000 Client Disk Space.....	6-36
6.7 High Availability System (SUSE Linux-Distributed).....	6-36
6.7.1 Checking Server Disks.....	6-36
6.7.1.1 Checking the Usage of U2000 Server Disks.....	6-37
6.7.1.2 Checking the Status of Server Disks.....	6-37
6.7.1.3 Checking the Disk Group Status of the U2000 Server.....	6-38
6.7.1.4 Checking the Disk Volume Status of the U2000 Server.....	6-39
6.7.1.5 Viewing the Disk Mirroring Status.....	6-41
6.7.1.6 Monitoring the Mounting Status of File Systems.....	6-44
6.7.2 Clearing Disk Space.....	6-44
6.7.2.1 Cleaning Up the U2000 Server Disk Space.....	6-45

6.7.2.2 Cleaning Up the U2000 Client Disk Space.....	6-45

7 Log Management.....7-1

7.1 Getting to Know Log Management.....	7-3
7.1.1 Log Management Function.....	7-3
7.1.2 Log Types.....	7-3
7.1.2.1 Security Logs.....	7-4
7.1.2.2 Operation Logs.....	7-5
7.1.2.3 NE Syslog.....	7-6
7.1.2.4 System Logs.....	7-8
7.2 Managing Operation Logs.....	7-9
7.2.1 Querying Operation Logs.....	7-10
7.2.2 Collecting Statistics on Operation Logs.....	7-11
7.3 Managing System Logs.....	7-12
7.3.1 Querying System Logs.....	7-13
7.3.2 Collecting Statistics on System Logs.....	7-14
7.4 Managing Security Logs.....	7-15
7.4.1 Querying Security Logs.....	7-15
7.4.2 Collecting Statistics on Security Logs.....	7-16
7.5 Managing NE Logs.....	7-18
7.5.1 Browsing the NE Syslog Running Logs.....	7-18
7.5.2 Synchronizing SNMP Device Logs.....	7-19
7.6 Setting Log Templates.....	7-19
7.7 Setting a Log Forwarding Server.....	7-21
7.8 Managing Log Data.....	7-22
7.8.1 Setting U2000 Log Timing Dumping.....	7-23
7.8.2 Setting U2000 Log Overflow Dump.....	7-23
7.8.3 Manually Dumping U2000 Logs.....	7-24
7.8.4 Setting U2000 Log Export.....	7-25
7.9 Managing NE Syslog.....	7-26
7.9.1 Syslog Management Overview.....	7-26
7.9.1.1 Functions of Syslog Management.....	7-26
7.9.1.2 Basic Concepts.....	7-27
7.9.2 Configuration Flow of Syslog Management.....	7-27
7.9.3 Deploying the NE Syslog Collector.....	7-27
7.9.4 Configuring the Information Center on the NEs.....	7-27
7.9.4.1 Enabling the Information Center.....	7-28
7.9.4.2 Configuring the Syslog Source Interface.....	7-29
7.9.4.3 Adding the Syslog Host.....	7-29
7.9.4.4 Configuring the Advanced Attributes of the Syslog Service.....	7-30
7.10 Transferring NE Logs to Log Servers.....	7-31
7.10.1 Syslog Service.....	7-31
7.10.2 Configuring the Syslog Server.....	7-35

7.10.3 Configuring the Syslog GNE.....	7-35
7.10.4 Configuring the Syslog Type and Severity.....	7-36
7.10.5 Starting the Syslog Service.....	7-36
8 Monitoring the U2000 Processes.....	8-1
8.1 Process Overview.....	8-2
8.1.1 Start Mode.....	8-2
8.1.2 U2000 Process List.....	8-2
8.2 Logging In to the System Monitor Client.....	8-17
8.3 Setting the Monitoring Parameters.....	8-18
8.3.1 Setting the Parameters for the U2000 Server Monitoring.....	8-19
8.3.2 Setting the Parameters for the U2000 Server Hard Disk Monitoring.....	8-20
8.3.3 Setting the Parameters for the U2000 Server Database Monitoring.....	8-21
8.3.4 Setting the Parameters for the U2000 Server Process Monitoring.....	8-22
8.4 Monitoring the Running Status of the U2000.....	8-23
8.5 Starting and Stopping a Process.....	8-25
8.6 Setting the Process Start Mode.....	8-25
9 Common Veritas Operations.....	9-1
9.1 Switchover Principle of the Two-Site Cluster.....	9-2
9.2 Managing the Login of VCS Users.....	9-3
9.2.1 Adding a Cluster.....	9-4
9.2.2 Logging In to the VCS Client.....	9-5
9.2.3 Deleting a Cluster.....	9-6
9.2.4 Logging Out of the VCS Client.....	9-6
9.2.5 Exiting the VCS Client.....	9-7
9.3 Managing Resource Groups.....	9-7
9.3.1 Bringing a Resource Group Online.....	9-7
9.3.2 Taking a Resource Group Offline.....	9-8
9.3.3 Locking a Resource Group.....	9-9
9.3.4 Unlocking a Resource Group.....	9-10
9.3.5 Enabling a Resource Group.....	9-10
9.3.6 Disabling a Resource Group.....	9-11
9.3.7 Clearing a Resource Group Fault Flag.....	9-11
9.4 Managing Resources.....	9-11
9.4.1 Bringing a Resource Online.....	9-12
9.4.2 Taking a Resource Offline.....	9-13
9.4.3 Enabling a Resource.....	9-14
9.4.4 Disabling a Resource.....	9-15
9.4.5 Detecting Resources.....	9-15
9.4.6 Clearing a Resource Fault Flag.....	9-16
9.4.7 Clearing the Current Operation.....	9-16
9.5 Managing Replication Volumes.....	9-17
9.5.1 Importing a Disk Group.....	9-17

9.5.2 Recovering a Disk Volume.....	9-18
9.5.3 Recovering the RVG.....	9-18
9.5.4 Recovering the RLink.....	9-19
9.5.5 Re-synchronizing the Data on Primary and Secondary Sites.....	9-19
9.6 Switching Over the Active Site and the Standby Site.....	9-20
9.6.1 Manual Switchover Between Active and Standby Sites.....	9-20
9.6.2 Automatic Switchover Between Primary and Secondary Sites.....	9-23
9.7 Monitoring Active and Standby Sites.....	9-24
9.7.1 Checking the Data Replication Status.....	9-24
9.7.2 Checking the Status of the Active and Standby Sites.....	9-25
10 U2000 Port List.....	10-1
10.1 U2000 Service Port Overview.....	10-2
10.2 Ports Between the U2000 Server and the NEs.....	10-4
10.3 Ports Between the U2000 Server and the Clients.....	10-11
10.4 Ports Between the U2000 Server and the OSS.....	10-19
10.5 Ports on Primary and Secondary Sites of the Veritas HA System.....	10-25
10.6 Ports for Internal Processes of the U2000 Server.....	10-29
10.7 Ports for Remote Maintenance.....	10-37
10.8 Ports for Other Connections.....	10-40
11 Changing the System IP Address and Host Name.....	11-1
11.1 How to Change the IP Address of the Single-Server System on Windows.....	11-2
11.2 How to Change the Host Name of the Single-Server System on Windows.....	11-3
11.3 How to Change the IP Address and Host Name for the Single-Server System (Solaris).....	11-5
11.4 How to Change the IP Address and Host Name of the Single-Server System (SUSE Linux-Distributed)	11-7
11.5 How to Modify the Server IP Address of High Availability System (Windows).....	11-9
11.6 How to Change the Host Name of the High Availability System (Windows).....	11-12
11.7 How to Change the IP Address and Host name for the High Availability System (Solaris).....	11-15
11.8 How to Change the IP Address and Host Name of the High Availability System (SUSE Linux-Distributed)	11-21
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 Check the Sybase Database Version.....	A-79
A.6.2.2 How to View the Server Name of the Sybase Database.....	A-80
A.6.2.3 How to Change the Password of User sa for the Sybase Database.....	A-81
A.6.2.4 How to Clear the Password of the Sybase Database.....	A-82
A.6.2.5 How to View the Bit Number of the Sybase Database.....	A-82
A.6.2.6 How to View the Details of the Sybase Database.....	A-83
A.6.2.7 How to View Data Tables.....	A-83
A.6.2.8 How to Query a Database Table if Only Part of the Table Name Is Remembered.....	A-84
A.6.2.9 How to Identify Database Errors Caused by Unexpected Powering-Off of the Workstation.....	A-84
A.6.2.10 How to Expand Space for the master Database.....	A-86
A.6.2.11 How to Set Up More User Connections to a Database.....	A-87
A.6.2.12 How to Check for Database Errors Using the dbcc Tool.....	A-88
A.6.2.13 How to Set the Network Transport Parameters of Databases.....	A-89
A.6.2.14 How to Delete a Suspect Database.....	A-91
A.6.2.15 How to Delete a Damaged User Database.....	A-93
A.6.2.16 How to Delete a Database from the Sybase Database?.....	A-94
A.6.2.17 How to View the Deadlock Information in the Database.....	A-94
A.7 Oracle Database.....	A-96
A.7.1 How to Check the Version of the Oracle Database.....	A-96
A.7.2 How to Check the Name of the Oracle Database.....	A-96
A.7.3 How to Start the Oracle Database in the High Availability System.....	A-97
A.7.4 How Can I Start the Oracle Database (Single-Server System)?.....	A-98
A.7.5 How to Shut Down the Oracle Database (High Availability System).....	A-99
A.7.6 How Can I Stop the Oracle Database (Single-Server System)?.....	A-100
A.7.7 How Can I Check Whether the Oracle Database Is Started?.....	A-101
A.7.8 How Can I Change the Password of an Oracle Database User?.....	A-101
A.7.9 How Can I Check Whether the Oracle Listener Is Started?.....	A-102
A.8 MSuite.....	A-102
A.8.1 How to Verify That The Process of the MSuite Server Is Started.....	A-103
A.8.2 How to Start the Process of the MSuite Server.....	A-103
A.8.3 How to End Processes on the MSuite Server.....	A-103
A.8.4 How to Start the MSuite Client.....	A-104
A.9 U2000 System.....	A-104
A.9.1 How to Change the System Time and Time Zone of the Single-Server System on Windows.....	A-106
A.9.2 How to Change the System Time and Time Zone of the Single-Server System (Solaris).....	A-107
A.9.3 How to Change the System Time and Time Zone of the Single-Server System (SUSE Linux-Distributed)	A-108
A.9.4 How to Change the System Time and Time Zone of the High Availability System on Windows	A-109

A.9.5 How to Change the System Time and Time Zone of the High Availability System (Solaris).....	A-110
A.9.6 How to Change the System Time and Time Zone of the High Availability System (SUSE Linux-Distributed).....	A-111
A.9.7 How to Verify That the Processes of the U2000 Single-Server System Are Running on Windows.....	A-112
A.9.8 How to Start the Processes of the U2000 Single-Server System on Windows.....	A-113
A.9.9 How to End the Processes of the U2000 Single-Server System on Windows.....	A-113
A.9.10 How to Verify That the Processes of the U2000 Single-Server System Are Running on Solaris.....	A-114
A.9.11 How to Start the Processes of the U2000 Single-Server System on Solaris.....	A-114
A.9.12 How to End the Processes of the U2000 Single-Server System on Solaris.....	A-115
A.9.13 How to Verify That the Processes of the U2000 Single-Server System (SUSE Linux-Distributed) Are Running.....	A-116
A.9.14 How to Start the Processes of the U2000 Single-Server System (SUSE Linux-Distributed).....	A-116
A.9.15 How to End the Processes of the U2000 Single-Server System (SUSE Linux-Distributed).....	A-117
A.9.16 How to Check Whether the U2000 Processes of the High Availability System (Windows) Are Started.....	A-117
A.9.17 How to Start the U2000 Processes of the High Availability System (Windows).....	A-118
A.9.18 How to End the U2000 Processes of the High Availability System (Windows).....	A-119
A.9.19 How to Check Whether the U2000 Processes of the High Availability System (Solaris) Are Started.....	A-120
A.9.20 How to Start the U2000 Processes of the High Availability System (Solaris).....	A-121
A.9.21 How to End the U2000 Processes of the High Availability System (Solaris).....	A-122
A.9.22 How to Check Whether the U2000 Processes of the High Availability System (SUSE Linux-Distributed) Are Started.....	A-123
A.9.23 How to Start the U2000 Processes of the High Availability System (SUSE Linux-Distributed).....	A-124
A.9.24 How to End the U2000 Processes of the High Availability System (SUSE Linux-Distributed).....	A-125
A.9.25 What Factors Affect the Response Speed of the NMS.....	A-126
A.9.26 How to Resolve the Problem Wherein Illegible Characters Occur in the NMS Window.....	A-127
A.9.27 How to Add Components Incrementally.....	A-127
A.9.28 How to Configure the ipmap.cfg Mapping File.....	A-130
A.9.29 How to Check Whether the daem Process Is Started.....	A-132
A.9.30 How to Start the daem Process.....	A-132
A.9.31 How to End the daem Process.....	A-133
A.9.32 How to Rectify the Application GUI Startup Failure Caused by User Switching.....	A-133
A.9.33 How to Rectify the U2000 Startup Failure After the IP Address or Host Name of the Single-Server System (Solaris) Is Changed Manually.....	A-134
A.9.34 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-135
A.9.35 How to View the U2000 and Sybase Database Installation Paths.....	A-137
A.9.36 How to View Network Configurations for the Primary Site or Secondary Site Installed with a HA System.....	A-138
A.9.37 How to Rectify the Mouse Detection Failure and Open the GUI After the T5220 Is Connected to the KVM.....	A-140

A.9.38 How to Check Downloaded Software Packages by Using MD5 Software.....	A-142
A.9.39 How to Rectify the Failure to Connect to the Sybase Database During U2000 Installation.....	A-142
A.9.40 Reinstalling the U2000 on or Migrating the U2000 to Another Computer.....	A-143
A.9.41 How to Set the Communication Mode on the U2000 server for the Single-Server System (Windows)	A-144
A.9.42 How to Set the Communication Mode on the U2000 server for the Single-Server System (Solaris)	A-144
A.9.43 How to Configure the Communication Mode for a Linux-based U2000 Server?.....	A-145
A.9.44 How to Set the Communication Mode on the U2000 Server for the High Availability System (Windows)	A-146
A.9.45 How to Set the Communication Mode of the Server in a High Availability System (Solaris)?...A-149	
A.9.46 How to Set the Communication Mode of the Server in a High Availability System (SUSE Linux- Distributed).....	A-151
B U2000 Utilities.....	B-1
C MSuite.....	C-1
C.1 Overview.....	C-2
C.1.1 Basic Concepts.....	C-2
C.1.2 System Architecture of the MSuite.....	C-4
C.1.3 Function Overview.....	C-5
C.1.4 Graphical User Interface.....	C-8
C.1.5 Command Line Interface.....	C-10
C.2 Starting and Stopping the MSuite.....	C-11
C.2.1 Starting the Process of the MSuite Server.....	C-12
C.2.2 Logging In to the MSuite Client.....	C-12
C.2.3 Exiting from the MSuite client.....	C-13
C.2.4 Ending the Process of the MSuite Server.....	C-14
C.3 System Management.....	C-14
C.3.1 Refreshing the NMS Information.....	C-14
C.3.2 Synchronizing the NMS Information.....	C-15
C.3.3 Synchronizing the NMS Information (High Availability System).....	C-16
C.3.4 Changing the Password of the MSuite.....	C-17
C.3.5 Logging Out of the MSuite Client.....	C-18
C.4 U2000 Deployment.....	C-18
C.4.1 Adding a Component.....	C-19
C.4.2 Deleting a Component.....	C-20
C.4.3 Adding an Instance.....	C-21
C.4.4 Deploying instances by License.....	C-22
C.4.5 Deleting an Instance.....	C-23
C.4.6 Changing the Name and Remarks of an Instance.....	C-24
C.4.7 Setting the System Time and Time Zone.....	C-25
C.4.8 Changing the Password of the Administrator of the Database.....	C-26
C.4.9 Changing the Password of the User of the Database.....	C-27
C.4.10 Configuring the NTP Service.....	C-28

C.5 Adjusting the NMS.....	C-29
C.5.1 Changing the Host Name and IP Address.....	C-29
C.5.1.1 How to Change the IP Address of the Single-Server System on Windows.....	C-31
C.5.1.2 How to Change the Host Name of the Single-Server System on Windows.....	C-33
C.5.1.3 How to Change the IP Address and Host Name for the Single-Server System (Solaris).....	C-34
C.5.1.4 How to Change the IP Address and Host Name of the Single-Server System (SUSE Linux-Distributed).....	C-36
C.5.1.5 How to Modify the Server IP Address of High Availability System (Windows).....	C-38
C.5.1.6 How to Change the Host Name of the High Availability System (Windows).....	C-41
C.5.1.7 How to Change the IP Address and Host name for the High Availability System (Solaris).....	C-44
C.5.1.8 How to Change the IP Address and Host Name of the High Availability System (SUSE Linux-Distributed).....	C-49
C.5.2 Configuring Routes.....	C-55
C.5.3 Synchronizing Network Configurations.....	C-56
C.6 Management of the High Availability System (Veritas hot standby).....	C-57
C.6.1 Establishing the HA Relationship Between the Primary and Secondary Sites.....	C-58
C.6.2 Deleting the HA Relationship Between the Primary and Secondary Sites.....	C-59
C.6.3 Deleting Replication Relations.....	C-60
C.6.4 Configuring the Current Server as the Active Server Forcibly.....	C-61
C.6.5 Performing the Dual-Active Operation.....	C-61
C.7 Maintaining a Distributed System.....	C-62
C.7.1 Adding a Slave Server.....	C-62
C.7.2 Deleting a Slave Server.....	C-63
C.7.3 Migrating an Instance.....	C-64
C.8 Configuring the Northbound Interface Instance.....	C-65
C.9 Managing Databases.....	C-65
C.9.1 Backing Up the System Database.....	C-66
C.9.1.1 Immediately Backing Up the U2000 Database to a Local Server Through the MSuite.....	C-66
C.9.1.2 Immediately Backing Up the U2000 Database to a Remote Server Through the MSuite.....	C-68
C.9.2 Restoring Data of a U2000 Single-Server System (Windows).....	C-70
C.9.2.1 Restoring U2000 Single-Server System (Windows) Data from a Local Server.....	C-70
C.9.2.2 Restoring U2000 Single-Server System (Windows) Data from a Remote Server.....	C-72
C.9.3 Restoring U2000 Single-Server System (Solaris) Data.....	C-74
C.9.3.1 Restoring U2000 Single-Server System (Solaris) Data from a Local Server.....	C-75
C.9.3.2 Restoring U2000 Single-Server System (Solaris) Data from a Remote Server.....	C-77
C.9.4 Restoring U2000 Single-Server System (SUSE Linux-Distributed) Data.....	C-80
C.9.4.1 Restoring U2000 Single-Server System (SUSE Linux-Distributed) Data from a Local Server....	C-80
C.9.4.2 Restoring U2000 Single-Server System (SUSE Linux-Distributed) Data from a Remote Server.....	C-82
C.9.5 Restoring U2000 High Availability System (Windows) Data.....	C-85
C.9.5.1 Restoring U2000 High Availability System (Windows) Data from a Local Server.....	C-85
C.9.5.2 Restoring U2000 High Availability System (Windows) Data from a Remote Server.....	C-87
C.9.6 Restoring U2000 High Availability System (Solaris) Data.....	C-90

C.9.6.1 Restoring U2000 High Availability System (Solaris) Data from a Local Server.....	C-90
C.9.6.2 Restoring U2000 High Availability System (Solaris) Data from a Remote Server.....	C-93
C.9.7 Restoring U2000 High Availability System (SUSE Linux-Distributed) Data.....	C-96
C.9.7.1 Restoring U2000 High Availability System (SUSE Linux-Distributed) Data from a Local Server	C-96
C.9.7.2 Restoring U2000 High Availability System (SUSE Linux-Distributed) Data from a Remote Server	C-98
C.9.8 Restoring Data of a U2000 High Availability System (Cross-U2000).....	C-101
C.9.9 Initializing the U2000 Database.....	C-102

D Reference of Solaris/Linux Commands.....D-1

D.1 Commands for Operating Solaris or Linux Folders.....	D-2
D.1.1 pwd Command.....	D-2
D.1.2 cd Command.....	D-2
D.1.3 mkdir Command.....	D-3
D.1.4 rmdir Command.....	D-4
D.1.5 ls Command.....	D-4
D.2 Commands for Operating Solaris or Linux Files.....	D-6
D.2.1 vi Command.....	D-7
D.2.2 cp Command.....	D-9
D.2.3 mv Command.....	D-9
D.2.4 rm Command.....	D-10
D.2.5 chmod Command.....	D-10
D.2.6 chown Command.....	D-12
D.2.7 chgrp Command.....	D-13
D.2.8 find Command.....	D-14
D.2.9 tar Command.....	D-16
D.2.10 gtar Command.....	D-18
D.2.11 compress Command.....	D-19
D.2.12 uncompress Command.....	D-20
D.2.13 pack Command.....	D-20
D.2.14 unpack Command.....	D-21
D.2.15 pkgadd Command.....	D-21
D.2.16 pkgrm Command.....	D-22
D.3 Commands for Viewing Solaris or Linux Text Files.....	D-22
D.3.1 echo Command.....	D-22
D.3.2 cat Command.....	D-23
D.3.3 more Command.....	D-24
D.3.4 head Command.....	D-25
D.3.5 tail Command.....	D-26
D.3.6 clear Command.....	D-26
D.3.7 grep Command.....	D-27
D.4 Commands for Managing Solaris or Linux Users.....	D-27
D.4.1 useradd Command.....	D-28

D.4.2 userdel Command.....	D-29
D.4.3 usermod Command.....	D-30
D.4.4 passwd Command.....	D-31
D.4.5 groupadd Command.....	D-31
D.4.6 groupdel Command.....	D-31
D.4.7 groupmod Command.....	D-32
D.5 Commands for Managing Solaris or Linux System Resources.....	D-32
D.5.1 man Command.....	D-33
D.5.2 df Command.....	D-34
D.5.3 du Command.....	D-35
D.5.4 ps Command.....	D-37
D.5.5 kill Command.....	D-38
D.5.6 who Command.....	D-39
D.5.7 which Command.....	D-40
D.5.8 hostname Command.....	D-40
D.5.9 uname Command.....	D-41
D.5.10 ifconfig Command.....	D-42
D.5.11 script Command.....	D-42
D.5.12 date Command.....	D-43
D.5.13 bc Command.....	D-45
D.5.14 prtconf Command.....	D-45
D.5.15 prstat Command.....	D-47
D.6 Commands for Network Communications in the Solaris or Linux System.....	D-48
D.6.1 ping Command.....	D-48
D.6.2 telnet Command.....	D-49
D.6.3 ftp Command.....	D-50
D.6.4 finger Command.....	D-52
D.6.5 netstat Command.....	D-53
D.6.6 route Command.....	D-55
E Reference of Sybase Database Commands.....	E-1
E.1 startserver Command.....	E-2
E.2 showserver Command.....	E-3
E.3 isql Command.....	E-3
E.4 shutdown Command.....	E-5
E.5 sp_configure Command.....	E-6
F Reference of Oracle Database Commands.....	F-1
F.1 sqlplus Command.....	F-2
F.2 startup Command.....	F-3
F.3 shutdown Command.....	F-4
F.4 show Command.....	F-5
F.5 alter Command.....	F-7

G Common Commands for HA System (Veritas Hot Standby).....G-1

 G.1 Overview of Commands.....G-2

 G.2 Status Query Commands.....G-3

 G.2.1 vxprint.....G-3

 G.2.2 vxdisk.....G-5

 G.2.3 vxdg.....G-6

 G.2.4 vradmin.....G-6

 G.2.5 hastatus.....G-9

 G.3 Maintenance Command.....G-11

 G.3.1 hagrp.....G-11

 G.3.2 hastop.....G-12

 G.3.3 hagui.....G-13

H Common Maintenance Tools.....H-1

I Abbreviations.....I-1

Figures

Figure 4-1 Implementation of security management.....	4-3
Figure 4-2 Networking of authority and domain-based management.....	4-22
Figure 6-1 Selecting profile.....	6-12
Figure 6-2 VEA login window.....	6-13
Figure 6-3 Connection.....	6-13
Figure 6-4 Accessing the login window.....	6-14
Figure 6-5 Viewing the usage of server disks.....	6-14
Figure 6-6 Selecting profile.....	6-15
Figure 6-7 VEA login window.....	6-16
Figure 6-8 Connection.....	6-16
Figure 6-9 Accessing the login window.....	6-17
Figure 6-10 Selecting profile.....	6-18
Figure 6-11 VEA login window.....	6-18
Figure 6-12 Connection.....	6-19
Figure 6-13 Accessing the login window.....	6-19
Figure 6-14 Viewing the disk group status.....	6-20
Figure 6-15 Selecting profile.....	6-21
Figure 6-16 VEA login window.....	6-21
Figure 6-17 Connection.....	6-22
Figure 6-18 Accessing the login window.....	6-22
Figure 6-19 Viewing the disk volume status.....	6-23
Figure 6-20 Selecting profile.....	6-31
Figure 6-21 Logging in VEA.....	6-32
Figure 6-22 Connect the server.....	6-32
Figure 6-23 Entering user name and password.....	6-33
Figure 6-24 Viewing the disk mirroring result.....	6-33
Figure 6-25 Selecting a profile.....	6-41
Figure 6-26 Logging in to the VEA.....	6-42
Figure 6-27 Connecting to the server.....	6-42
Figure 6-28 Entering the user name and password.....	6-43
Figure 6-29 Viewing the disk mirroring result.....	6-43
Figure 7-1 Process of configuring Syslog management.....	7-27
Figure 7-2 IP and ECC hybrid networking-1.....	7-32

Figure 7-3 IP and ECC hybrid networking-2.....	7-33
Figure 7-4 ECC independent networking.....	7-34
Figure 9-1 shows the conversion relations between the four status.....	9-3
Figure 9-2 Adding a cluster.....	9-4
Figure 9-3 Cluster monitor.....	9-5
Figure 9-4 Logging in to the VCS.....	9-6
Figure 9-5 Bringing a resource group online.....	9-8
Figure 9-6 Bringing a resource group offline.....	9-9
Figure 9-7 Bringing a resource online.....	9-13
Figure 9-8 Enabling a resource.....	9-14
Figure 9-9 Clearing the current operation.....	9-16
Figure 9-10 Viewing the status of the remote cluster.....	9-22
Figure 9-11 Switching over the global group.....	9-22
Figure 9-12 Confirming the switchover.....	9-23
Figure 9-13 Status of the resource groups on the active site.....	9-26
Figure 9-14 Heartbeat status of the center standby site.....	9-27
Figure 9-15 Resource group status of the center standby site.....	9-28
Figure 9-16 Heartbeat status of the active server.....	9-28
Figure 10-1 Relationship between the U2000 server and peripherals.....	10-3
Figure 11-1 High Availability System (Solaris) resources.....	11-16
Figure 11-2 High Availability System (Solaris) resources.....	11-18
Figure 11-3 High Availability System (SUSE Linux-Distributed) resources.....	11-22
Figure 11-4 High Availability System (SUSE Linux-Distributed) resources.....	11-24
Figure A-1 Starting the FTP, TFTP, and Telnet services.....	A-10
Figure A-2 Selecting the service path.....	A-89
Figure A-3 Selecting the database service.....	A-90
Figure A-4 Selecting available network transport settings.....	A-90
Figure A-5 Modifying the transport type.....	A-91
Figure C-1	C-3
Figure C-2 System architecture of the MSuite.....	C-4
Figure C-3 GUI of the MSuite client.....	C-9
Figure C-4 High Availability System (Solaris) resources.....	C-45
Figure C-5 High Availability System (Solaris) resources.....	C-47
Figure C-6 High Availability System (SUSE Linux-Distributed) resources.....	C-50
Figure C-7 High Availability System (SUSE Linux-Distributed) resources.....	C-53

Tables

Table 1-1 Server parameter settings.....	1-16
Table 4-1 Parts of a .csv file.....	4-42
Table 4-2 NE license states.....	4-72
Table 5-1 Characteristics and application scenarios of two data maintenance methods.....	5-5
Table 5-2 Script files the U2000 provides.....	5-49
Table 5-3 U2000 database list.....	5-57
Table 6-1 Major directory architecture for the U2000 server software in the Windows OS.....	6-2
Table 6-2 Directory structure of the U2000 server software in the Solaris or SUSE Linux OS.....	6-3
Table 6-3 Directory structure of the U2000 client software in the Windows OS.....	6-4
Table 6-4 Directory structure of the U2000 client software in the Solaris OS.....	6-5
Table 6-5 Field description for disk volume status.....	6-30
Table 6-6 Field description for disk volume status.....	6-40
Table 7-1 Configuration List.....	7-33
Table 7-2 Configuration List.....	7-35
Table 8-1 U2000 process list.....	8-2
Table 9-1 HA system status.....	9-2
Table 10-1 Ports on the NEs for connecting the U2000.....	10-4
Table 10-2 Ports on the U2000server for connecting NEs.....	10-7
Table 10-3 Ports on the U2000 server for connecting the clients.....	10-11
Table 10-4 Ports on the U2000 server for connecting the OSS.....	10-19
Table 10-5 Ports on the OSS for connecting the U2000 server.....	10-25
Table 10-6 Veritas on primary and secondary sites of the HA system ports.....	10-26
Table 10-7 Ports for internal processes of the U2000 server.....	10-30
Table 10-8 Ports for remote maintenance.....	10-38
Table 10-9 Ports for other connections.....	10-40
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 Space requirement for Solaris or SUSE Linux.....	A-128

Table A-9 Space requirement for Windows.....	A-128
Table A-10 Mapping relationship between U2000 IP addresses and NAT server IP addresses.....	A-131
Table B-1 Common applications in the Windows OS.....	B-1
Table B-2 Common applications in the Solaris OS.....	B-1
Table B-3 Common applications in the SUSE Linux OS.....	B-2
Table C-1 Functions of the MSuite.....	C-5
Table C-2 Common CLI commands for the MSuite.....	C-10
Table D-1 Option description of the mkdir command.....	D-3
Table D-2 Option description of the ls command.....	D-5
Table D-3 Operations in the text input mode.....	D-7
Table D-4 Operations related to moving the cursor in the text input mode.....	D-8
Table D-5 Operation for exiting the text input mode and switching to the command mode.....	D-8
Table D-6 Operations related to deleting characters in the command mode.....	D-8
Table D-7 Commands for exiting the vi editor.....	D-9
Table D-8 Common options in symbol mode of the chmod command	D-11
Table D-9 Conditions for file search.....	D-14
Table D-10 Logical operators of conditions.....	D-15
Table D-11 Option description for the tar command.....	D-17
Table D-12 Descriptions of gtar command options.....	D-18
Table D-13 Option description of the echo command.....	D-23
Table D-14 Option description of the more command.....	D-25
Table D-15 option description of the useradd command.....	D-28
Table D-16 Option description of the usermod command.....	D-30
Table D-17 Description of the uname options.....	D-41
Table D-18 Format of the command output.....	D-44
Table D-19 Common ftp commands.....	D-51
Table D-20 Examples of the finger command.....	D-53
Table D-21 Description of routing flags.....	D-54
Table D-22 Description of the route commands.....	D-56
Table E-1 Condition List Description.....	E-2
Table E-2 Condition List Description.....	E-4
Table E-3 Condition List Description.....	E-5
Table E-4 Condition List Description.....	E-6
Table F-1 Option.....	F-2
Table F-2 Parameters.....	F-3
Table F-3 Parameters.....	F-4
Table F-4 Parameters.....	F-6
Table F-5 Option list.....	F-7
Table G-1 Common commands.....	G-2
Table G-2 Screen output format description of vxprint	G-4
Table G-3 Screen output description of vxprint -l datarlk	G-4
Table G-4 Screen output description of vxprint -l datarvg	G-5

Table G-5 Screen output format description of vxdisk.....G-6

Table G-6 Screen output format description of vx dg.....G-6

Table G-7 Screen output format description.....G-7

Table G-8 Screen output format description.....G-8

Table G-9 Screen output format description.....G-10

Table G-10 Screen output format description.....G-10

Table H-1 Common maintenance tools in the U2000.....H-1

1 Starting the U2000 System

About This Chapter

This topic describes how to start the U2000 System.

[1.1 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.

[1.2 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.

[1.3 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.

[1.4 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.

[1.5 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.

[1.6 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.

[1.7 Logging In to the U2000 Client](#)

Log in to a U2000 using the client, and then perform management operations in the GUI of the U2000 client.

1.1 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.9.41 How to Set the Communication Mode on the U2000 server for the Single-Server System \(Windows\)](#).

----End

1.2 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.
- 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 [4.2.2 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.9.42 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 [1.7 Logging In to the U2000 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.9.42 How to Set the Communication Mode on the U2000 server for the Single-Server System \(Solaris\)](#).

----End

1.3 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 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

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 [1.7 Logging In to the U2000 Client](#).

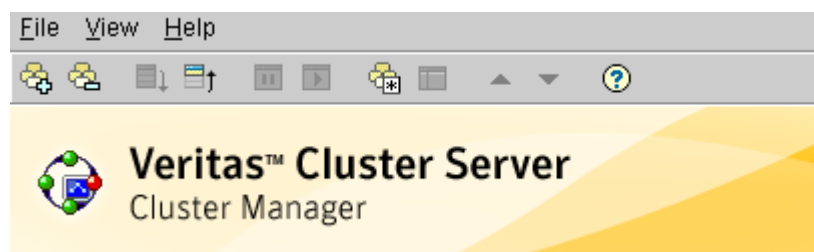
----End

1.4 Starting the High Availability System (Windows)

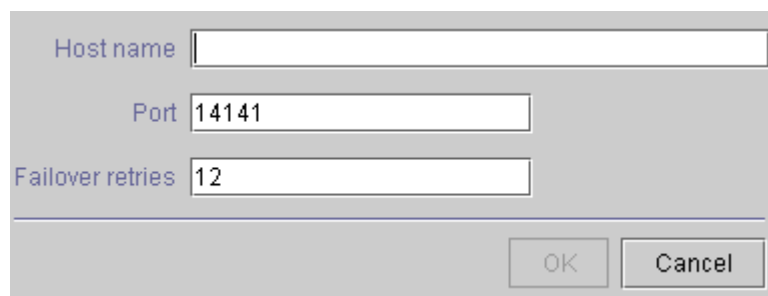
This topic describes how to start the high availability system. Starting the U2000 high availability system includes starting the U2000 server and logging in to the U2000 client.

Procedure

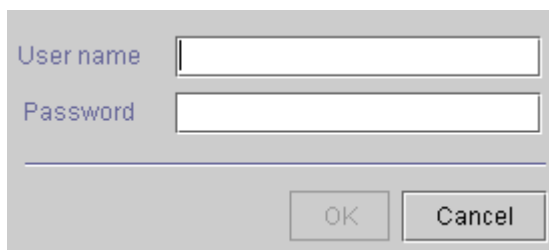
- 1 Log in to the OS of the server of the active site.
- 2 Choose **Start > Programs > Symantec > Veritas Cluster Server > Veritas Cluster Manager - Java Console** to start the VCS client.



- 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 [4.2.2 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.9.42 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.9.44 How to Set the Communication Mode on the U2000 Server for the High Availability System \(Windows\)](#).

----End

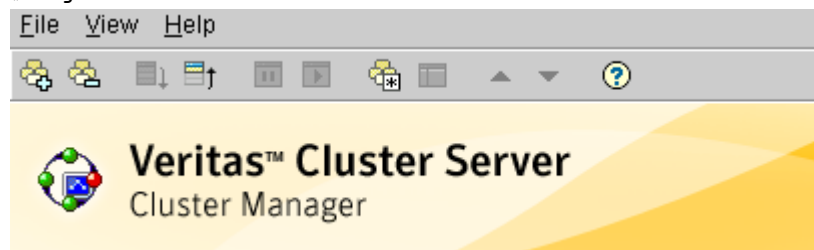
1.5 Starting a High Availability System (Solaris)

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.

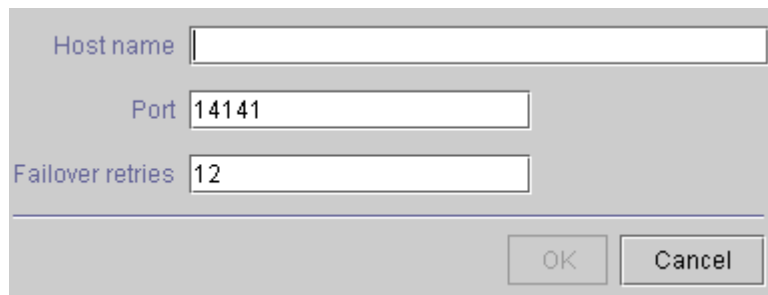
Procedure

- 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:

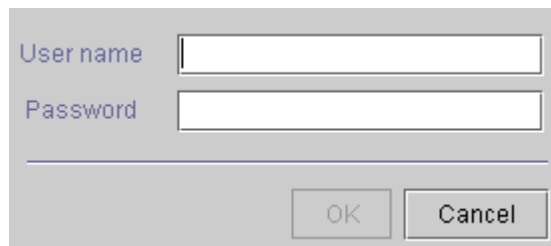
```
# hagui &
```



- 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.9.45 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 [1.7 Logging In to the U2000 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

1.6 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.

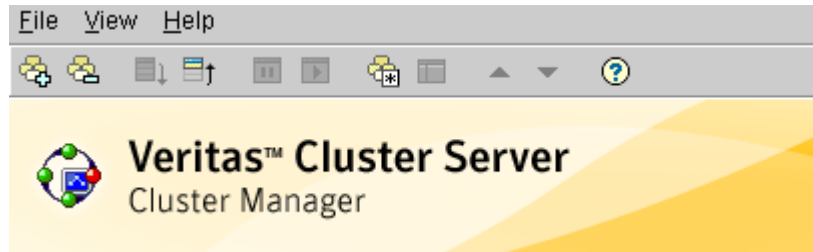
Prerequisite

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:

```
# 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 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 [1.7 Logging In to the U2000 Client](#).

----End

1.7 Logging In to the U2000 Client

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 [10.3 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 [4.2.2 Setting the Access Control List](#).

- The legitimate U2000 user account and password must be allocated.

Context

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 1-1 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.
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.

Parameter	Settings
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.9.41 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.9.42 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.9.43 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.9.44 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.9.45 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.9.46 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.

2 Shutting Down the U2000

About This Chapter

This topic describes how to shut down the U2000 server and client. The shutdown procedure varies according to the deployment scheme.

[2.1 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.

[2.2 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.

[2.3 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).

[2.4 Shutting Down the Single-Server System \(SUSE Linux-Distributed\)](#)

This topic describes how to shut down the U2000 Single-Server System (SUSE Linux-Distributed).

[2.5 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).

[2.6 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).

[2.7 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).

2.1 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.

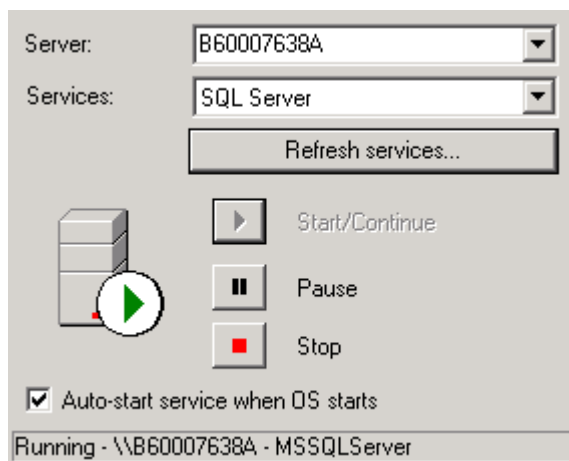
----End

2.2 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

2.3 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 imapmrbl
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

2.4 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
```

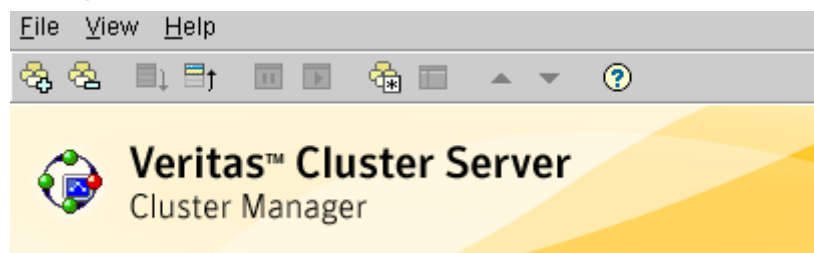
----End

2.5 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

2.6 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.

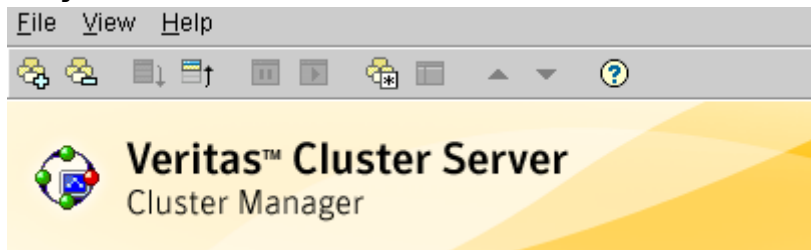
- 2 Stop the U2000 processes.

The U2000 processes consist of the U2000 server process and the Sybase process.

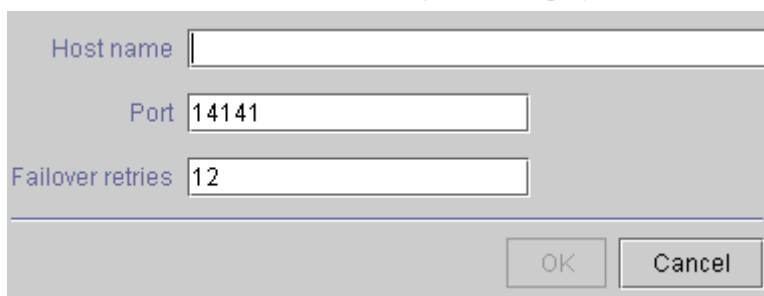
Check whether the U2000 processes are stopped and perform the following operations:

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:

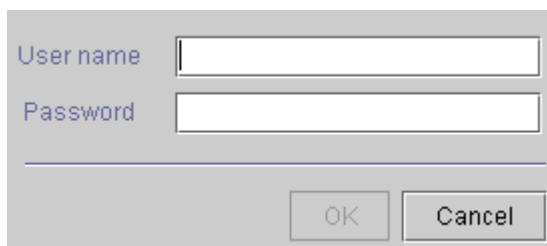
```
# haguai &
```



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

2.7 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:

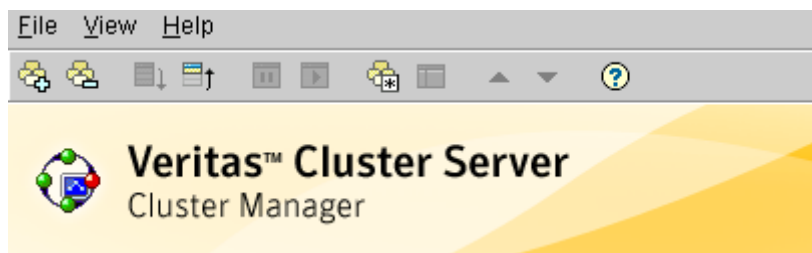
1. Access the **GNOME** session process of the OS of the master server of the active site as the **root** user.

 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

3 Applying for and Updating the License

About This Chapter

This topic describes the license file of the U2000, and how to apply for, install, and use the U2000 license.

[3.1 U2000 License Precautions](#)

This topic describes the U2000 license file. The license file is used to control the functions and management capabilities of the U2000. If the license file is unavailable, you cannot log in to the U2000 client but can only log in to the System Monitor client.

[3.2 Applying for the U2000 License](#)

This topic describes how to apply for the U2000 license.

[3.3 Updating the U2000 License](#)

This topic describes how to update the U2000 license.

[3.4 Checking the Status of the U2000 License](#)

This topic describes how to check the status of the U2000 license. By checking the license status, you can learn the usage of the license, so as to apply for a new license file from Huawei in time before the NMS needs to be expanded or the validity of the license is due.

[3.5 Setting the Threshold of the Accessing NEs](#)

When the number of accessing NEs reaches the preset threshold, the U2000 sends an NE license alarm and displays an **Information** dialog box periodically.

[3.6 Verifying the U2000 License](#)

Introduce how to correctly use a U2000 License.

3.1 U2000 License Precautions

This topic describes the U2000 license file. The license file is used to control the functions and management capabilities of the U2000. If the license file is unavailable, you cannot log in to the U2000 client but can only log in to the System Monitor client.

- The U2000 license file naming format is: ONxxxxxxx.dat.
- One license file corresponds to the equipment serial number (ESN) in an NMS computer and can be used only on the corresponding computer.
- 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.
- Do not make any change to the license file. Otherwise, the license becomes invalid.
- The license folder contains only one license file in the **server/etc/conf/license** directory of the U2000.
- The license control items vary according to the versions of the U2000. When you fill in the application form, use the template that matches the intended version of the U2000.
- The requirements for the server ESN to which a license needs to be bound vary according to the installation scheme. You need to obtain the server ESN based on the installation scheme.
 - In the single-server System (centralized) scheme, the license needs to be bound to the ESN of the server.
 - In the single-server System (distributed) scheme, the license needs to be bound to the ESN of the master server.
 - In the high availability system (Veritas hot standby-centralized) scheme, the license needs to be bound to the ESNs of both the primary site server and the secondary site server.
 - In the high availability system (Veritas hot standby-distributed) scheme, the license needs to be bound to the ESNs of the master servers of both the primary site and the secondary site.
- The licenses of different R versions of the U2000 are incompatible. For example, the license of V100R001 cannot be used by V100R002.

3.2 Applying for the U2000 License

This topic describes how to apply for the U2000 license.

Context

- The license file is not delivered to customers along with the U2000 installation DVD. Contact Huawei engineers to apply for the licenses according to the contract number and the equipment serial number (ESN) of the U2000 server.
- The 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 requirements for the server ESN to which a license needs to be bound vary according to the installation scheme. You need to obtain the server ESN based on the installation scheme.
 - In the single-server System (centralized) scheme, the license needs to be bound to the ESN of the server.
 - In the single-server System (distributed) scheme, the license needs to be bound to the ESN of the master server.
 - In the high availability system (Veritas hot standby-centralized) scheme, the license needs to be bound to the ESNs of both the primary site server and the secondary site server.
 - In the high availability system (Veritas hot standby-distributed) scheme, the license needs to be bound to the ESNs of the master servers of both the primary site and the secondary site.

Procedure

- 1 Obtain the contract number.
- 2 Use the ESN tool provided by the NMS to view the server ESN.

NOTE

Before installing the U2000, you can do as follows to view the ESN of the U2000 server by using the ESN tool provided with the U2000. Alternatively, you can obtain an ESN tool from <http://support.huawei.com> to generate the ESN. The ESN tool names are as follows:

- Solaris OS: U2000`version`_ESN_solaris_SPARC.tar
- Linux OS: U2000`version`_ESN_sles_x64.tar
- Windows OS: U2000`version`_ESN_win32_x86.zip

In Solaris or SUSE Linux OS

1. Log in to the OS of the U2000 server as the **root** user.

NOTE

When the Veritas hot standby HA system is used, you need to log in to the primary and secondary sites OS as the **nmsuser** user.

2. Run the following command to view the ESN:

- In Solaris OS

```
# . /export/home/nmsuser/.profile
# cd /opt/U2000/server/lbin
# ./esn
```
- In the SUSE Linux OS

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

NOTE

There must be a space between the dot (.) and the command (/nmsuser/.profile) in the commands.

A message similar to the following will be displayed:

```
ESN0:EBB74B99612CEDC82AD0A59886EC5018CE44DD4
ESN1:BDA706C825FE0543DC028209778AA66396545412
```

```
ESN2:E1B00EEF6947DD95687AA5C608B72ACC532AB2BD
ESN3:F72F9EC08AEE78AA05A42EFD7BFD89F5E03139C4
.....
```

 NOTE

When the Veritas hot standby HA system is used, you need to respectively save the ESNs of the network interfaces on the primary and secondary sites. During the application for the formal license file, you need to provide the ESNs of the network interfaces of the primary and secondary sites for external communication.

In the Windows OS, you can do as follows to obtain the ESN:

1. Choose **Start > Run**.
2. In the **Run** dialog box, enter **cmd**. The CLI is displayed.
3. Run the following commands:

```
>esn
```

A message similar to the following will be 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 send the license file to you after obtaining it.

The license file provided with the U2000 exist as a .dat file.

----End

3.3 Updating the U2000 License

This topic describes how to update the U2000 license.

Prerequisite

- The OS and database must run properly.
- The processes of the U2000 must be properly started.
- You must log in to the U2000 as the **admin** user.
- The license file of the U2000 must be obtained.
 - **Through the GUI of the client:** Save the new U2000 license to the server where the U2000 client is located.
 - **Through the CLI:** The new license file must be transferred to the U2000 server through FTP.
 - In the Solaris OS, upload the license file to the **/export/home/nmsuser** path on the server as the **nmsuser** user.
 - In the SUSE Linux OS, upload the license file to the **/export/home/nmsuser** path on the server as the **root** user.

- In the high availability system, upload the new U2000 license file to the **/export/home/nmsuser** path on the server on the primary site through FTP.
- Confirm that the license file is transferred in text mode, that is, in ASCII mode.

Context

- In the case that the device types supported by the new license are different from those supported by the original license, the license is updated as follows:
 - If the device types supported by the new license are more than the device types supported by the original license and the added device types are supported by the current version, the license can be updated. If the added device types are not supported by the current version, the license cannot be updated.
 - If the device types supported by the new license are less than the device types supported by the original license and no NEs of the reduced device types are created in the NMS, the license can be updated. If certain NEs of the reduced device types are created in the NMS, the license cannot be updated.
- If the function items supported by the new license are less those supported by the original license, the license cannot be updated.
- In the case that the number of clients supported by the new license is different from that supported by the original license, the license is updated as follows:
 - If the number of clients supported by the new license is less than that supported by the original license but the number of online clients is less than the number of clients supported by the new license, the license can be updated. If the number of online clients is greater than the number of clients supported in the new license, the license cannot be updated.
 - If the number of clients supported by the new license is greater than that supported by the original license, the license can be updated.

In scenarios where you can change the license, you can update the U2000 license through the following methods.



CAUTION

- It is recommended that you update the U2000 license through the GUI of the client.
 - To ensure the normal running of the U2000, do not manually replace the license file.
-
- Through the GUI of the Client
 - Application scenario: This method is recommended if you can log in to the U2000 client and access the GUI.
 - Operation method: Log in to the U2000 client, and then click **Update License** to update the license.
Restart the client after you update the license. Then, the client automatically reloads GUI elements according to control items defined in the new license.
 - Through the CLI
 - Application scenario: This method is applicable to the scenario where you need to remotely update the license through commands because logging in to the U2000 client is not allowed and the client does not provide any GUI.

- Operation method: Check that the processes of the U2000 are properly started, and then run the **updateLicense -file filename** command to update the license file.

Procedure

- **Through the GUI of the Client**

For the single-server system

1. On the U2000 workstation, back up the original license file.
 - In the Windows OS: Create the **backup** folder in the default directory **D:\U2000\server\etc\conf\license**. Copy the original license file to the created folder.
 - In the Solaris or SUSE Linux OS: Create the **backup** folder in the default directory **/opt/U2000/server/etc/conf/license**. Copy the original license file to the created folder.
2. Choose **Help > License Management > License Information** from the client main menu. Then, click **Update License**. In the **Open** dialog box that is displayed, select the new license file and click **Open**.

For the HA system

1. Log in to the U2000 server on the primary site.
2. Back up the original U2000 license file on the primary and secondary sites.

Create the **backup** folder in the default path. Then, copy the original license file to this folder.

 NOTE

- The default path of U2000 license file in the Solaris or SUSE Linux OS is **/opt/U2000/server/etc/conf/license**.
 - The default path of U2000 license file in the Windows OS is **D:\U2000\server\etc\conf\license**.
3. Update the license file on the primary site.
 - (1) Log in to the OS where the U2000 client is installed.
 - In Windows, log in to the OS as the **administrator** user.
 - In Solaris, log in to the OS as the **nmsuser** user.
 - (2) Save the license to be loaded to the server where the U2000 client is installed.
 - (3) On the desktop, double-click **U2000 Client**. The **Login** dialog box is displayed.
 - (4) In the **Server** drop-down list, select the server (server on the primary site) to be logged in to. Then, set **User Name** and **Password** to the valid values, and click **Login**. If you have logged in to the System Monitor before, enter the password for logging in to the System Monitor. If you have never logged in to the System Monitor before and this is the first time that you log in to the U2000 client, the password is empty and you must change the password.
-  **NOTE**
- If a message indicating that no license is available is displayed when you log in to the U2000 client, select the license to be updated as prompted.
 - If an access domain component is selected during installation, choose **Help > License Management > License Information** from the main menu of the U2000 client. In the **License Information** dialog box, click **Update License**. In the **Open** dialog box, select the new license file and click **Open**.
4. Update the license file on secondary site.

- (1) On the primary site, log in to the VCS client.
- (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**.

● **Through the CLI**

For the single-server system

1. On the U2000 workstation, back up the original license file.
 - In the Windows OS: Create the **backup** folder in the default directory **D:\U2000\server\etc\conf\license**. Copy the original license file to the created folder.
 - In the Solaris or SUSE Linux OS: Create the **backup** folder in the default directory **/opt/U2000/server/etc/conf/license**. Copy the original license file to the created folder.
2. Update the U2000 license.
 - (1) In the Windows OS:

- a. Log in to the OS of the server.
- b. 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
Export	1	1	Alarm
no change:	U2000	COMMON	LSW1RENOTI01
Client	1	1	

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

- c. Enter **Y**, and then press **Enter**.
- (2) In the Solaris OS:
 - a. log in to the OS of the U2000 server as the **nmsuser** user.
 - b. Run the following command to update the U2000 license file:

```
$ cd /export/home/nmsuser
$ 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
Export	1	1	Alarm
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) In the SUSE Linux OS:
 - a. log in to the OS of the U2000 server as the **root** user.
 - b. Run the **svc_profile** script to set environment variables.

Run the following command:

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

 NOTE

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

- c. Run the following command to update the U2000 license file:

```
# cd /export/home/nmsuser
# 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
Export	1	1	Alarm
no change:	U2000	COMMON	LSW1RENOTI01
Client	1	1	

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

- d. Enter **Y**, and then press **Enter**.

For the HA system

1. Log in to the U2000 server on the primary site.
2. Back up the original U2000 license file on the primary and secondary sites.

Create the **backup** folder in the default path. Then, copy the original license file to this folder.

 NOTE

- The default path of U2000 license file in the Solaris or SUSE Linux OS is **/opt/U2000/server/etc/conf/license**.
 - The default path of U2000 license file in the Windows OS is **D:\U2000\server\etc\conf\license**.
3. Run the **updateLicense** command to update the license file on the primary site. For details, see [2](#).
 4. Transfer the updated license file on the primary site to the **/opt/U2000/server/etc/conf/license** path on the server on the secondary site in text mode, that is, ASCII mode.

 NOTE

- The default path of U2000 license file in the Solaris or SUSE Linux OS is **/opt/U2000/server/etc/conf/license**.
- The default path of U2000 license file in the Windows OS is **D:\U2000\server\etc\conf\license**.
- In the Solaris or SUSE Linux OS: You should transfer the updated license file on the primary site to the server on the secondary site in text mode, that is, ASCII mode. In the Windows OS: Copy and paste the updated license file on the primary site to the the server on the secondary site.

----End

Result

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

3.4 Checking the Status of the U2000 License

This topic describes how to check the status of the U2000 license. By checking the license status, you can learn the usage of the license, so as to apply for a new license file from Huawei in time before the NMS needs to be expanded or the validity of the license is due.

Procedure

- 1 Log in to the U2000 Client.
- 2 Choose **Help > License Information**.
- 3 In the **License Information** dialog box that is displayed to view the condition of the license.

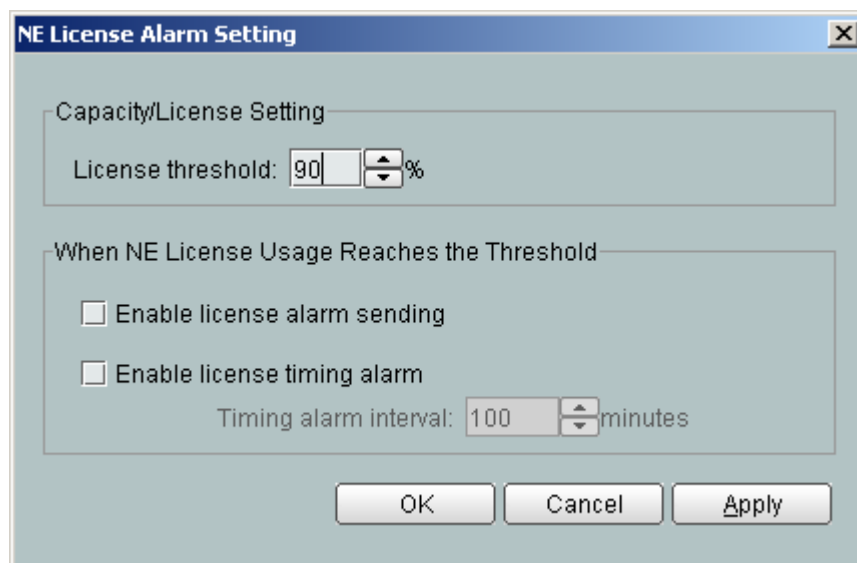
----End

3.5 Setting the Threshold of the Accessing NEs

When the number of accessing NEs reaches the preset threshold, the U2000 sends an NE license alarm and displays an **Information** dialog box periodically.

Procedure

- 1 Choose **Administration > Settings > NE License Alert** from the main menu.



- 2 In the **NE License Alarm Setting** dialog box, enter the license threshold in **License threshold**.
- 3 Select the **Enable license alarm sending** check box to enable the function of sending the license alarms.
- 4 Select the **Enable license timing alarm** check box and set the interval of sending the alarms.
- 5 Click **OK**.

----End

3.6 Verifying the U2000 License

Introduce how to correctly use a U2000 License.

Context

NOTE

Do not modify the name, the content, or the format of the license file. Otherwise the license will be invalid.

If the license file is invalid, follow the procedure described as follows to check the correctness of the license.

Procedure

- Check the correctness of the license on Solaris.

Check whether the text mode, namely ASCII mode, is adopted to transfer the license file.

NOTE

To check the transfer mode, open the **licenseXXXXXX.dat** file at the workstation by the **vi** command. If every line is ended with "^M", it indicates that the transfer mode is incorrect, and the transfer should be repeated in the mode of ASCII.

- Check the correctness of the license on SUSE Linux.

Check whether the text mode, namely ASCII mode, is adopted to transfer the license file.



NOTE

To check the transfer mode, open the **licenseXXXXXX.dat** file at the workstation by the **vi** command. If every line is ended with "**^M**", it indicates that the transfer mode is incorrect, and the transfer should be repeated in the mode of ASCII.

- Check the correctness of the license on Windows.
 - Check whether the network adapter is available or not.
If not, the MAC address cannot be detected, and the license will be invalid.
 - Check whether there is any error during the transfer of the license.
If yes, re-transfer the license file and store it in the D:\U2000\server\etc\conf\license directory. Re-activate the U2000 to see whether it is valid.

----End

4 Security Management

About This Chapter

Security management is a crucial function to prevent unauthorized logins and ensure network data security. Security management includes the NM user management, NE user management, and security log management.

[4.1 Security Management Strategy](#)

The security management function provides the management for the U2000 and NEs. With this function, the U2000 can also monitor in real time the users that already log in to the U2000 and NEs. In this way, the network and data security ensures that login failures or illegal operations are captured.

[4.2 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.

[4.3 Creating U2000 Users and Assigning Permissions](#)

This topic describes a user of the SMMangers group to create U2000 users and assign rights to them.

[4.4 Comparing the U2000 User Rights](#)

By comparing the rights of two U2000 users, a user of the SMMangers group can understand the differences between their rights.

[4.5 Querying the Authorization](#)

In the U2000, a user of the SMMangers group can query the users or user groups that certain operation rights are assigned to.

[4.6 Modifying a U2000 User](#)

This topic describes a user of the SMMangers group to modify the password, general properties, managed domain, and operation rights of the U2000 user.

[4.7 Managing U2000 Object Sets](#)

This topic describes a user of the SMMangers group to create, modify, and delete object sets.

[4.8 Managing U2000 Operation Sets](#)

This topic describes how to create, modify, and delete operation sets.

[4.9 Monitoring a U2000 User](#)

This topic describes how to monitor U2000 user sessions and operations, force U2000 users to exit, unlock U2000 user accounts and send messages to online users.

[4.10 Managing the Remote Maintenance User](#)

The U2000 remote maintenance function allows login to the U2000 server from a remote maintenance terminal. Strict management for the remote maintenance user not only ensures U2000 system security, but also makes maintenance operations easier.

[4.11 Managing NE Users](#)

To ensure NE data security, you can manage the authorities and passwords for NE users.

[4.12 Managing NE Login](#)

To ensure NE data security, you can manage the users who are logged in to NEs.

[4.13 Setting the Security Access of an NE](#)

To ensure the NE security, you need to disable the unused interfaces on the NE.

[4.14 Setting the NE ACL](#)

You can ensure the security of NEs by setting the NE ACL.

[4.15 Auditing Changes](#)

If changes occur on a device in the network, you can query information about the changes through U2000.

[4.16 NE License Management](#)

By using the NE license management function, you can query, apply for, install, and change NE licenses. In addition, you can adjust capacities in licenses. By setting licenses for NEs, you can obtain the rights to use certain functions according to service requirements. Because licenses control NE validity periods or functions, you can understand the NE status in real time and perform operations properly by using the license management function. Currently, only certain versions of the OSN equipment, NG WDM equipment, OptiX PTN 910, and OptiX PTN 950 support this function.

4.1 Security Management Strategy

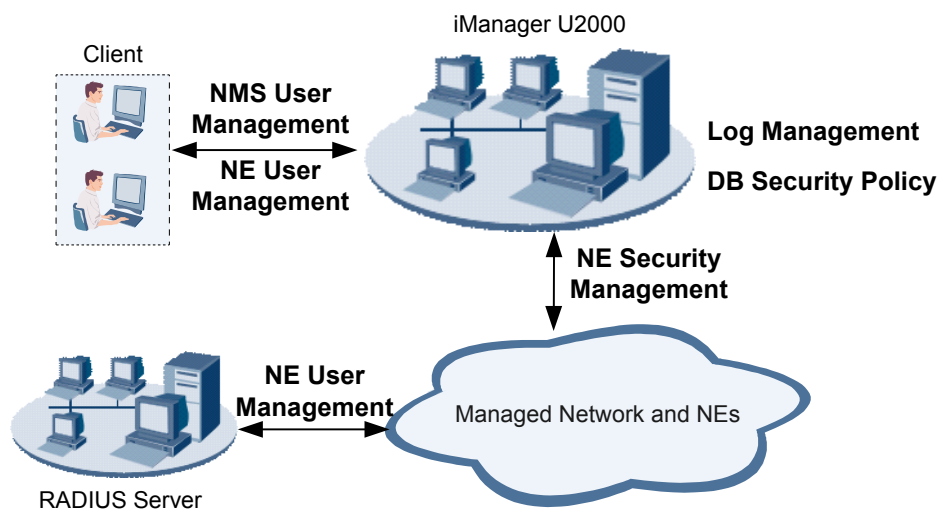
The security management function provides the management for the U2000 and NEs. With this function, the U2000 can also monitor in real time the users that already log in to the U2000 and NEs. In this way, the network and data security ensures that login failures or illegal operations are captured.

The U2000 security management includes NM user management, NE user management, NM login management, NE login management, and log management. Before using the U2000, you must create an NM user, and specify what authority the user has, what equipment the user is able to operate on, and what clients the user is allowed to log in to. If you want to operate on NEs, you must also create an NE user and assign its authority. With NM user management and NE user management, the user is only able to perform authorized operations on specified NEs and through specified clients.

With NM login management, NE login management and log management, the administrator can monitor in real time the users that already log in to the U2000 or NEs, and force the logged-in users at any time to log out of the U2000 or NEs.

Figure 4-1 shows the mechanism for implementing security management.

Figure 4-1 Implementation of security management



NOTE

For details about the Log management and database security policy, see chapter "Log Management" and "Backing Up and Restoring the U2000 Database".

4.1.1 User Security Policy

The U2000 security management mainly involves the objects management, password management, access control management, and role-based and domain-based management.

4.1.2 Log Management Policy

Log security management includes the U2000 operation log, U2000 security log, NE security log, log dump, and log forwarding management.

4.1.3 Database Security Policy

The U2000 data is saved in the database. Therefore, ensure the database security with priority, including protecting the security of the database password, backing up the database periodically, viewing the database status, and dumping the database.

4.1.4 NE Security Management

The NE security management includes NE access control, NE user management, NE operation right management and NE data security management.

4.1.1 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 SMManger 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.

 NOTE

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.

4.1.2 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.

4.1.3 Database Security Policy

The U2000 data is saved in the database. Therefore, ensure the database security with priority, including protecting the security of the database password, backing up the database periodically, viewing the database status, and dumping the database.

To ensure the database security, you can take measures as follows:

- To ensure security of the database password, change the password regularly. After the U2000 is installed, database users sa and NMSuser are automatically created.
- Back up the database periodically. Copy each backup file to other storage devices. In the case of a U2000 or database fault, you can use the backup database for restoration. In general situations, do as follows:
 - Back up all databases of the U2000 once a week at scheduled time. For details of the operation method, refer to [5.4.1 Periodically Backing Up the U2000 Data to a Local Server Through the U2000 Client](#) and [5.5.1 Periodically Backing Up the U2000 Database to a Remote Server Through the U2000 Client](#).
- View the database status and dump the database periodically.

4.1.4 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.

4.2 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.

4.2.1 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.

4.2.2 Setting the Access Control List

By setting the system or current user access control list (ACL), a user of the SMMangers can allow the client or user to log in to the U2000 from the computer with specified IP address or network segment.

4.2.3 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.

4.2.4 Setting the Account Policy

A user of the SMMangers group can set the account policy to ensure account security.

4.2.1 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.

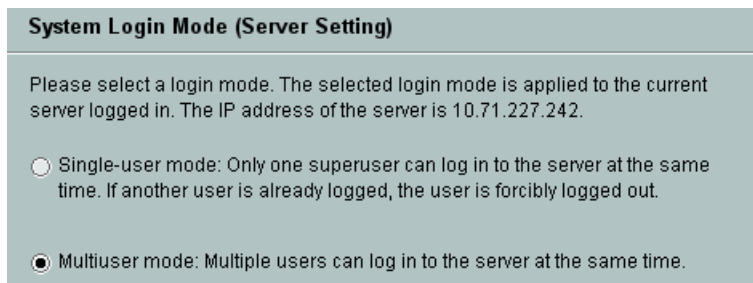


CAUTION

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

4.2.2 Setting the Access Control List

By setting the system or current user access control list (ACL), a user of the SMMangers 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

4.2.3 Setting the Password Policy

To improve U2000 security, a user of the SManagers 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

4.2.4 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

4.3 Creating U2000 Users and Assigning Permissions

This topic describes a user of the SMMangers group to create U2000 users and assign rights to them.

4.3.1 Procedure for Creating U2000 Users

This topic describes how to create U2000 users after the initial installation of the U2000 and during routine maintenance.

4.3.2 Creating an Object Set

Devices and device services can be allocated and managed in a unified manner based on object sets.

4.3.3 Creating an Operation Set

The operation set is a collection of operations. Permissions on devices and applications can be assigned and managed in a unified manner based on operation sets.

4.3.4 Creating a U2000 User Group

A user of the SMMangers group can create a U2000 user group. The users with the same permissions assigned belong to the same user group. After you set the managed domain and operation rights for a user group, all users in this group have the rights. This helps you to assign rights to multiple users conveniently.

4.3.5 Creating a U2000 User Account

A user of the SMMangers group can create a user account of the U2000 and assign rights to U2000 users based on their responsibilities.

4.3.6 Example for Creating User Accounts and Assigning Rights in the Authority- and Domain-based Management Scenario

This topic provides the example for creating user accounts and assigning rights in the authority- and domain-based management scenario.

4.3.1 Procedure for Creating U2000 Users

This topic describes how to create U2000 users after the initial installation of the U2000 and during routine maintenance.

Scenario	Procedure	Description
Operations performed after the initial installation of the U2000 is successful	1. Creating an Object Set 2. Creating an Operation Set 3. Creating an iMAP User Group 4. Assigning the Managed Domain for a U2000 User Group 5. Assigning Operation Rights to a U2000 User Group 6. Creating a U2000 User Account 7. Adding a U2000 User to a User Group 8. Assigning the Managed Domain for a U2000 User 9. Assigning Operation Rights to a U2000 User 10. Assigning the User ACL	In this scenario, the object sets, operation sets, and user groups have not been created and configured. Therefore, you need to create and configure them before creating users.
Operations performed during routine maintenance of the U2000	1. Creating a U2000 User Account 2. Adding a U2000 User to a User Group	In this scenario, the object sets, operation sets, and user groups are already created and configured. Therefore, you need to create U2000 users and add them to the user groups only.

4.3.2 Creating an Object Set

Devices and device services can be allocated and managed in a unified manner based on object sets.

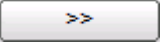
Context

- Object sets can be allocated to users or user groups.
- If an object set is allocated to a user group, all members in the user group have the permissions of the object included in the object set.
- The U2000 provides default object set: **AllObjects**. The **AllObjects** contains all security objects.

Procedure

- 1 Choose **Administration > NMS Security > NMS User Management** from the main menu.
- 2 In the **NMS User Management** navigation tree, right-click the **Object Set** node and then choose **New Object Set**. Otherwise, click  on the toolbar of the navigation tree, choose **New Object Set**.

- 3 In the **New Object Set** dialog box, set the properties of the new Object set.

Properties of Object Set	Operations
Details of Object set	On the Details tab, enter the name, type, and description of the new Object set. NOTE Name is mandatory.
Members of Object set	On the Members tab, perform the following operations: - Click Select. - Select an devices or object set, and move it to Selected devices and object sets. - You can click  to move all devices and object sets to Selected devices and object sets. - You can select devices or object sets from the Available devices and object sets navigation tree, and then click  to move the selected devices or object sets to Selected devices and object sets. - Click OK.

 NOTE

Click **Copy member from Object Set**. In the **Copy member from Object Set** dialog box, select object sets and copy the permissions of these object sets.

- 4 In the **New Object Set** dialog box, click **OK**.

----End

4.3.3 Creating an Operation Set

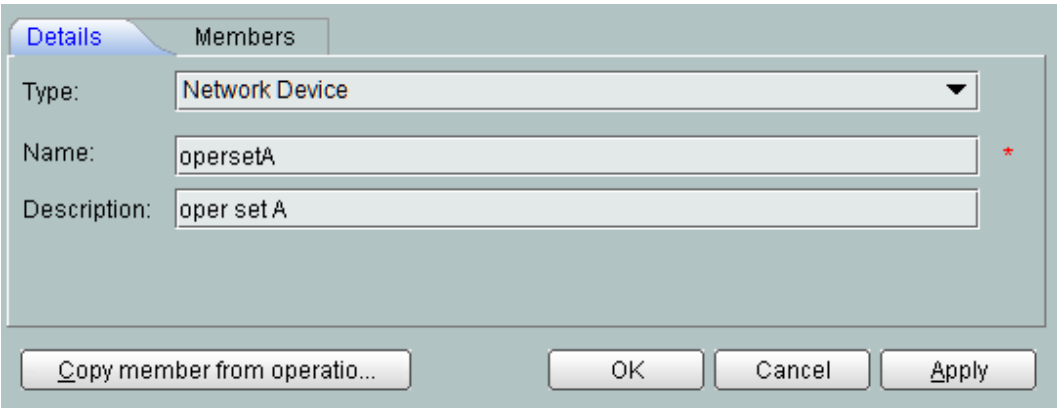
The operation set is a collection of operations. Permissions on devices and applications can be assigned and managed in a unified manner based on operation sets.

Context

- Operation sets can be allocated to users or user groups.
- If an operation set is allocated to a user group, all members in the user group have the permissions of the operations included in the operation set.
- **AllApplicationOperations** and **AllObjectOperations** are default operation sets provided by the U2000. **AllObjectOperations** is the operation set of network devices. **AllApplicationOperations** is the operation set of network management applications.

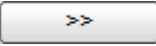
Procedure

- 1 Choose **Administration > NMS Security > NMS User Management** from the main menu.
- 2 In the **NMS User Management** navigation tree, right-click the **Operation Set** node and then choose **New Operation Set**. Otherwise, click  on the toolbar of the navigation tree, choose **New Operation Set**.



- 3 In the **New Operation Set** dialog box, set the properties of the new operation set.

Properties of Operation Set	Operations
Details of Operation set	On the Details tab, enter the type, name, and description of the new operation set. NOTE Name is mandatory.

Properties of Operation Set	Operations
Members of Operation set	On the Members tab, perform the following operations: - Click Select. - Select an operation or operation set, and move it to Selected Rights. - You can click  to move all operations and operation sets to Selected Rights. - You can select operations or operation sets from the Available Rights navigation tree, and then click  to move the selected operations or operation sets to Selected Rights. - Click OK.

**NOTE**

Click **Copy member from operation set**. In the **Copy member from operation set** dialog box, select operation sets and copy the members of these operation sets.

- In the **New Operation Set** dialog box, click **OK**.

----End

4.3.4 Creating a U2000 User Group

A user of the SMManagers group can create a U2000 user group. The users with the same permissions assigned belong to the same user group. After you set the managed domain and operation rights for a user group, all users in this group have the rights. This helps you to assign rights to multiple users conveniently.

Procedure

- Choose **Administration > NMS Security > NMS User Management** from the main menu.
- In the **NMS User Management** navigation tree, right-click the **User Group** node and choose **New User Group**.

3 In the **New User Group** dialog box, set the properties of the new user group.

You must manually set the name of the user group. For the other properties of user group, you can set them after you create the user group successfully.

User Group Properties	Operations
User group name information	On the Details tab, set the user group name, description, type and maximum sessions.
Members of user group	- To add members, on the Details tab, click Add. In the Add User dialog box, set the members to be added to the user group. - To delete members, on the Details tab, select the members to be deleted from Members, and then click Delete.
Management domain of user group	On the Domain tab, click Select . In the Select Domain dialog box, set the management domain of the user group, and then click OK .
Operation permissions of user group	On the Operation Rights tab, click Select , in the Select Operation Rights dialog box, set the operation rights of the user group, and then click OK .

 NOTE

Click **Copy Rights from User Group**. In the **Copy Rights from User Group** dialog box, select user groups and copy the management domain rights and operation permissions of these user groups.

- 4 In the **New User Group** dialog box, click **OK**.

----End

4.3.5 Creating a U2000 User Account

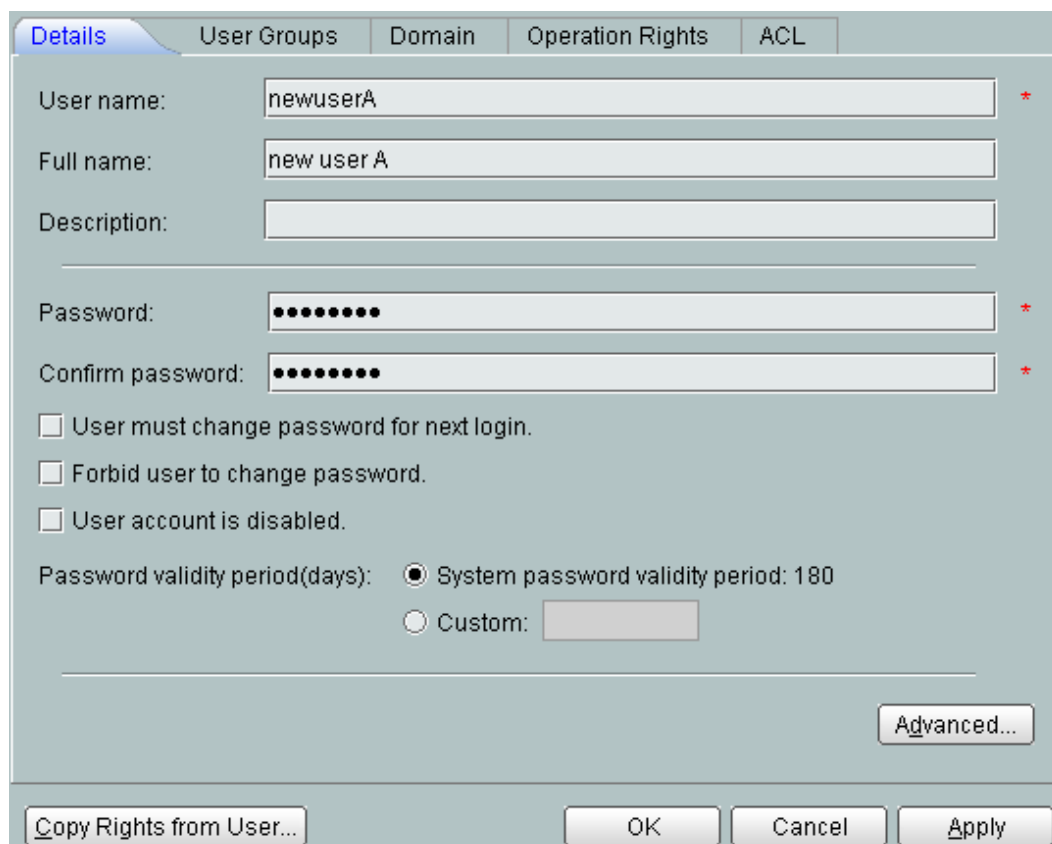
A user of the SMMangers group can create a user account of the U2000 and assign rights to U2000 users based on their responsibilities.

Context

When you create a U2000 user, the property settings must comply with the password policy and the account policy. For details about how to set a password policy and an account policy, see [4.2.3 Setting the Password Policy](#) and [4.2.4 Setting the Account Policy](#).

Procedure

- 1 Choose **Administration > NMS Security > NMS User Management** from the main menu.
- 2 In the **NMS User Management** navigation tree, right-click the **User** node and choose **New User**.



- 3 In the **New User** dialog box, set the properties of the new user.

You must manually set the user name and password. For the other properties, you can use default values or set them after you create the user account successfully.

User Properties	Operations
Normal properties	On the Details tab, set user properties, such as user name, description content, and password.
Owner group	- To add owner groups, on the User Groups tab, click Add, select the user groups to which you want to add the user. NOTE Only users of the the SMManagers group can view their own rights. - To delete owner groups, on the User Groups tab, select the user groups to be deleted from the user group list, and then click Delete.
Management domain of user	On the Domain tab, click Select . In the Select Domain dialog box, set the management domain of the user.
Operation rights of user	On the Operation Rights tab, click Select . In the Select Operation Rights dialog box, set operation rights of the user.
Access control list (ACL)	On the ACL tab, set the ACL for the user.

 NOTE

Click **Copy Rights from User**. In the **Copy Rights from User** dialog box, select user groups and copy the management domain rights and operation permissions of these users.

4 In the **New User** dialog box, click **OK**.

----End

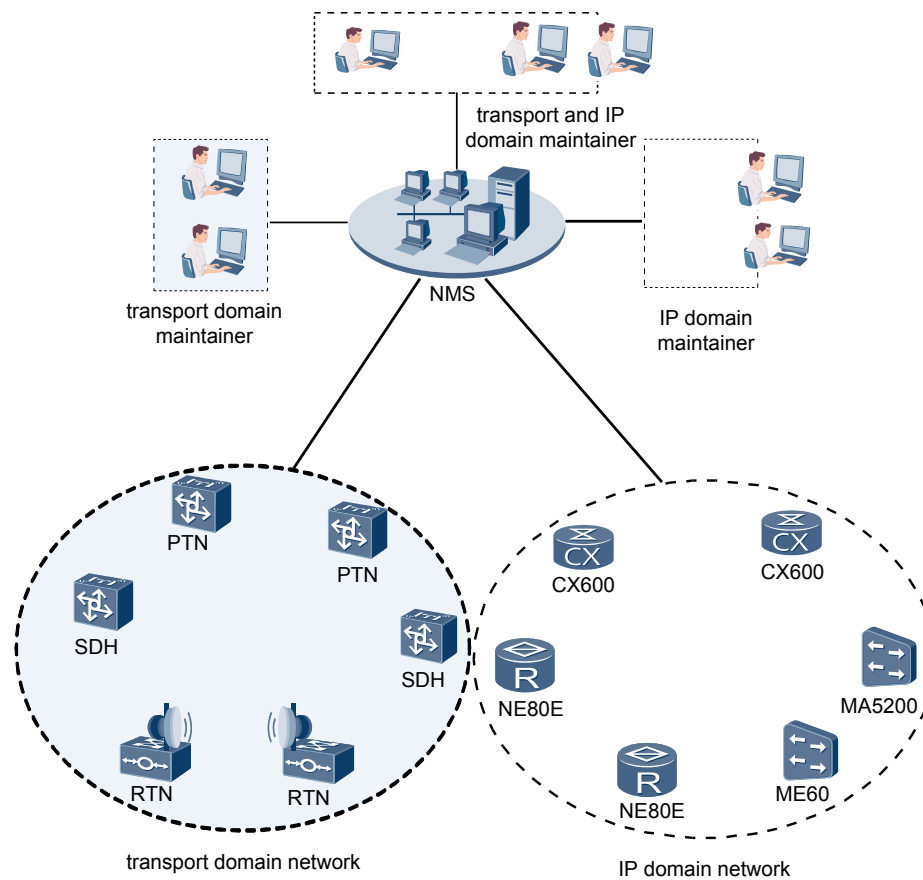
4.3.6 Example for Creating User Accounts and Assigning Rights in the Authority- and Domain-based Management Scenario

This topic provides the example for creating user accounts and assigning rights in the authority- and domain-based management scenario.

Application Scenario

Create a new office. Monitor and manage NEs in the new office through the U2000 in a centralized manner. The NEs are divided into two parts according to the NE domain (transport domain or IP domain), and are monitored and maintained separately. To enable different users to monitor and maintain NEs through the U2000, associated U2000 user accounts and rights need to be assigned to them.

Figure 4-2 shows the networking.

Figure 4-2 Networking of authority and domain-based management

Data Planning

Plan the following subnets according to the NE domain:

- Transport domain subnet: All managed transport NEs are included.
- IP domain subnet: All managed IP NEs are included.

Plan four user groups according to user group types:

User Group Type	User Group Name	Responsibility	Management Domain	Operation Right
Transport domain maintainer group	T2000group-admin	Responsible for maintaining NEs in the transport domain.	NEs in the transport domain	Operation set of the transport domain NE maintainer Operation set of the transport domain service maintainer

User Group Type	User Group Name	Responsibility	Management Domain	Operation Right
Transport domain monitor group	T2000group-view	Responsible for monitoring NEs in the transport domain.	NEs in the transport domain	Operation set of the transport domain NE monitor Operation set of the transport domain service monitor
IP domain maintainer group	DMSgroup-admin	Responsible for maintaining NEs in the IP domain.	NEs in the IP domain	Operation set of the IP domain NE maintainer Operation set of the IP domain service maintainer
IP domain monitor group	DMSgroup-view	Responsible for monitoring NEs in the IP domain.	NEs in the IP domain	Operation set of the IP domain NE monitor Operation set of the IP domain service monitor

**NOTE**

The operation sets listed in the **Operation Right** column refer to general operation sets associated with NEs in the transport and IP domains. Determine the actual operation sets to be added according to the types of managed NEs and the operation rights of user groups.

Plan the seven users according to user responsibilities:

User Type	User Name	Responsibility	User Group
Transport domain maintainer	T2000-admin	Responsible for maintaining NEs in the transport domain.	Transport domain maintainer group
Transport domain monitor	T2000-view	Responsible for monitoring NEs in the transport domain.	Transport domain monitor group
IP domain maintainer	DMS-admin	Responsible for maintaining NEs in the IP domain.	IP domain maintainer group
IP domain monitor	DMS-view	Responsible for monitoring NEs in the IP domain.	IP domain monitor group

User Type	User Name	Responsibility	User Group
Transport domain maintainer & IP domain monitor	T2000-admin-DMS-view	Responsible for maintaining NEs in the transport domain and monitoring NEs in the IP domain.	Transport domain maintainer group and IP domain monitor group
IP domain maintainer & transport domain monitor	DMS-admin-T2000-view	Responsible for maintaining NEs in the IP domain and monitoring NEs in the transport domain.	IP domain maintainer group and Transport domain monitor group
Transport domain monitor & IP domain monitor	T2000-view-DMS-view	Responsible for maintaining NEs in the transport and IP domains.	Transport domain monitor group and IP domain monitor group

Configuration Process

on the U2000, do as follows to create a user account and assign associated rights:

1. Create subnets.
Create a transport domain subnet and an IP domain subnet, and add NEs in the transport and IP domains to the subnets.
2. Create user groups and assign management domains and operation sets of the user groups.
You can easily assign rights to multiple users by using the user group function.
 - According to responsibilities of user groups, configure management domains of the user groups so that different user groups can manage different NE domains.
 - According to responsibilities of user groups, configure operation rights of the user groups so that different user groups have different operation rights.
 For details about how to create a user group, see [4.3.4 Creating a U2000 User Group](#).
3. Create user accounts.
Create user accounts according to actual personnel condition, and configure user groups according to responsibilities of users. Then, each user account has the management domain and operation rights of the user group.
For details about how to create a user account, see [4.3.5 Creating a U2000 User Account](#).

 NOTE

When creating user accounts, do as follows to ensure the security of the U2000:

- Set different login times based on the shifts.
- Bind IP addresses of area workstations to users.
- Change the user password when you are logging in for the first time.

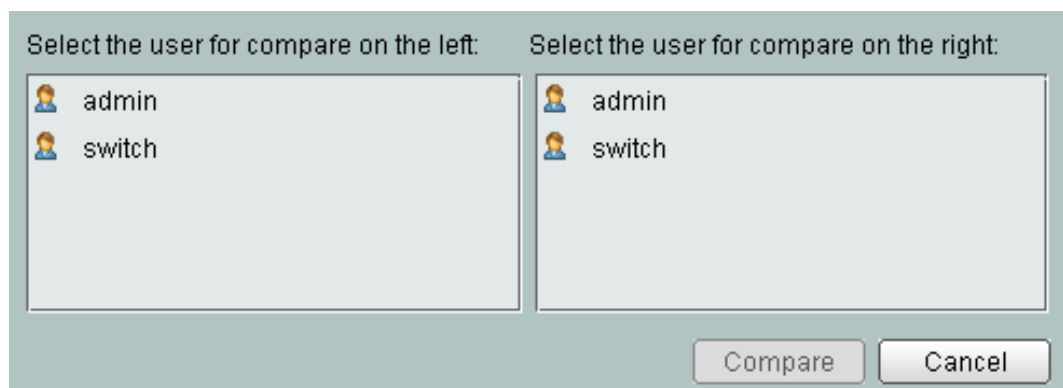
When the configuration is complete, the administrator can provide the accounts to relevant personnel.

4.4 Comparing the U2000 User Rights

By comparing the rights of two U2000 users, a user of the SMMangers group can understand the differences between their rights.

Procedure

- 1 Choose **Administration > NMS Security > NMS User Management** from the main menu.
- 2 On the top of the **NMS User Management** navigation tree click .



- 3 In the **Select User for Compare** dialog box, select a user from the left and right group boxes respectively.

 NOTE

On the U2000, you cannot compare the same user. If you select the same user in the left and right areas, the **Compare** button becomes unavailable.

- 4 Click **Compare**.

In the **Compare User Rights Result** dialog box, the U2000 can display user rights in the following two modes:

- **Display all rights:** All user rights are displayed in the group box.
- **Display only differences:** Only the differences between user rights are displayed in the group box.

----End

4.5 Querying the Authorization

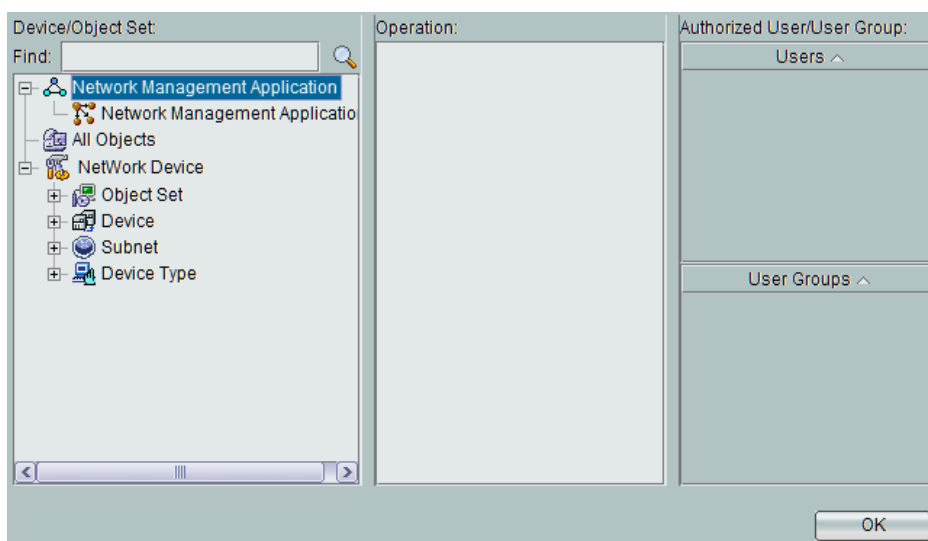
In the U2000, a user of the SMMangers group can query the users or user groups that certain operation rights are assigned to.

Context

The Administrators group contains all U2000 operation rights except the security management rights. In the query authorization dialog box, if you select an operation node or operation set node, the **Authorized User/User Group** area always displays the information that the operation rights are assigned to the Administrator group.

Procedure

- 1 Choose **Administration > NMS Security > NMS User Management** from the main menu.
- 2 On the top of the **NMS User Management** navigation tree, click .



- 3 In the **Authorization Details** dialog box, expand the root node or parent node in the navigation tree, and select a node.
After selection, the corresponding operations or operation sets are displayed in the **Operation** area.
- 4 In the **Operation** area, expand the root node or parent node, and then select an operation.
On the right of the interface, the users and user groups that the operation rights are assigned to are displayed in the **Authorization User/User Group** area.

----End

4.6 Modifying a U2000 User

This topic describes a user of the SMMangers group to modify the password, general properties, managed domain, and operation rights of the U2000 user.

4.6.1 Resetting the Password of a U2000 User

This topic describes how the user in SMMangers reset the password of a U2000 user.

4.6.2 Modifying an Object Set

A user of the SMMangers group can modify the common properties of the specified object set, add or delete members of a object set.

4.6.3 Modifying an Operation Set

A user of the SMMangers group can modify an operation set, such as the name and description of an operation set. You can also add operations to an operation set, or delete operations from an operation set.

4.6.4 Modifying a User Group

This topic describes a user of the SMMangers group to modify the basic information about a U2000 user group, permissions, and manageable devices.

4.6.5 Modifying the Information About a U2000 User

This topic describes a user of the SMMangers group to modify the basic information about a U2000 user, permissions, and manageable devices.

4.6.1 Resetting the Password of a U2000 User

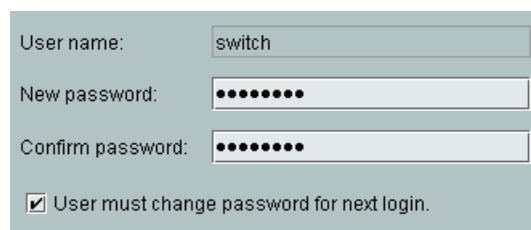
This topic describes how the user in SMMangers reset the password of a U2000 user.

Context

- The password setting must comply with the password policy. For details on how to set a password policy, see [4.2.3 Setting the Password Policy](#).
- The **SMMangers** user can reset the passwords of other users (excluding the admin user). The password of the admin can be changed by only the admin through the U2000 client.
- If you forget your password, contact the user in SMMangers to reset the password.

Procedure

- 1 Choose **Administration > NMS Security > NMS User Management** from the main menu.
- 2 In the **NMS User Management** navigation tree, expand the **User** node. Right-click the user whose password is to be reset and choose **Reset Password**.



- 3 In the **Reset Password** dialog box, set **New Password** and **Confirm Password**, and then click **OK**.

NOTE

If **User must change password for next login** is selected, you need to change the password when you log in to the U2000 next time. Otherwise, you need not to change the user password when you log in to the U2000 next time.

- 4 In the displayed dialog box, click **OK**.

----End

4.6.2 Modifying an Object Set

A user of the SMMangers group can modify the common properties of the specified object set, add or delete members of a object set.

Context

- You are not allowed to change names, type and members of the default object sets.
- Only the users in Sub Domain User Group and SMManagers Group have the right to modify object sets.

Procedure

- 1 Choose **Administration > NMS Security > NMS User Management** from the main menu.
- 2 In the **NMS User Management** navigation tree, expand the **Object Set** node, and then select the object set to be modified.

The screenshot shows a web interface with three tabs: 'Details', 'Members', and 'Applicable for'. The 'Details' tab is active. It contains three input fields: 'Type' with a dropdown menu showing 'VPN Series', 'Name' with a text box containing 'Device_Set', and 'Description' with a text box containing 'Device_Set'.

- 3 In the area on the right , select a tab to modify the information about the object set.

Modifying a Object Set	Operations
Modify normal properties	Click the Details tab. In the list on the right, modify the name and description of the object set. At the bottom of the list box, click Apply .
Modify members of a object set	Click the Members tab. At the bottom of the tab, click Select . In the Select Object Set Member dialog box, set the object set member, and then click OK .
View the users or user groups served by an object set	On the Applicable for tab, you can view only the users or user groups served by the object set. The Applicable for tab displays the users or user groups served by the object set. NOTE To allocate a object set to a user or user group, do as follows: 1. Expand the User or User Group node and choose a user or user group. 2. Click the Domain tab on the right of the interface. 3. Click Select. In Select, select a object set and move it to Selected device and object sets. 4. Click OK.

----End

4.6.3 Modifying an Operation Set

A user of the SMMangers group can modify an operation set, such as the name and description of an operation set. You can also add operations to an operation set, or delete operations from an operation set.

Prerequisite

Operation sets and operation permissions are already created on the U2000.

Context

- You cannot modify the default operation set.
- Only the users in Sub Domain User Group and Security Manager User Group have the right to modify operation sets.

Procedure

- 1 Choose **Administration > NMS Security > NMS User Management** from the main menu.
- 2 In the **NMS User Management** navigation tree, expand the **Operation Set** node, and then select the operation set to be modified.



- 3 In the area on the right, select a tab to modify the information about the operation set.

Modifying an Operation Set	Operations
Modify normal properties	Click the Details tab. Modify the operation set name and description (the type of operation set cannot be changed). After modification, click Apply .
Set members of a operation set	Click the Members tab. At the bottom of the tab, click Select . In the Select Operation Set Member dialog box, set the member of the operation set, and then click OK .

Modifying an Operation Set	Operations
Set parameters on the Applicable for tab page	On the Applicable for tab, you can view only the users or user groups served by the operation set. The Applicable for tab displays the users or user groups served by the operation set.
Allocate an operation set	To allocate an operation set to a user or user group, do as follows: 1. Expand the User or User Group node and choose a user or user group. 2. Click the Domain tab on the right of the interface. Click Select. 3. In the displayed Select Domain dialog box, add a object set to the user or user group. Click OK. 4. Click the Operation Rights tab on the right of the window. Click Select. 5. Select network device operations or network management applications. ● Network Device In the Select Operation Rights dialog box, select a operation set. In the Operations area, select the corresponding operation set. ● Network Management Application In the Select Operation Rights dialog box, choose Network Management Application in the navigation tree of authorized objects. In the Operations area, select the corresponding operation set. 6. Click  to move the selected operation set to Selected Rights. 7. Click Ok.

----End

4.6.4 Modifying a User Group

This topic describes a user of the SMManagers group to modify the basic information about a U2000 user group, permissions, and manageable devices.

Procedure

- 1 Choose **Administration > NMS Security > NMS User Management** from the main menu.
- 2 On the top of the **NMS User Management** navigation tree, expand the **User Group** node. Select the user group to the modified.

The screenshot shows the 'Details' tab of a user group configuration window. The 'Name' field contains 'switch'. The 'Description' field is empty. The 'User Group Type' is set to 'Common User Group'. The 'Maximum Sessions' is set to 100, with an 'Unlimited' checkbox that is currently unchecked.

- 3 In the area on the right , select a tab to modify the information about the user group.

Modify Properties	Operation
Modify general properties	Click the Details tab. Modify the user group name, maximum sessions and description (the type of user group cannot be changed). After modification, click Apply .
Modify members	To add users, click Add on the Members tab. In Add User , add users. To delete users, select the user group and then click Delete . On the Members tab, view the users that belong to the user group.
Modify the managed domain	On the Domain tab, click Select . In Select Domain dialog box, add or delete devices or object sets.
Modify operation rights	On the Operation Rights tab, click Select . In Select Operation Rights dialog box, add or delete the permissions to operate network management applications and network device operate sets.
Query current sessions	Click the Current Session tab to view the online users of the user group.

----End

4.6.5 Modifying the Information About a U2000 User

This topic describes a user of the SMMangers group to modify the basic information about a U2000 user, permissions, and manageable devices.

Procedure

- 1 Choose **Administration** > **NMS Security** > **NMS User Management** from the main menu.
- 2 In the **NMS User Management** navigation tree, expand the **User** node.

The screenshot shows the 'Details' tab of a user management interface. It contains several input fields and dropdown menus for configuring a user. The 'User name' field is filled with 'switch'. The 'User type' dropdown is set to 'Local User'. The 'User must change password for next login', 'Forbid user to change password', and 'User account is disabled' dropdowns are all set to 'No'. The 'Password validity period(days)' field is set to 'System password validity period'.

- 3 Select the user whose information you want to modify, and then modify the information about this user on a tab in the right area.

Modify Properties	Operation
Modify general properties	Perform operations on the Details tab, modify user information(The dimmed controls are unavailable).
Change the owner user group	To add a user group, click Add on the User Groups tab. In Add User Group , add a user group. To delete a user group, click Delete .
Modify the managed domain	On the Domain tab, click Select . In Select Domain , you can perform the following operations: ● Add objects or object sets. ● Delete objects or object sets.
Modify operation rights	On the Operation Rights tab, click Select . In Select Operation Rights , you can perform the following operations: ● Add the permissions to operate NMS applications, object, object sets and so on. ● Delete the permissions to operate NMS applications, object, object sets and so on.
Modify the ACL	To set the IP addresses that the user can access, select Use all the ACLs in the system and Use the specified ACLs on the ACL tab. To add, modify, or delete IP addresses or network segments, select ACL .

----End

4.7 Managing U2000 Object Sets

This topic describes a user of the SMMangers group to create, modify, and delete object sets.

4.7.1 U2000 Object Set

This topic describes the basic meaning and function of the object set.

4.7.2 Creating an Object Set

Devices and device services can be allocated and managed in a unified manner based on object sets.

4.7.3 Modifying an Object Set

A user of the SMMangers group can modify the common properties of the specified object set, add or delete members of a object set.

4.7.4 Deleting an Object Set

The object set used no longer must be deleted immediately by a user of the SMMangers group.

4.7.1 U2000 Object Set

This topic describes the basic meaning and function of the object set.

The object set is a collection of manageable devices and device services. By default, the U2000 provides **AllObjects**. If a user or user group can manage an object set, it indicates that the user or user group can manage all the objects in the object set.

The administrator can create a object set, add objects that can be managed in a centralized manner to the object set, and specify a user or user group to manage the objects in the object set. In this way, the management cost of the administrator can be reduced.

4.7.2 Creating an Object Set

Devices and device services can be allocated and managed in a unified manner based on object sets.

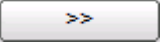
Context

- Object sets can be allocated to users or user groups.
- If an object set is allocated to a user group, all members in the user group have the permissions of the object included in the object set.
- The U2000 provides default object set: **AllObjects**. The **AllObjects** contains all security objects.

Procedure

- 1 Choose **Administration > NMS Security > NMS User Management** from the main menu.
- 2 In the **NMS User Management** navigation tree, right-click the **Object Set** node and then choose **New Object Set**. Otherwise, click  on the toolbar of the navigation tree, choose **New Object Set**.

- 3 In the **New Object Set** dialog box, set the properties of the new Object set.

Properties of Object Set	Operations
Details of Object set	On the Details tab, enter the name, type, and description of the new Object set. NOTE Name is mandatory.
Members of Object set	On the Members tab, perform the following operations: - Click Select. - Select an devices or object set, and move it to Selected devices and object sets. - You can click  to move all devices and object sets to Selected devices and object sets. - You can select devices or object sets from the Available devices and object sets navigation tree, and then click  to move the selected devices or object sets to Selected devices and object sets. - Click OK.

 NOTE

Click **Copy member from Object Set**. In the **Copy member from Object Set** dialog box, select object sets and copy the permissions of these object sets.

- 4 In the **New Object Set** dialog box, click **OK**.

----End

4.7.3 Modifying an Object Set

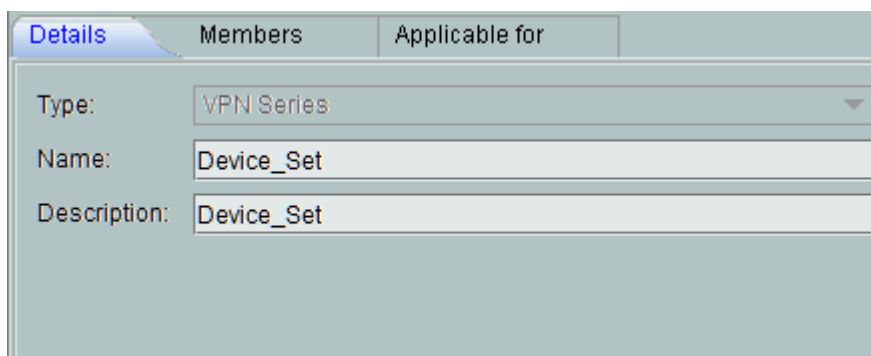
A user of the SMMangers group can modify the common properties of the specified object set, add or delete members of a object set.

Context

- You are not allowed to change names, type and members of the default object sets.
- Only the users in Sub Domain User Group and SMManagers Group have the right to modify object sets.

Procedure

- 1 Choose **Administration > NMS Security > NMS User Management** from the main menu.
- 2 In the **NMS User Management** navigation tree, expand the **Object Set** node, and then select the object set to be modified.



The screenshot shows a web interface with three tabs: 'Details', 'Members', and 'Applicable for'. The 'Details' tab is active. It contains three input fields: 'Type' with a dropdown menu showing 'VPN Series', 'Name' with a text box containing 'Device_Set', and 'Description' with a text box containing 'Device_Set'.

- 3 In the area on the right , select a tab to modify the information about the object set.

Modifying a Object Set	Operations
Modify normal properties	Click the Details tab. In the list on the right, modify the name and description of the object set. At the bottom of the list box, click Apply .
Modify members of a object set	Click the Members tab. At the bottom of the tab, click Select . In the Select Object Set Member dialog box, set the object set member, and then click OK .
View the users or user groups served by an object set	On the Applicable for tab, you can view only the users or user groups served by the object set. The Applicable for tab displays the users or user groups served by the object set. NOTE To allocate a object set to a user or user group, do as follows: 1. Expand the User or User Group node and choose a user or user group. 2. Click the Domain tab on the right of the interface. 3. Click Select. In Select, select a object set and move it to Selected device and object sets. 4. Click OK.

----End

4.7.4 Deleting an Object Set

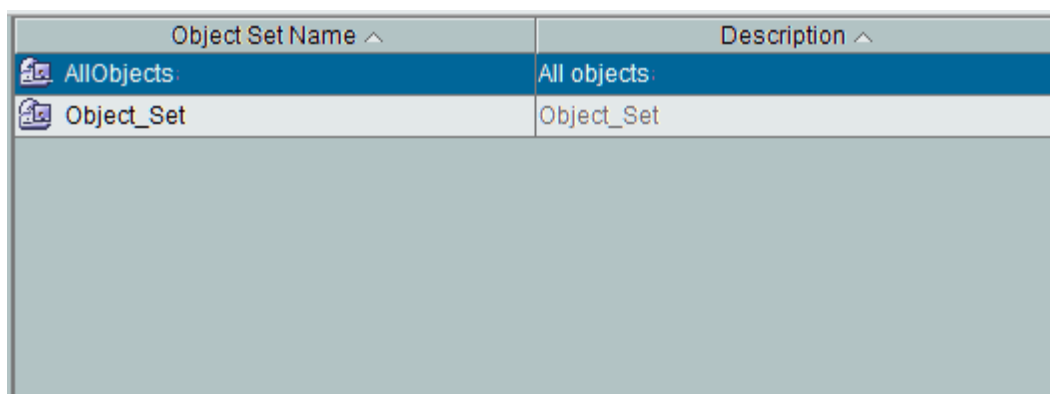
The object set used no longer must be deleted immediately by a user of the SMManagers group.

Context

You are not allowed to delete the default object set **AllObjects**.

Procedure

- 1 Choose **Administration > NMS Security > NMS User Management** from the main menu.
- 2 In the **NMS User Management** navigation tree, choose the **Object Set** node.



Object Set Name ^	Description ^
AllObjects	All objects
Object_Set	Object_Set

The table on the right displays all the object sets on the U2000.

- 3 Right-click the object sets you want to delete and then choose **Delete** or click **Delete** at the bottom of the list.
- 4 In the **Confirm** dialog box, click **Yes**.

----End

4.8 Managing U2000 Operation Sets

This topic describes how to create, modify, and delete operation sets.

4.8.1 U2000 Operation Set

This topic describes the basic meaning and function of the operation set.

4.8.2 Creating an Operation Set

The operation set is a collection of operations. Permissions on devices and applications can be assigned and managed in a unified manner based on operation sets.

4.8.3 Modifying an Operation Set

A user of the SMManagers group can modify an operation set, such as the name and description of an operation set. You can also add operations to an operation set, or delete operations from an operation set.

4.8.4 Deleting an Operation Set

The operation set used no longer should be deleted immediately by a user of the SMManagers group.

4.8.5 Exporting or Importing Operation Sets

The U2000 supports the export and import of operation sets. You can arrange the operation sets on the U2000 by importing an operation set file.

4.8.1 U2000 Operation Set

This topic describes the basic meaning and function of the operation set.

The U2000 operation set is a collection of operation rights provided by the U2000. By default, the U2000 provides two operation sets: **All Application Operations** and **All Object Operations**. If a user or user group can manage an operation set, it indicates that the user or user group has all the operation rights in the operation set.

The administrator can create a operation set, and then add the operation rights required in a service to the operation set. Thus, the administrator can assign the operation rights to the related user or user group in a centralized manner. In this way, the management cost of the administrator is greatly reduced.

4.8.2 Creating an Operation Set

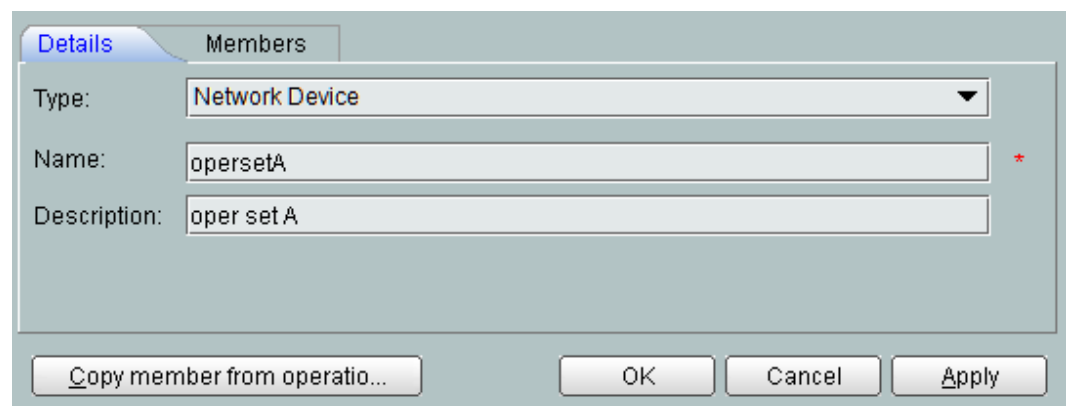
The operation set is a collection of operations. Permissions on devices and applications can be assigned and managed in a unified manner based on operation sets.

Context

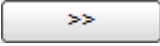
- Operation sets can be allocated to users or user groups.
- If an operation set is allocated to a user group, all members in the user group have the permissions of the operations included in the operation set.
- **AllApplicationOperations** and **AllObjectOperations** are default operation sets provided by the U2000. **AllObjectOperations** is the operation set of network devices. **AllApplicationOperations** is the operation set of network management applications.

Procedure

- 1 Choose **Administration > NMS Security > NMS User Management** from the main menu.
- 2 In the **NMS User Management** navigation tree, right-click the **Operation Set** node and then choose **New Operation Set**. Otherwise, click  on the toolbar of the navigation tree, choose **New Operation Set**.



- 3 In the **New Operation Set** dialog box, set the properties of the new operation set.

Properties of Operation Set	Operations
Details of Operation set	On the Details tab, enter the type, name, and description of the new operation set. NOTE Name is mandatory.
Members of Operation set	On the Members tab, perform the following operations: - Click Select. - Select an operation or operation set, and move it to Selected Rights. - You can click  to move all operations and operation sets to Selected Rights. - You can select operations or operation sets from the Available Rights navigation tree, and then click  to move the selected operations or operation sets to Selected Rights. - Click OK.



NOTE

Click **Copy member from operation set**. In the **Copy member from operation set** dialog box, select operation sets and copy the members of these operation sets.

- 4 In the **New Operation Set** dialog box, click **OK**.

----End

4.8.3 Modifying an Operation Set

A user of the SMManagers group can modify an operation set, such as the name and description of an operation set. You can also add operations to an operation set, or delete operations from an operation set.

Prerequisite

Operation sets and operation permissions are already created on the U2000.

Context

- You cannot modify the default operation set.
- Only the users in Sub Domain User Group and Security Manager User Group have the right to modify operation sets.

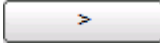
Procedure

- 1 Choose **Administration > NMS Security > NMS User Management** from the main menu.
- 2 In the **NMS User Management** navigation tree, expand the **Operation Set** node, and then select the operation set to be modified.

The screenshot shows a web-based configuration interface for an Operation Set. It has three tabs: 'Details' (selected), 'Members', and 'Applicable for'. Under the 'Details' tab, there are three input fields: 'Type' with a dropdown menu showing 'Network Device', 'Name' with the text 'OpeSetA', and 'Description' with the text 'Operation Set A'. At the bottom right of the form is an 'Apply' button.

- 3 In the area on the right , select a tab to modify the information about the operation set.

Modifying an Operation Set	Operations
Modify normal properties	Click the Details tab. Modify the operation set name and description (the type of operation set cannot be changed). After modification, click Apply .
Set members of a operation set	Click the Members tab. At the bottom of the tab, click Select . In the Select Operation Set Member dialog box, set the member of the operation set, and then click OK .
Set parameters on the Applicable for tab page	On the Applicable for tab, you can view only the users or user groups served by the operation set. The Applicable for tab displays the users or user groups served by the operation set.

Modifying an Operation Set	Operations
Allocate an operation set	To allocate an operation set to a user or user group, do as follows: 1. Expand the User or User Group node and choose a user or user group. 2. Click the Domain tab on the right of the interface. Click Select. 3. In the displayed Select Domain dialog box, add a object set to the user or user group. Click OK. 4. Click the Operation Rights tab on the right of the window. Click Select. 5. Select network device operations or network management applications. ● Network Device In the Select Operation Rights dialog box, select a operation set. In the Operations area, select the corresponding operation set. ● Network Management Application In the Select Operation Rights dialog box, choose Network Management Application in the navigation tree of authorized objects. In the Operations area, select the corresponding operation set. 6. Click  to move the selected operation set to Selected Rights. 7. Click Ok.

----End

4.8.4 Deleting an Operation Set

The operation set used no longer should be deleted immediately by a user of the SMMangers group.

Context

You are not allowed to modify default operation sets **All Object Operations** and **All Application Operations**.

Procedure

- 1 Choose **Administration** > **NMS Security** > **NMS User Management** from the main menu.
- 2 In the **NMS User Management** navigation tree, choose the **Operation Set** node.

Operation Set Name ^	Type ^	Description ^
 AllApplicationOperations	Network Management Application	All application operations
 AllObjectOperations	AllObjectOperations	All object operations
 OperaSetA	Network Device	Operation Set A

The table on the right displays all the operation sets on the U2000.

- 3 Select the operation sets you want to delete, right-click to choose **Delete** or click **Delete** at the bottom of the list.
- 4 In the **Confirm** dialog box, click **Yes**.

----End

4.8.5 Exporting or Importing Operation Sets

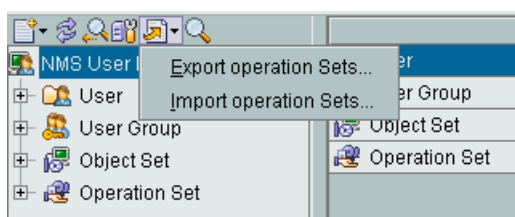
The U2000 supports the export and import of operation sets. You can arrange the operation sets on the U2000 by importing an operation set file.

Context

- Only the administrator has the permissions to export and import operation sets.
- The U2000 supports the export and import of .csv files.
- The U2000 supports the function of adding the information about operation sets in columns one by one. After a .csv file that contains the operation set information is imported to the U2000, the information is displayed as operation sets of the U2000.
- To add a column of operation set information to a .csv file, you need to fill in the following two types of information so that operation sets can be imported to the U2000 successfully:
 - Apart from the information that already exists in a .csv file, you must enter the name of the operation set in the first row of the column where operation sets are to be added.
 - Apart from the information that already exists in a .csv file, if you want to add operation rights, enter an uppercase **Y** in the other rows of the column where operation sets are to be added. **Y** indicates that the information in the rows with **Y** is included in operation sets and is to be displayed on the U2000.

Procedure

- 1 Choose **Administration > NMS Security > NMS User Management** from the main menu.
- 2 On the top of the **NMS User Management** navigation tree click .



- 3 Export and import operation sets.

Export and import operation sets	Operation
Export operation Sets	1. Select Export operation Sets in the drop-down list. 2. In the Save dialog box, set the path and file name for saving the exported operation sets. NOTE The number of the operation set files that are generated by the U2000 is the same as that of the existing operation set types. 3. Click Save.
Import operation Sets	1. Select Import operation Sets in the drop-down list. 2. In the Open dialog box, select the file to be imported. NOTE If the names of the operation sets in a column of a file are the same as those on the U2000, the U2000 cannot import the operation set information of this column. 3. Click Open.

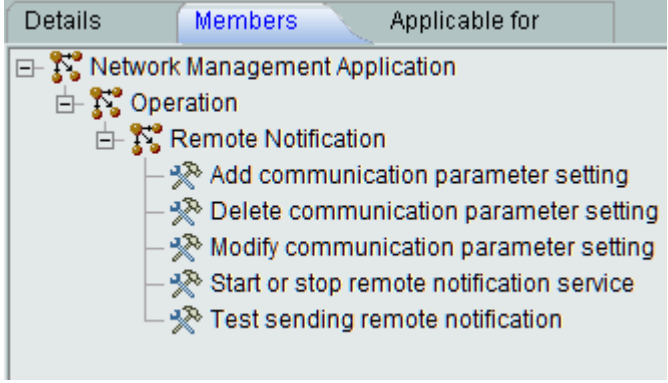
The following table describes the function of each part of a .csv file and helps you to understand specific operations.

The following is a sample of an exported .csv file:

	A	B	C	D	E	F	G
1							
2							
3	Network Management Application						
4	Save Time: 11/13/2009 14:39:27						
5	User Name:Administrator						
6							
7							
8	Total 89 Records						
9							
10	SECURITY_OBJECT_TYPE	OPAERATION NAME	OPERATION	OPAERAT	OPAERATION TYPE	ID	OpeSet_A
11	Remote Notification	Test sending remote notification	Test sendi	116	RemoteNotification	MY	
12	Remote Notification	Delete communication parameter setting	Delete com	115	RemoteNotification	MY	
13	Remote Notification	Modify communication parameter setting	Modify com	114	RemoteNotification	MY	
14	Remote Notification	Add communication parameter setting	Add commun	113	RemoteNotification	MY	
15	Remote Notification	Start or stop remote notification servi	Start or s	112	RemoteNotification	MY	
16	System Management	Log Forwarding	Log Forwar	19	SystemMaintenance		
17	System Management	Operations of System Monitor	Operations	27	SystemMaintenance		

Table 4-1 Parts of a .csv file

Column/Row	Description
Columns A to E	U2000This part displays the information about operation rights that is provided by default. WARNING If service requirements are met, do not modify this part. If you modify it, the U2000 may run abnormally. If an exception occurs after modification, contact Huawei technical support engineers.

Column/Row	Description
Column F	In column F, OpeSet_A indicates the exported operation sets. Y indicates a member that belongs to OpeSet_A on the U2000. The following figure shows that the operations sets in a .csv file are displayed on the U2000: 
Columns G to the end	You can add an operation set to the tenth row according to service requirements, and fill Y in the corresponding column.

----End

4.9 Monitoring a U2000 User

This topic describes how to monitor U2000 user sessions and operations, force U2000 users to exit, unlock U2000 user accounts and send messages to online users.

4.9.1 Monitoring the U2000 User Sessions

User sessions record the login time, group, client, and status of the user. By monitoring the user sessions, you can know the users who have logged in to the system and force the users who may affect system security to log out as required, thus ensuring system security.

4.9.2 Monitoring the U2000 User Operations

A user of the SMManagers group can monitor operations of U2000 users to prevent unauthorized operations.

4.9.3 Forcing a U2000 User to Quit

A user of the SMManagers group can force a U2000 user to quit session if the user performs dangerous operations or initiates illegal sessions.

4.9.4 Unlocking a User Account

This topic describes how the user with the right to unlock a user unlocks a locked user.

4.9.5 Sending Messages to Online Users

A user of the SMManagers group can send messages to the users of the specified sessions or all sessions. Thus, users in different regions can communicate with each other on the U2000 maintenance experience in real time.

4.9.1 Monitoring the U2000 User Sessions

User sessions record the login time, group, client, and status of the user. By monitoring the user sessions, you can know the users who have logged in to the system and force the users who may affect system security to log out as required, thus ensuring system security.

Context

- A session refers to the connection established between the client and the server. The session starts when the user logs in to the client, and ends when the user logs out of the client.
- Multiple sessions can be created by using one U2000 user account.
In the U2000, a user account can be used to log in to multiple clients concurrently. You can set the maximum number of clients that a user account can log in to concurrently in **Maximum of online users** on the **Details** tab. If this user account is used to log in to a certain number of clients, the same number of sessions are established.
- When the client uses multiple network adapters, the value of **Operation Terminal** is selected randomly among available IP addresses of the client.

Procedure

- 1 Choose **Administration > NMS Security > Monitor User Sessions** from the main menu.
- 2 In the **Monitor User Sessions** window, view the information about login and other operations performed by U2000 users.
- 3 In the **Session Monitor** area, you can view the information about online users and sessions.



NOTE

- After the U2000 server is restarted or the network is recovered from a disconnection, you need to click **Refresh** to update the session monitoring table.
- If you select the local client in the **Session Monitor** area, **Force User to Log Out** becomes unavailable.

----End

4.9.2 Monitoring the U2000 User Operations

A user of the SMManagers group can monitor operations of U2000 users to prevent unauthorized operations.

Procedure

- 1 Choose **Administration > NMS Security > Monitor User Operations** from the main menu.
- 2 Click **Filter**. In the displayed **Filter** dialog box, set the operation information to be displayed.
- 3 In the **User Session Monitoring** window, view the information about login and other operations performed by U2000 users.

User N...	Operati...	Operation	Operation Ob...	Risk Level	Operation Result	Start Time	End Time	Details
Administ...	10.70.14...	Set security ...	Network Manag...	Minor	Success	27/07/2009 ...	27/07/200...	
Administ...	10.70.14...	Set security ...	Network Manag...	Minor	Success	27/07/2009 ...	27/07/200...	

Filter...

When an operation affects the U2000, you can restrict the user who performs this operation according to the actual U2000 applications. For example, you can force the user to log out in the **User Session Monitoring** window.

----End

4.9.3 Forcing a U2000 User to Quit

A user of the SMManagers group can force a U2000 user to quit session if the user performs dangerous operations or initiates illegal sessions.

Context

- Only administrators, users of the **SMManagers** group, and subdomain security administrators can force a user to quit. If you force a user to quit session, only the user corresponding to a session is logged out forcibly. For example, user **user_z** logs in to the same U2000 server through clients A and B. In this case, sessions a and b are generated. If you want to force the user **user_z** of session a to quit, session b of user A is not affected.
- Current users logged in cannot force themselves to quit from their corresponding sessions.

Procedure

- Choose **Administration > NMS Security > Monitor User Sessions** from the main menu.
- From the session monitoring table, select the records of the sessions to quit forcibly, and then click **Force User to Log Out**.

Session Monitor					
User Name	Operation Terminal	Type	Session Start Time	User Groups	Details
Administrator	10.70.140.122	NMS Client	16/05/2009 18:24:19	SMManagers:Administrators	Default administrator
NewUserA	10.70.141.134	NMS Client	16/05/2009 19:14:48	Normal	User A
Administrator	10.70.141.134 (Local client)	NMS Client	16/05/2009 19:15:04	SMManagers:Administrators	Default administrator

Total records: 3

Refresh

Force User to Log Out

- In the confirm dialog box, click **Yes**.

----End

4.9.4 Unlocking a User Account

This topic describes how the user with the right to unlock a user unlocks a locked user.

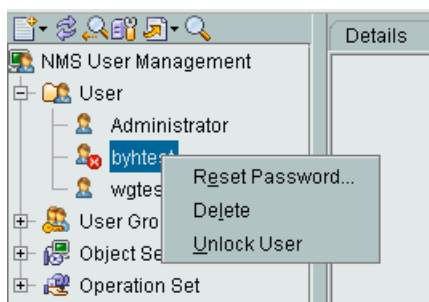
Context

- The **SMManagers** user has the permission to unlock a user.
- In the U2000, a user can be unlocked manually or automatically.
- You can set the automatic unlocking time in **Account Policy**.

Choose **Administration > NMS Security > Security Policies** from the main menu. In the displayed **Security Policy** dialog box, click the **Account Policy** tab, and then set **Auto Unlock**.

Procedure

- 1 The U2000 supports the following user unlocking modes.



Unlocking Mode	Operation
Manual unlocking	Only the user with the rights of the SMManagers group can perform the following operations: 1. Choose Administration > NMS Security > NMS User Management. 2. In the NMS User Management navigation tree, expand the User node. 3. Right-click the locked user account, and choose Unlock User. After that, the unlocked user can log in to the U2000 successfully.
Automatic unlocking	The locked user can log in successfully only when the time reaches the preset automatic unlocking time.

----End

4.9.5 Sending Messages to Online Users

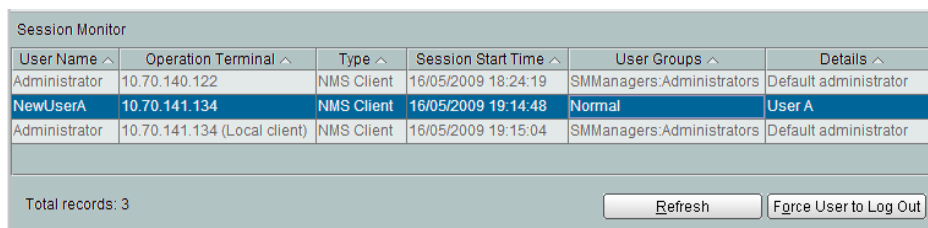
A user of the SMManagers group can send messages to the users of the specified sessions or all sessions. Thus, users in different regions can communicate with each other on the U2000 maintenance experience in real time.

Context

On the U2000, the user of the current session cannot send messages to himself or herself.

Procedure

- 1 Choose **Administration > NMS Security > Monitor User Sessions** from the main menu.



User Name ^	Operation Terminal ^	Type ^	Session Start Time ^	User Groups ^	Details ^
Administrator	10.70.140.122	NMS Client	16/05/2009 18:24:19	SMMangers:Administrators	Default administrator
NewUserA	10.70.141.134	NMS Client	16/05/2009 19:14:48	Normal	User A
Administrator	10.70.141.134 (Local client)	NMS Client	16/05/2009 19:15:04	SMMangers:Administrators	Default administrator

Total records: 3

- 2 In the **Session Monitor** area, send messages to the users of the specified sessions or all sessions.

Sessions to Be Sent	Operation
A session	Right-click a session and choose Send Message . Enter the message contents, and then click Send .
Multiple sessions	Press the Ctrl or Shift to select multiple sessions. Right-click the selected sessions and choose Send Message . Enter the message contents, and then click Send .
All sessions	Use the combination key Ctrl+A to select all sessions. Right-click the selected sessions and choose Send Message . Enter the message contents, and then click Send .

----End

4.10 Managing the Remote Maintenance User

The U2000 remote maintenance function allows login to the U2000 server from a remote maintenance terminal. Strict management for the remote maintenance user not only ensures U2000 system security, but also makes maintenance operations easier.

Prerequisite

- You must be an NM user with "NM maintainer" authority or higher.
- The remote maintenance user must be enabled before you set operation authority or set validity parameters.

Context

- To facilitate easy maintenance, the U2000 supports remote maintenance functions. In the maintenance field, maintenance personnel can log in to the remote maintenance terminal as the remote maintenance user and maintain NEs. Under normal conditions, do not enable this option for security reasons. Enable this option for a user only when a fault occurs or in special conditions.
- For security purposes, it is recommended to set a valid period for the remote maintenance user.

Procedure

- 1 Choose **Administration > NMS Security > Remote Maintenance User Management** from the main menu.

Set Remote Maintenance User Parameter

Disable/Enable ☐ Disabled ☒ Enabled

Operation Authority ☒ Query ☐ Configuration

Valid Forever or Not ☒ No ☐ Yes

Validity Period 26/05/2009 10:24 ... ☐ DST

Login Status ☐ Logged in ☒ Not logged in

Remote Maintenance User of Current Login

OK Cancel Apply

- 2 Enable the remote maintenance user.
- 3 Set the **Operation Authority**. You can select **Query** or **Configuration** as needed.
- 4 Set **Valid Forever or Not** to **No**. Set **Validity Period**.
- 5 Click **OK**.

----End

4.10.1 Enabling a Remote Maintenance User

To facilitate easy maintenance, the U2000 supports remote maintenance functions. In the maintenance field, maintenance personnel can log in to the remote maintenance terminal as the remote maintenance user and maintain NEs. Under normal conditions, do not enable this option for security reasons. Enable this option for a user only when a fault occurs or in special conditions.

4.10.2 Setting the Remote Maintenance User Authority

Operation authority must be assigned to the remote maintenance user reasonably to guarantee the U2000 security. Currently there are two types of operation authority: query and configuration.

4.10.3 Setting the Remote Maintenance User Validity

For security purposes, it is recommended to set a valid period for the remote maintenance user. In the U2000, the remote maintenance is permanently valid by default. While in practical application, the user can set the valid period as needed.

4.10.1 Enabling a Remote Maintenance User

To facilitate easy maintenance, the U2000 supports remote maintenance functions. In the maintenance field, maintenance personnel can log in to the remote maintenance terminal as the remote maintenance user and maintain NEs. Under normal conditions, do not enable this option for security reasons. Enable this option for a user only when a fault occurs or in special conditions.

Prerequisite

You must be an NM user with "NM maintainer" authority or higher.

Procedure

- 1 Choose **Administration > NMS Security > Remote Maintenance User Management** from the main menu. The **Remote Maintenance User Management** dialog box is displayed. Enable the remote maintenance user and set its other parameters.

Set Remote Maintenance User Parameter

Disable/Enable ☐ Disabled ☒ Enabled

Operation Authority ☒ Query ☐ Configuration

Valid Forever or Not ☒ No ☐ Yes

Validity Period 26/05/2009 10:24 ... ☐ DST

Login Status ☐ Logged in ☒ Not logged in

Remote Maintenance User of Current Login

OK Cancel Apply

- 2 Click **OK**.

----End

4.10.2 Setting the Remote Maintenance User Authority

Operation authority must be assigned to the remote maintenance user reasonably to guarantee the U2000 security. Currently there are two types of operation authority: query and configuration.

Prerequisite

- You must be an NM user with "NM maintainer" authority or higher.
- The remote maintenance user must be enabled.

Procedure

- 1 Choose **Administration > NMS Security > Remote Maintenance User Management** from the main menu. The **Remote Maintenance User Management** dialog box is displayed. Enable the remote maintenance user.
- 2 Set the **Operation Authority**. You can select **Query** or **Configuration** as needed.

Set Remote Maintenance User Parameter

Disable/Enable ☐ Disabled ☒ Enabled

Operation Authority ☒ Query ☐ Configuration

Valid Forever or Not ☒ No ☐ Yes

Validity Period 26/05/2009 10:24 ... ☐ DST

Login Status ☐ Logged in ☒ Not logged in

Remote Maintenance User of Current Login

OK Cancel Apply

- 3 Click **OK**.

----End

4.10.3 Setting the Remote Maintenance User Validity

For security purposes, it is recommended to set a valid period for the remote maintenance user. In the U2000, the remote maintenance is permanently valid by default. While in practical application, the user can set the valid period as needed.

Prerequisite

- You must be an NM user with "NM maintainer" authority or higher.
- The remote maintenance user must be enabled.

Procedure

- 1 Choose **Administration > NMS Security > Remote Maintenance User Management** from the main menu. The **Remote Maintenance User Management** dialog box is displayed. Enable the remote maintenance user.
- 2 Set **Valid Forever or Not** to **No**.
- 3 Set **Validity Period**.

Set Remote Maintenance User Parameter

Disable/Enable ☐ Disabled ☒ Enabled

Operation Authority ☒ Query ☐ Configuration

Valid Forever or Not ☒ No ☐ Yes

Validity Period 26/05/2009 10:24 ... ☐ DST

Login Status ☐ Logged in ☒ Not logged in

Remote Maintenance User of Current Login

OK Cancel Apply

- 4 Click **OK**.

----End

4.11 Managing NE Users

To ensure NE data security, you can manage the authorities and passwords for NE users.

By using the U2000 you can perform the following NE user management tasks.

NOTE

The following functions are applies to the MSTP, WDM, NA WDM, RTN, PTN, Marine series NEs.

[4.11.1 Querying the NE User Information](#)

By querying the additional information of an NE user, you can learn the basic information of this user for the purpose of management or task allocation.

[4.11.2 Creating an NE User](#)

To ensure NE data security, only the users with NE user authority can log in to the NEs. An NE user is able to perform operations on the NEs according to the assigned authority. The U2000 administrator is advised to create NE users before configuring services.

[4.11.3 Modifying NE Users](#)

You need to modify the settings of an NE user, so that the NE user can use the special functions of the NE.

[4.11.4 Changing the NE User Password](#)

To ensure network security, you are recommended to change the NE user password periodically.

[4.11.5 Querying NE Security Parameters](#)

According to the default security settings, the NE is able to determine whether the NE user password is valid and decide whether the login is allowed. The U2000 administrator needs to know the NE security settings and modify the NE user password before it becomes invalid.

[4.11.6 Querying NE User Groups](#)

NE users of different levels are divided into different NE user groups. In this user interface, you can query NE users included by various NE user groups of an NE.

[4.11.7 Deleting NE Users](#)

To ensure NE and network security, you need to delete the NE users that are no longer used. This prevents misoperations or damage caused by user account theft.

4.11.1 Querying the NE User Information

By querying the additional information of an NE user, you can learn the basic information of this user for the purpose of management or task allocation.

Prerequisite

- You must be an NM user with "NE monitor" authority or higher, and belonged to "SMManager" user group.
- The level of the NE user to be queried must be lower than that of the NE user who has logged in.

NOTE

Choose **Administration > NE Security Management > NE Login Management**. You can view the logged in information of NE users on the **NE Login Management** tab.

Procedure

- 1 Choose **Administration > NE Security Management > NE User Management** from the main menu.
- 2 In the NE list on the left, select an NE and click .
- 3 **Optional:** Click **Query** to query the NE user information from the NE.
- 4 Click **User Additional Information** to query the additional information of this NE user (such as login policy, password validity policy, and last login time).

----End

4.11.2 Creating an NE User

To ensure NE data security, only the users with NE user authority can log in to the NEs. An NE user is able to perform operations on the NEs according to the assigned authority. The U2000 administrator is advised to create NE users before configuring services.

Prerequisite

- You must be an NM user with "NE administrator" authority or higher, and belonged to "SMManager" user group.
- The level of the NE user to be created must be lower than that of the NE user who has logged in.

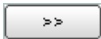
NOTE

Choose **Administration > NE Security Management > NE Login Management**. You can view the logged in information of NE users on the **NE Login Management** tab.

Context

The default NE user has the monitor level authority. To ensure NE data security, it is recommended that you assign NE users with different authorities as required.

Procedure

- 1 Choose **Administration > NE Security Management > NE User Management** from the main menu.
- 2 In the NE list on the left, select an NE and click .
- 3 Click **Add** and the **Add NE User** dialog box is displayed.

Add NE User Attribute/Value

Attribute	Attribute Value
NE User	
User Level	Monitor Level
NE User Flag	LCT NE User
Detailed Description	
New Password	•
Confirm Password	•
Whether the password is allowed to be modified immediately	Yes

NE List of Added NE User

NE Name ^
NE1801
NE202
NE209
NE86
NE93

- 4 Optional:** For the NA NE, you can click the **Add NA User** button, and the **Add NA NE User** dialog box is displayed.

Add NE User Attribute/Value

Attribute	Attribute Value
NE User	
User Level	RTRV
Allow Multi-Terminal Login	DISABLE
New Password	•
Confirm Password	•
Canceling User Automatically	Yes
Time of Canceling User Automatically(m)	60
User Permanently Valid	Yes
User Valid Till(days)	0
Password Permanently Valid	Yes
Password Valid Till(days)	0

NE List of Added NE User

NE Name ^
NA65
NE121

- 5** Enter the NE user name in the **NE User** field.
- 6** Select the **User Level** as needed.
- 7** In the **NE User Flag** field, select a user type according to the type of the terminal through which the user logs in to the NE.

- 8 Enter the password in the **New Password** field and enter it again in the **Confirm Password** field.



NOTE

The password is a string of 6-16 characters. It can consist of letters, symbols and numerals, and must contain at least one letter and one numeral.

- 9 In the **NE Name** field, select one or multiple NEs that this NE user is allowed to manage.
 - 10 Click **OK**.
- End

4.11.3 Modifying NE Users

You need to modify the settings of an NE user, so that the NE user can use the special functions of the NE.

Prerequisite

- You must be an NM user with "NE administrator" authority or higher, and belonged to "SMManager" user group.
- The NE user must be created.
- The level of the NE user to be modified must be lower than that of the NE user who has logged in.



NOTE

Choose **Administration > NE Security Management > NE Login Management**. You can view the logged in information of NE users on the **NE Login Management** tab.

Procedure

- 1 Choose **Administration > NE Security Management > NE User Management** from the main menu.
- 2 In the left-hand NE list, select an NE and click .
- 3 In **NE User Management Table**, select the NE user to be modified and click **Modify**. A dialog box is displayed.
- 4 In the dialog box displayed, modify the settings of the attributes of the NE user. Click **Apply**.
- 5 Click **OK**.

----End

4.11.4 Changing the NE User Password

To ensure network security, you are recommended to change the NE user password periodically.

Prerequisite

- You must be an NM user with "NE administrator" authority or higher, and belonged to "SMManager" user group.
- The NE user must be created.
- The level of the NE user to be modified must be lower than that of the NE user who has logged in.

**NOTE**

Choose **Administration > NE Security Management > NE Login Management**. You can view the logged in information of NE users on the **NE Login Management** tab.

Context

**CAUTION**

Change the password periodically for security purposes.

Procedure

- 1 Choose **Administration > NE Security Management > NE User Management** from the main menu.
- 2 In the Object Tree, select an NE that you want to query and click .
- 3 Select an NE user whose password need to be modified from the NE user list and choose **Set Password**. The **Set Password of NE User** dialog box is displayed. Enter the password in the **New Password** field and enter the new password again in the **Confirm Password** field.

The List of NE User Setting Password

NE ^	NE User ^
NE26	necems2

Input Password Area

New Password

Confirm Password

- 4 Click **OK**.

----End

4.11.5 Querying NE Security Parameters

According to the default security settings, the NE is able to determine whether the NE user password is valid and decide whether the login is allowed. The U2000 administrator needs to know the NE security settings and modify the NE user password before it becomes invalid.

Prerequisite

You must be an NM user with "NE administrator" authority or higher.

Applies to the release 5.0 NEs of transport domain equipments.

Procedure

- 1 In the NE Explorer, select an NE and choose **Security > NE Security Parameters** from the Function Tree.
- 2 Click **Query** to query the settings of NE security parameters.

----End

4.11.6 Querying NE User Groups

NE users of different levels are divided into different NE user groups. In this user interface, you can query NE users included by various NE user groups of an NE.

Prerequisite

You must be an NM user with "NE administrator" authority or higher.

Applies to the MSTP, WDM, RTN, PTN NEs.

Procedure

- 1 In the NE Explorer, select an NE and choose **Security > NE User Group Management** from the Function Tree.
- 2 Click **Query** to query NE users included by various NE user groups of the NE.

----End

4.11.7 Deleting NE Users

To ensure NE and network security, you need to delete the NE users that are no longer used. This prevents misoperations or damage caused by user account theft.

Prerequisite

- You must be an NM user with "NE administrator" authority or higher.
- The NE user must be created.
- The level of the NE user to be deleted must be lower than that of the NE user who has logged in.



NOTE

Choose **Administration > NE Security Management > NE Login Management**. You can view the logged in information of NE users on the **NE Login Management** tab.

Procedure

- 1 Choose **Administration > NE Security Management > NE User Management** from the main menu.
- 2 In the left-hand NE list, select an NE and click .

- 3 In **NE User Management Table**, select the NE user to be deleted and click **Delete**. A dialog box is displayed asking you whether to delete the NE user.
 - 4 Click **OK**.
- End

4.12 Managing NE Login

To ensure NE data security, you can manage the users who are logged in to NEs.

Context

By using the U2000 you can perform the following NE login management tasks:

4.12.1 Locking Out NE Login

An NE user can lock out the NE, to deny login attempts from other users of the same level or lower level. If there is an NE user of the same level or higher level logged in to the NE, the NE user cannot lock out the NE. NE users of higher levels automatically unlock the NE login that is locked by lower-level users.

4.12.2 Locking Out NE Settings

An NE user can lock out the settings of an NE, preventing other NE users of the same level or higher level from performing any settings on the NE. If a user of the same level or higher level has logged in to the NE, the NE user cannot lock out the NE settings. NE users of higher levels automatically unlock the NE settings locked by lower-level users.

4.12.3 Querying the Information About an Online NE User

To ensure the security of NE operations, the NMS maintainers or administrators can use the U2000 to view all the online NE users within the management rights and the way in which the users log in to the NEs. The NE user at a higher level can forcibly kick off the NE user at a lower level.

4.12.4 Switching a Logged-In NE User

During a new deployment, after the root NE user creates the NE, this user can create another NE user. You can log in to the NE with the new NE user name.

4.12.5 Forcing an NE User to Log Out of the U2000

For network security management, you can force a specified NE user to log out of the U2000 as required. In the single user mode, this function also forces all other users to log out of the U2000. In addition, an NE user will be forced to log out by the U2000 after a long period of time without any activities.

4.12.6 Setting NE Login Prompt Message

You can set the custom information of an NE logs in to the U2000 in this interface.

4.12.1 Locking Out NE Login

An NE user can lock out the NE, to deny login attempts from other users of the same level or lower level. If there is an NE user of the same level or higher level logged in to the NE, the NE user cannot lock out the NE. NE users of higher levels automatically unlock the NE login that is locked by lower-level users.

Prerequisite

- You must be an NM user with "NE administrator" authority or higher.
- The current NE user has the highest level among all login NE users.
- The NE must be a release 4.0 transport equipment.

Procedure

- 1 Choose **Administration > NE Security Management > Lock Out NE Login** from the main menu.
- 2 In the Object Tree, select an NE and click the double-right-arrow button (red).
- 3 Click **Query** to query the **Login Lock Status**.
- 4 **Optional:** If the value of **Login Lock Status** is **Not Locked out**, select it and click **Lock Login** or right-click it and choose **Lock Login**.

----End

4.12.2 Locking Out NE Settings

An NE user can lock out the settings of an NE, preventing other NE users of the same level or higher level from performing any settings on the NE. If a user of the same level or higher level has logged in to the NE, the NE user cannot lock out the NE settings. NE users of higher levels automatically unlock the NE settings locked by lower-level users.

Prerequisite

- You must be an NM user with "NE administrator" authority or higher.
- Applies to the release 4.0 transport NEs.

Procedure

- 1 Choose **Administration > NE Security Management > Lock Out NE Settings** from the main menu.
- 2 In the left pane, select an NE and click the double-right-arrow button (red).
- 3 Click **Query** to query the **Set Lock Status**.
- 4 If the value of **Set Lock Status** is **No**, select it and click **Lockout** or right-click it and select **Lockout**. The **Set Lock Window** dialog box is displayed.
- 5 Check the **Lock Permanently** check box to permanently lock the current NE settings or enter the value of **Continues Time** to temporarily lock the settings. Click **OK**.

----End

4.12.3 Querying the Information About an Online NE User

To ensure the security of NE operations, the NMS maintainers or administrators can use the U2000 to view all the online NE users within the management rights and the way in which the users log in to the NEs. The NE user at a higher level can forcibly kick off the NE user at a lower level.

Prerequisite

You must be a U2000 user with NMS maintainer or NMS administrator rights or higher.

This operation is applicable to the MSTP, WDM, NA WDM, RTN, PTN, Marine series NEs.

Procedure

- 1 Choose **Administration > NE Security Management > NE Login Management** from the main menu. Click the **Online User Management** tab.
- 2 Select the NE to be queried from the NE list and click .
- 3 Click **Query** to query the user of the online NE and the login way of this user.
- 4 **Optional:** Click **Filter**. Set **Current Connected User** and **Login Mode** as the filter criteria to view the information about the online NE user.

----End

4.12.4 Switching a Logged-In NE User

During a new deployment, after the root NE user creates the NE, this user can create another NE user. You can log in to the NE with the new NE user name.

Prerequisite

- You must be an NM user with "NE administrator" authority or higher.
- The NE user must be created.
- This operation is applicable to the MSTP, WDM, NA WDM, RTN, PTN, Marine series NEs.

Background Information

One NE user cannot log in or manage an NE at multiple clients at the same time. After you use an NE user to log in to an NE through a U2000 server, if you use the same NE user to log in to the same NE through another U2000 server, the NE user is forced to log out from the first U2000 server.

Procedure

- 1 Choose **Administration > NE Security Management > NE Login Management** from the main menu.
- 2 Click **NE Login Management** or **DC Login User Management** tab.
- 3 Select an NE from the NE list to switch its user. Click .
- 4 Click **Query** to query the current NE user.
- 5 In the table, select the NE and click **Switch NE User**. In the **Switch Current NE User** dialog box, enter the NE user name and password.
- 6 Click **OK**.

----End

4.12.5 Forcing an NE User to Log Out of the U2000

For network security management, you can force a specified NE user to log out of the U2000 as required. In the single user mode, this function also forces all other users to log out of the U2000. In addition, an NE user will be forced to log out by the U2000 after a long period of time without any activities.

Prerequisite

- You must be an NM user with "NE administrator" authority or higher.
- The NE user must be created.
- The NE user must be logged in to the NE.
- The current NE user has the higher level than the other login NE users.

Context

Applies to the MSTP, WDM, NA WDM, RTN, PTN, Marine series NEs.

Procedure

- 1 Choose **Administration > NE Security Management > NE Login Management** from the main menu.
- 2 In the Object Tree, select an NE and click the double-right-arrow button (red).
- 3 Click **NE Login Management** or **Online User Management** tab, select the NE entry. Click **Logout** or **Forced Logout**. A prompt appears telling you that the operation was successful.
- 4 Click **Close**.

----End

4.12.6 Setting NE Login Prompt Message

You can set the custom information of an NE logs in to the U2000 in this interface.

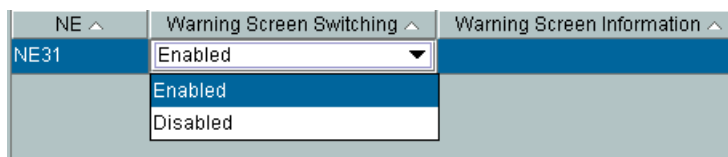
Prerequisite

You must be an NM user with "NE operator" authority or higher.

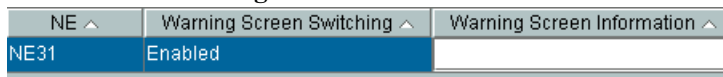
Applies to the MSTP, WDM, NA WDM, RTN, PTN, Marine series NEs.

Procedure

- 1 In the NE Explorer, select an NE and choose **Security > NE Security Parameters** from the Function Tree.
- 2 **Optional:** Click **Query** to query the settings of NE security parameters.
- 3 Select an NE, double-click **Warning Screen Switching** and choose whether to enable the warning screen.



- 4 Double-click **Warning Screen Information** and enter the information.

**NOTE**

You can enter information in the **Warning Screen Information** field only when you set **Warning Screen Switching** to **Enabled**.

- 5 Click **Apply**. A prompt appears telling you that the operation was successful. Click **Close**.

----End

4.13 Setting the Security Access of an NE

To ensure the NE security, you need to disable the unused interfaces on the NE.

Prerequisite

Applies to the MSTP, WDM, NA WDM, RTN, PTN, Marine series NEs.

4.13.1 Controlling Communication Between NE and U2000 Through Ethernet Port

By default, an NE can be connected to the U2000 through an Ethernet port. This operation enables you to query and set the Ethernet access function for an NE.

4.13.2 Controlling Communication Between NE and U2000 Through a Serial Port

NEs can be accessed to the U2000 through a serial port or the command line tool. This operation views and sets the serial port access function of NEs.

4.13.3 Setting the NE OAM Access

The U2000 installed in a PC or a workstation can use the OAM port of an NE to manage and maintain the NE. The OAM port can also be used in remote maintenance if necessary. To configure an NE through the OAM port, you need to enable the OAM access function of the NE.

4.13.4 Setting the NE COM Access

The COM port of an NE is a port used for on-site commissioning. If you need to use the COM port to configure an NE, you need to enable the COM access function of the NE.

4.13.5 Controlling Communication Between NE and LCT

For NE operation security, NEs are managed by the U2000 under normal circumstances. But under special circumstances, you need to use the U2000 LCT or Web LCT to commission an NE. You can turn on LCT access for the NE on the U2000.

4.13.1 Controlling Communication Between NE and U2000 Through Ethernet Port

By default, an NE can be connected to the U2000 through an Ethernet port. This operation enables you to query and set the Ethernet access function for an NE.

Prerequisite

You must be an NM user with "NM maintainer" authority or higher.

Applies to the MSTP, WDM, NA WDM, RTN, PTN, Marine series NEs.

Context



CAUTION

This operation may affect the communication between the U2000 and NEs.

Procedure

- 1 In the NE Explorer, select an NE and choose **Communication > Access Control** from the Function Tree.
- 2 In the **Ethernet Access Control** area, click **Refresh** to query the Ethernet access enable status.
- 3 Set **The First Network Port** as **Enabled** and click **Apply**. The Ethernet access function for the NE is enabled.



NOTE

- If you want to disable this function, set **The First Network Port** as **Disabled** and click **Apply**.
- If the second network port exists, you can enable Ethernet access for the port. For OptiX OSN equipment, the second network port is EXT port.

For certain types of devices, you can click the **Enable Ethernet Access** checkbox to enable the Ethernet access function.

----End

4.13.2 Controlling Communication Between NE and U2000 Through a Serial Port

NEs can be accessed to the U2000 through a serial port or the command line tool. This operation views and sets the serial port access function of NEs.

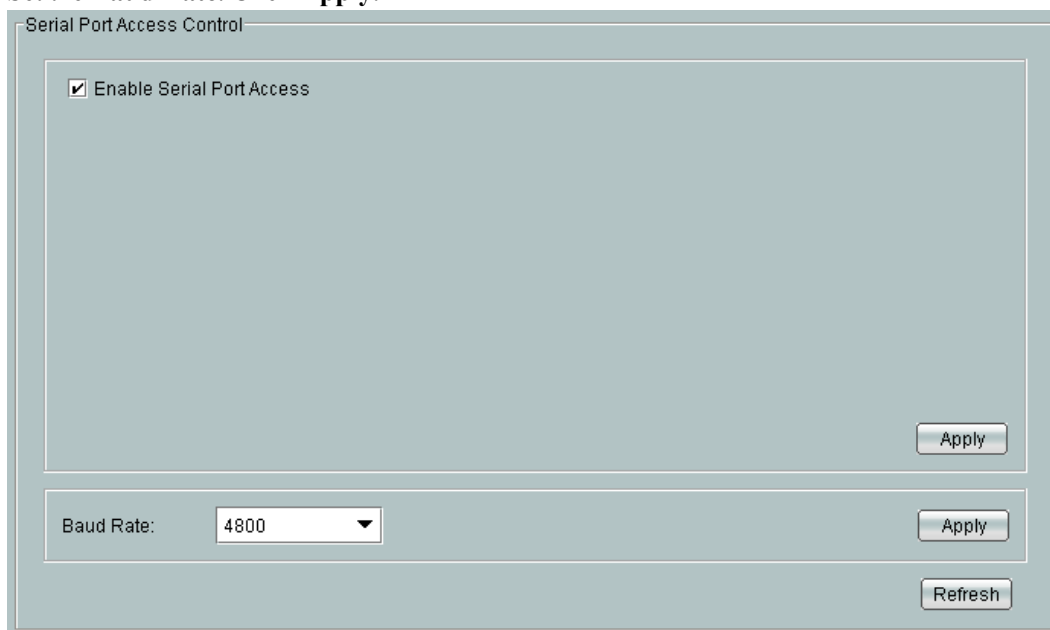
Prerequisite

You must be an NM user with "NM maintainer" authority or higher.

Applies to the MSTP, WDM, NA WDM, RTN, PTN, Marine series NEs.

Procedure

- 1 In the NE Explorer, select an NE and choose **Communication > Access Control** from the Function Tree.
- 2 Check the **Enable Serial Port Access** check box. Click **Refresh** to query whether the current NE allows serial port access. Click **Apply** to enable the serial access function of the NE.

3 Set the Baud Rate. Click Apply.The image shows a 'Serial Port Access Control' dialog box. It has a title bar with the text 'Serial Port Access Control'. Inside the dialog, there is a large rectangular area with a checkbox labeled 'Enable Serial Port Access' which is checked. To the right of this area is an 'Apply' button. Below this area, there is a 'Baud Rate:' label followed by a dropdown menu showing '4800'. To the right of the dropdown is another 'Apply' button. At the bottom right of the dialog is a 'Refresh' button.

----End

4.13.3 Setting the NE OAM Access

The U2000 installed in a PC or a workstation can use the OAM port of an NE to manage and maintain the NE. The OAM port can also be used in remote maintenance if necessary. To configure an NE through the OAM port, you need to enable the OAM access function of the NE.

Prerequisite

You must be an NM user with "NM maintainer" authority or higher.

Applies to the MSTP, Metro WDM, LH WDM, RTN, PTN, Marine NEs.

Procedure

- 1 In the NE Explorer, click an NE and choose **Communication > Access Control** from the Function Tree.
- 2 Select **Enable OAM Access** and click **Apply**. The OAM access of the NE is now enabled.

The image shows an 'OAM Access Control' dialog box. It has a title bar with the text 'OAM Access Control'. Inside the dialog, there is a checkbox labeled 'Enable OAM Access' which is unchecked. To the right of this checkbox are two buttons: 'Refresh' and 'Apply'.

----End

4.13.4 Setting the NE COM Access

The COM port of an NE is a port used for on-site commissioning. If you need to use the COM port to configure an NE, you need to enable the COM access function of the NE.

Prerequisite

You must be an NM user with "NM maintainer" authority or higher.

Applies to the MSTP, Metro WDM, LH WDM, RTN, PTN Marine equipment.

Context

- The COM port directly connects to the SCC board, improper usage may affect the normal service handling on the NE, and the rate of the COM port is slow. Hence, it is recommended to use Ethernet access for the LCT (U2000 or Web LCT) in most cases.
- Use COM port access only when the Ethernet access fails, or the NE already connects to the U2000, or certain lower layer commissioning commands need be run.
- For security measures, the COM port access is disabled by default after NE initialization or downloading. If necessary, you can use the U2000 to temporarily enable COM access.

Procedure

- 1 In the NE explorer, click an NE and choose **Communication > Access Control** from the Function Tree.
- 2 Select **Enable COM Access** and click **Apply**. The COM access of the NE is now enabled.



----End

4.13.5 Controlling Communication Between NE and LCT

For NE operation security, NEs are managed by the U2000 under normal circumstances. But under special circumstances, you need to use the U2000 LCT or Web LCT to commission an NE. You can turn on LCT access for the NE on the U2000.

Prerequisite

You must log in to the NM as user admin.

This operation is applicable to the MSTP, WDM, NA WDM, RTN, PTN, Marine series NEs.

Background Information

- When no U2000 user logs in to an NE and an LCT user requests to log in to the NE, the NE does not refer to the **LCT Access Control Switch** parameter and allows the LCT access directly.
- When a U2000 user has logged in to an NE and then an LCT user requests to log in to the NE, the NE determines whether to allow the LCT user to log in according to the **LCT Access Control Switch** parameter.
- When an LCT user has logged in to an NE and then a U2000 user requests to log in to the NE, the login of the LCT user does not affect the login of the U2000 user, and the successful login of the U2000 user does not affect the logged-in LCT user.

- When the LCT user and the U2000 user log in to the NE at the same time, set **LCT Access Control Switch** to **Disable Access**. This does not affect the LCT user that is already logged in.
- After the OptiX OSN 500 is disconnected to the U2000 for over 30 minutes, the OptiX OSN 500 automatically allows the LCT access.

Procedure

- If you want to manage LCT access network-wide, use the following method to navigate to the window.
 1. Choose **Administration > NE Security Management > NE Login Management** from the main menu. Click the **LCT Access Control** tab.
 2. Select the NE to be set from the NE list and click .
 3. Click **Query** to query whether the current NE allows LCT access.
 4. **Optional:** Select an NE and click **Access Allowed** to enable LCT access.
 5. **Optional:** Select an NE and click **Disable Access** to disable LCT access.
 6. **Optional:** To set LCT access for multiple NEs in batches, select the NEs, right-click, and then choose a menu item from the shortcut menu.
- If you want to manage LCT access for a certain NE, use the following method.
 1. In the NE Explorer, select an NE and choose **Security > LCT Access Control** from the Function Tree.
 2. Click **Query** to query whether the current NE allows LCT access.

LCT Access Control	
NE	LCT Access Control Switch
NE26	Disable Access

3. Click **Access Allowed** to enable LCT access.

NOTE

If you want to disable this function, click **Disable Access**.

----End

4.14 Setting the NE ACL

You can ensure the security of NEs by setting the NE ACL.

Prerequisite

Applies to the MSTP, WDM, NA WDM, RTN, PTN, Marine series NEs.

4.14.1 Overview of ACL

Access control list (ACL) can be used for basic traffic filtering. ACL can be configured for all the NEs to filter IP packets as they pass through an NE. ACL can prevent certain traffic from entering or exiting a network.

4.14.2 Setting Basic ACL Rules

In the case of ordinary NEs that do not have high security requirements, you can set the basic ACL rules. The basic ACL rules examine the source IP address of the packets. The basic ACL rules do not use many system resources.

4.14.3 Setting the Advanced ACL Rules

In the case of NEs that have very high security requirements, you can set the advanced ACL rules. The advanced ACL rule, examines the source and the sink IP address, the source and the sink port number, and the protocol type. The implementation of advanced ACL rules use many system resources. The advanced ACL rules have higher priority than the basic ACL rules.

4.14.1 Overview of ACL

Access control list (ACL) can be used for basic traffic filtering. ACL can be configured for all the NEs to filter IP packets as they pass through an NE. ACL can prevent certain traffic from entering or exiting a network.

Purpose

The most important reason to configure ACL is to provide security for the network. With proper ACL rules, the entire network can be prevented from security threats. ACL can also provide the basic flow control function.

Implementation

The ACL can control whether the IP packets are received or dropped by certain NEs. Every IP packets is examined by the NEs according to predefined ACL rules. After the examination, the NEs determine whether to receive or to drop this packet.

4.14.2 Setting Basic ACL Rules

In the case of ordinary NEs that do not have high security requirements, you can set the basic ACL rules. The basic ACL rules examine the source IP address of the packets. The basic ACL rules do not use many system resources.

Prerequisite

- You must be an NM user with "NE operator" authority or higher.
- It is applicable to the MSTP, WDM, PTN and RTN equipment.

Procedure

- 1 In the NE Explorer, select an NE and choose **Security > ACL** from the Function Tree.
- 2 Click the **Basic ACL** tab. The basic ACL rule list is displayed.

NOTE

If the equipment only supports basic ACL settings, by clicking **ACL** from the Function Tree, you directly access the list of the basic ACL rule.

- 3 Click **Query** to load the basic ACL rules from the NE.
- 4 Click **New**.
An undefined basic ACL rule is added to the basic ACL rules list.
- 5 Set the proper values for all the parameters according to the network requirements.
- 6 Click **Apply** to apply the new configuration data to the NE.
A prompt appears indicating the operation was successful.

- 7 Click **Close** to complete the operation.
- 8 **Optional:** Repeat Step 4 through Step 7 to set more basic ACL rules to this NE.
- 9 **Optional:** Repeat Step 1 through Step 7 to set the basic ACL rules to other NEs.

----End

4.14.3 Setting the Advanced ACL Rules

In the case of NEs that have very high security requirements, you can set the advanced ACL rules. The advanced ACL rule, examines the source and the sink IP address, the source and the sink port number, and the protocol type. The implementation of advanced ACL rules use many system resources. The advanced ACL rules have higher priority than the basic ACL rules.

Prerequisite

You must be an NM user with "NE operator" authority or higher.

It is applicable to the MSTP, WDM, PTN and RTN equipment.

Procedure

- 1 In the NE Explorer, select an NE and choose **Security > ACL** from the Function Tree.
- 2 Click the **Advanced ACL** tab. The advanced ACL rule list is displayed.
- 3 Click **Query** to load the advanced ACL rules from the NE.
- 4 Click **New**.
An undefined advanced ACL rule is added to the list.
- 5 Set proper values for all the parameters according to the network requirements.
- 6 Click **Apply** to apply the new configuration data to the NE.
A prompt appears indicating the operation was successful.
- 7 Click **Close** to complete the operation.
- 8 **Optional:** Repeat Step 4 through Step 7 to set more advanced ACL rules to this NE.
- 9 **Optional:** Repeat Step 1 through Step 7 to set the advanced ACL rules to other NEs.

----End

4.15 Auditing Changes

If changes occur on a device in the network, you can query information about the changes through U2000.

With change audit, you can view the following changes:

- Entity changes
The system generates a change record after the change of the device entity is found by polling or manually refreshing the device.
- Device configuration changes

After a device configuration file is backed up in DC management, you can find the change of the device configuration file by comparing it with the previous configuration file. A device configuration change record is generated.

- **Software image changes**

The change record is generated when the system polls the device and finds the change of the software version.

[4.15.1 Viewing Information About Change Auditing](#)

This describes how to view information about change auditing. If changes occur on a device in the network, you can query information about the changes through change auditing.

[4.15.2 Dumping Information About Change Audit](#)

This describes how to dump information about change audit.

[4.15.3 Deleting Information About Change Audit](#)

This describes how to delete information about change audit.

4.15.1 Viewing Information About Change Auditing

This describes how to view information about change auditing. If changes occur on a device in the network, you can query information about the changes through change auditing.

Prerequisite

This operation is applicable to the Router series, Switch series, Security series NEs.

Procedure

- 1 Choose **Administration > NE Security Management > Change Audit** from the main menu.
- 2 On the **Change Audit** tab, click **Condition**.
- 3 In the **Set Filter Condition** dialog box, set the query conditions and then click **OK**.
- 4 On the **Change Audit** tab, click **Query**.

All eligible records are displayed in the query result area. The records displayed in the query result area cannot be refreshed in real time. To view the latest records, you need to click **Query** before viewing.

- 5 Click a record. The details about the record are displayed in the detailed information area.

NOTE

- For a record with **Change Type** being **Software Image**, the **Details** tab displays two records. The upper one shows software version information before change and the lower one shows the latest software version information after change.
- For a record with **Change Type** being **Entity**, the **Details** tab displays the specific change type, either **Add** or **Delete**.

----End

4.15.2 Dumping Information About Change Audit

This describes how to dump information about change audit.

Prerequisite

This operation is applicable to the Router series, Switch series, Security series NEs.

Context

The U2000 deletes the records in the database after information about change audit is dumped. Thus, you cannot query the dumped records through the client.

Procedure

- 1 Choose **Administration > NE Security Management > Change Audit** from the main menu.
- 2 On the **Change Audit** tab, set query conditions and then click **Query**.
All records meeting the conditions are displayed in the query result area.
- 3 In the query result area, select one or more records to be dumped and then right-click them.
Then, select **Dump**.
- 4 In the **Confirm** dialog box, click **OK**.

The system automatically generates a **.dat** file and dumps it to a specified file folder.



NOTE

The files are dumped to the path %IMAPROOT%\server\dump in Windows and \$IMAPROOT/server/dump/ in Solaris with the file name as **current time.dat**. For example, if the file is dumped at 16:30:40 on July 15, 2007, then the file name is **20070715163040.dat**.

- 5 Click **OK**.

----End

4.15.3 Deleting Information About Change Audit

This describes how to delete information about change audit.

Prerequisite

This operation is applicable to the Router series, Switch series, Security series NEs.

Context

The U2000 deletes the records in the database after information about change audit is deleted. Thus, you cannot query the deleted records through the client.

Procedure

- 1 Choose **Administration > NE Security Management > Change Audit** from the main menu.
- 2 On the **Change Audit** tab, set query conditions and then click **Query**.
All records meeting the conditions are displayed in the query result area.
- 3 In the query result area, select one or more records to be deleted and then right-click them. Then, select **Delete**.
- 4 In the **Confirm** dialog box, click **OK**.

----End

4.16 NE License Management

By using the NE license management function, you can query, apply for, install, and change NE licenses. In addition, you can adjust capacities in licenses. By setting licenses for NEs, you can obtain the rights to use certain functions according to service requirements. Because licenses control NE validity periods or functions, you can understand the NE status in real time and perform operations properly by using the license management function. Currently, only certain versions of the OSN equipment, NG WDM equipment, OptiX PTN 910, and OptiX PTN 950 support this function.

4.16.1 Getting to Know NE License Management

This topic describes the scenarios and states that you need to understand for managing NE licenses. By viewing operation scenarios, you can know how to manage NE licenses in different scenarios. By viewing NE license states, you can judge whether licenses meet service requirements.

4.16.2 Querying the NE License Information

By querying the NE license information, you can understand the status of NE licenses and find out the NE licenses to be maintained.

4.16.3 Applying for an NE License

Before NE installation, you need to apply for an NE license.

4.16.4 Installing an NE License

Functions are running properly only after you install a valid license for an NE.

4.16.5 Synchronize NE Information

You can upload the ESN and license information of an NE to the U2000. This function is applicable when an NE accesses the U2000 or after communications recovery after network disconnection between an NE and the U2000.

4.16.6 Adjusting the NE License Capacity

You can adjust the capacity in an NE license to improve the license usage and reduce the maintenance cost of the carrier.

4.16.7 Changing an NE License

If an NE ESN changes or the capacity specified in a license is adjusted for the other NE, you need to change the NE license.

4.16.1 Getting to Know NE License Management

This topic describes the scenarios and states that you need to understand for managing NE licenses. By viewing operation scenarios, you can know how to manage NE licenses in different scenarios. By viewing NE license states, you can judge whether licenses meet service requirements.

NE License Operation Scenarios

When you apply for an NE license, you can query, install, and change the NE license. You can also change the capacities defined in the NE license.

NE License States

An NE license has five states. Before maintaining NE licenses, you need to familiarize yourself with each state. [Table 4-2](#) shows the NE license states.

Table 4-2 NE license states

State	Description
Default	In this state, the NE license is incorrect, does not exist, or expires and exceeds the protection period. The NE whose license is in this state is unavailable.
Demo	If an NE license that you apply for during NE Demo, the state of the license is Demo. In this state, you can use NE functions in a certain period. However, if the license expires, you cannot use the functions. Therefore, you need to apply for a commercial license before the license expires.
Normal	When the NE license obtained from a commercial contract is used, this License is in the Commercial use state. In this state, you can use the resources and functions in the NE license.
Protected	After an NE license expires, it has a protection period. In this period, you can apply for a new license. In the protection period, all control items in the NE license are available.
Emergency	In emergent situations such as a disaster, the NE license state can be set to Critical. In this state, the NE license control is cancelled, and the device capacity is set to the maximum. This prevents the NE services from being damaged. NOTE If an NE license is in the Critical state, contact Huawei technical support engineers to perform operations.
Trial	In this state, you can continue to use the device resources and functions defined in an NE license. The cause for this state is that verification of the correctness of the NE license file fails. In this case, the NE license keeps valid for 60 days (keep-alive period) by default.

4.16.2 Querying the NE License Information

By querying the NE license information, you can understand the status of NE licenses and find out the NE licenses to be maintained.

Context

The state of an NE license affects the use of the functions defined in the NE license.

Procedure

- 1 Choose **Administration > NE License Management** from the main menu.

2 On the **NE License Management** tab, click **License Information Query**

3 Click **Filter**.

 NOTE

- When you start the U2000 client and then access the **NE License Management** for the first time, the **Filter** dialog box is displayed by default.
- when you can choose **License Information Query** in the navigation tree on the left of the **NE License Management** window, and then click **Filter** to access the **Filter** dialog box.

4 In the **Filter** dialog box, select the license state to be queried from **License status**. Select the NE software version to be queried from the **Select version** drop-down list.

5 In the **Device** area click **Select**.

6 In the **Select NE** dialog box, select the NE software version to be queried from the **Select version** drop-down list in the **Available device** area. click , , , and  to select or remove devices from **Available device** and **Selected devices**. click **OK**.

7 In the **Filter** dialog boxes, click **OK**.

8 In the license list, view **NE Name**, **NE Description**, **NE Type**, **Version**, **ESN**, and **License Status** of the license.

 NOTE

- Select an NE license record. In the **Detail Message** area, **OperatorIndex**, **OperatorName**, **LicenseItem**, **LicenseDesc**, and **AssignedValue** are displayed.
- Select one or more NE license records. Right-click them and choose **Export Selected Record** or **Export All Record** to save the details of the queried NE licenses to the local computer.

----End

4.16.3 Applying for an NE License

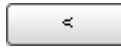
Before NE installation, you need to apply for an NE license.

Prerequisite

Applying for an NE license is applicable only for installation of an NE.

Procedure

- 1 Choose **Administration > NE License Management** from the main menu.
- 2 In the **NE License Management** navigation tree, choose **NE License Maintenance**. On the **NE License Management** tab, click **Export NE Application Information**.
- 3 In the **Export NE Application Information** dialog box click **Select**.
- 4 In the **Select NE** dialog box, select an NE.
 1. Select the required NE software version from the **Select version** drop-down list in the **Available device** area.

2. In the **Select NE** dialog box, click , , , and  to select or remove devices from **Available device** and **Selected devices**. In the **Select NE** dialog box, click **OK**.
- 5 Click  next to **Select export file**. In the **Save** dialog box, set the file name and file path that are used for storing the application information of an NE license. Then click **Save**.
- 6 In the **Export NE Application Information** dialog box, click **OK**. The system exports the NE application information to the specified location and provides a prompt.
- 7 Send the exported NE application information to Huawei technical support engineers to apply for an NE license.

----End

4.16.4 Installing an NE License

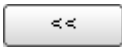
Functions are running properly only after you install a valid license for an NE.

Prerequisite

The NE file Huawei technical support engineers applied for by license exists on the local host.

Procedure

- 1 Choose **Administration > NE License Management** from the main menu.
- 2 In the **NE License Management** navigation tree, choose **NE License Maintenance**.
- 3 Click **Load License File**. In the **Load License File** dialog box, click . In the **Open** dialog box, select a license file and click **Open**. Then click **Next**.

license File Format	Loading Mode	Operation
TXT or DAT	Single	If the U2000 fails to automatically identify the NE matching with a license, do as follows to manually match the license with the NE: 1. In the Load License File dialog box, click Select. 2. In Select NE, change the version in the Select version drop-down list. a. Click , , , or  to change the devices in Selected devices. Then click OK. b. In the Load License File dialog box, click Finish.

license File Format	Loading Mode	Operation
ZIP	Batch	- On the right of the Load License File dialog box, right-click a license file and choose Match. - In the Select NE dialog box, select an NE to be matched. Then click OK. In the Load License File dialog box, the ESN Name column displays the matched NE. - In the Is Loaded column, select the license file to be loaded. - Click Finish.

 NOTE

In the steps for matching an NE, the matched license file list is displayed on the right of the **Load License File** dialog box.

----End

4.16.5 Synchronize NE Information

You can upload the ESN and license information of an NE to the U2000. This function is applicable when an NE accesses the U2000 or after communications recovery after network disconnection between an NE and the U2000.

Procedure

- Choose **System > NE License Management** from the main menu.
- In the **NE License Management** navigation tree, choose **NE License Maintenance**.
- Click **Synchronize NE Information**.
- In the **Synchronize NE Information** dialog box, click **Select**.
- In the **Select NE** dialog box, set the device for which you want to synchronize the NE information. Click **OK** to go back to the **Synchronize NE Information** dialog box.

 NOTE

Set the selected device: In the **Select NE** dialog box, click , , , or  to modify the NEs in **Available devices**.

- In the **Synchronize NE Information** dialog box, click **OK** to synchronize the NE information.

----End

4.16.6 Adjusting the NE License Capacity

You can adjust the capacity in an NE license to improve the license usage and reduce the maintenance cost of the carrier.

Prerequisite

The Huawei technical support engineers provides a valid NE license.

Context

- The U2000 supports the exchange of license capacities among different NEs. For example, a carrier has NE A and NE B. The capacities specified in the licenses of both NEs are 50. According to the service requirements, the capacity for NE B needs to increase to 80, and that for NE A needs to decrease to 20. In the precondition that the total capacity specified in the licenses of the carrier is unchanged, you can add the redundant capacity in the license of NE A to the license of NE B by using the NE license capacity exchange function.
- When you adjust the NE license capacity, it changes the state of the old license to No valid license file, and then applies the new NE license. After that, the adjustment is complete.

Procedure

- 1 Choose **Administration > NE License Management** from the main menu.
- 2 In the **NE License Management** navigation tree, choose **NE License Maintenance**.
- 3 Click **Adjust License Capacity**, then click **Yes** in the displayed dialog box.
- 4 In the **Adjust License Capacity** dialog box, click **Select**. In the **Select NE** dialog box, move the NE to **Selected devices**. This indicates that you have selected the NE whose license you want to adjust. Click **OK**.
- 5 In the **Adjust License Capacity** dialog box, click  next to **Select export file** to set the name of the file to be saved, and save NE license information. Click **OK**.

NOTE

Export the NE license information that you will use when applying for a new NE license.

- 6 In the **NE License Management** window, click **Load License File** to add the NE license applied for to the U2000. For details, see [4.16.4 Installing an NE License](#).

----End

4.16.7 Changing an NE License

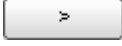
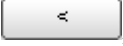
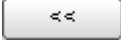
If an NE ESN changes or the capacity specified in a license is adjusted for the other NE, you need to change the NE license.

Prerequisite

The old NE license is invalidated. You can apply for an NE license only when the license invalidation file of the NE exists.

Procedure

- 1 Invalidate the old NE license.
 1. Choose **Administration > NE License Management** from the main menu.
 2. In the **NE License Management** navigation tree, choose **NE License Maintenance**.

3. Click **Invalidate License**.
 4. In the **confirm** dialog box, confirm that you want to invalidate the NE license.
 5. In the **Invalidate License** dialog box, click **Select**. In **Select NE**, change the version in the **Select version** drop-down list.
 6. Click , ,  or  to change the devices in **Selected devices**. Then click **OK**.
 7. Click . In the **Open** dialog box, select a path for exporting a file, and then enter the name of the file to be exported.
The invalidation information is exported to the file.
 8. In the **Invalidate License** dialog box, click **OK**.
- 2 Send the exported invalidation information in the file to Huawei technical support engineers so that Huawei technical support engineers can apply for an NE license.
- 3 Install the new NE license. For details, see [4.16.4 Installing an NE License](#).

----End

5 Backing Up and Restoring the U2000 Database

About This Chapter

To ensure the security of network data, the U2000 provides the function of backing up and restoring network data.

[5.1 Basic Concepts and Application Scenarios](#)

This topic describes basic concepts and application scenarios of backup and restoration of U2000 data.

[5.2 Methods of Backing Up and Restoring the U2000 Data](#)

This topic describes how to configure the policies for backing up and restoring data. You can back up and restore the U2000 data in two ways: Back up and restore all data in U2000 databases, and back up and restore the U2000 network configuration data by using scripts.

[5.3 Suggestions on Data Backup and Restoration](#)

This topic provides suggestions on backup and restoration of U2000 data.

[5.4 Backing Up U2000 Data to a Local Server](#)

This topic describes how to back up the U2000 data to a local server. The U2000 data backup is essential to restore the U2000 database safely and quickly.

[5.5 Backing Up U2000 Data to a Remote Server](#)

This topic describes how to back up the U2000 data to a remote server. The U2000 data backup is essential to restore the U2000 database safely and quickly.

[5.6 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.

[5.7 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.

[5.8 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.

5.9 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.

5.10 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.

5.11 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.

5.12 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.

5.13 Backing Up and Restoring the U2000 Network Configuration Data by Using Scripts

This topic describes how to back up and restore the U2000 network configuration data by using scripts.

5.14 Managing the U2000 Database

This topic describes how to manage the U2000 database. Managing the U2000 database includes initializing the U2000 database and checking the database status.

5.15 Setting Alarm/Event Timing Dump

The U2000 automatically dumps alarms or events based on the specified period. Dumped alarms/events are deleted from the database, thereby preventing insufficiency of database space.

5.16 Setting U2000 Log Timing Dumping

By setting U2000 log dump, you can periodically or instantly dump security logs, operation logs, and system logs of the U2000. The dumped logs are saved in files and deleted from the database. This prevents database space insufficiency.

5.17 Dumping Performance Data

This topic describes how to dump performance data. The performance data can be dumped in two modes, namely, automatic dumping and manual dumping.

5.1 Basic Concepts and Application Scenarios

This topic describes basic concepts and application scenarios of backup and restoration of U2000 data.

Basic Concepts

- Backup

Back up is a method used to store important data to prevent the damage of the original data. You can back up network configuration data, alarm data and performance data.

The U2000 provides the following schemes to backup the database: backup of the U2000 databases and the data by using scripts. For details on the differences between the three schemes, refer to the [5.2 Methods of Backing Up and Restoring the U2000 Data](#).

- Restoration

Restoration coexists with backup. When certain data is damaged or destroyed, you can restore the data.

Restoration is to restore database data from the backup file, and then overwrite the existing data file. Both backup and restoration are used to ensure the security of network data.

- Dump

Dump is a method used to store the log information in databases as operating system files in text format, to clear database space.

The dumped objects are various types of logs, including alarm events, abnormal events, operation logs and different types of performance events.

The U2000 provides three methods of dumping logs. The three methods are overflow dump, scheduled dump and immediate dump.

- The overflow dump is performed when the logs in the databases reach the maximum storage capacity. You can specify the number of logs to dump.
- The scheduled dump, which is the alternative method of overflow dump, is optional. You can set whether to create a scheduled task, and if you create a scheduled task you can specify the schedule time and duration.
- The immediate dump is also referred to as manual dump. This method is used to dump data that was created on a specific date.

The three methods of dumping logs automatically delete the corresponding data in databases. You can open a text file to view the log contents.

Application Scenarios

- Backup and restoration of U2000 data can be implemented in the following scenarios based on the OS type:
 - Single-server system (Solaris)
 - Single-server system (SUSE Linux)
 - Single-server system (Windows)
 - High availability system (Solaris)
 - High availability system (SUSE Linux)
 - High availability system (Windows)
- Backup and restoration of U2000 data can be implemented in the following scenarios based on the location of backup data:

- Local data backup and restoration

Data of a specific server is backed up to a local disk and the backup data is then used to restore U2000 data. For example, back up data of server A to disk D on server A, and then use the backup data on disk D to restore data of server A.

- Remote data backup and restoration

Data of the U2000 server is backed up to a remote server and the backup data on the remote server is then used to restore U2000 data. For example, back up data of server A to remote server B, and then use the backup data on remote server B to restore data of server A.

- Backup and restoration of U2000 data can be implemented in the following scenarios based on the source of data for restoration.

- Local data restoration

Backup data of the local server is used to restore server data. For example, use backup data of server A to restore data of server A.

- Remote data restoration

Backup data of another server is used to restore data of the specific server. For example, use backup data of server B to restore data of server A.

5.2 Methods of Backing Up and Restoring the U2000 Data

This topic describes how to configure the policies for backing up and restoring data. You can back up and restore the U2000 data in two ways: Back up and restore all data in U2000 databases, and back up and restore the U2000 network configuration data by using scripts.

Backing Up and Restoring the U2000 Databases

The U2000 databases are automatically created during the initial installation of the U2000. When you back up the U2000 databases, the databases are saved as operating system files. The information that is backed up includes the user-defined data at the U2000 side, network layer trail data, NE-side configuration data, alarm data and performance data. In addition, a backup is created for the structure of the entire database, all database tables (including the system tables and the user tables), table structure, and stored procedures.

**NOTE**

The following data is not backed up when you back up the U2000 database:

- The data that is not saved at the NE side, that is, the data that cannot be uploaded. For details, refer to the appendix **Configuration Data Management Information List** of the online help.
- The custom options of the system.

Importing and Exporting Script Files (This Function is Applicable Only to the Transport Domain)

The U2000 provides the function of exporting and importing script files, to back up and restore the network configuration data of the U2000. This realizes the upgrade of the configuration data with zero loss during the U2000 upgrade. For details, see [5.13 Backing Up and Restoring the U2000 Network Configuration Data by Using Scripts](#).

**NOTE**

- The default coding format in a script file is UTF-8. To change the coding format of the script file, in the Windows OS, you can change **encoding** configuration item in the **installation path of the NMS/server/cbb/trans/core/conf/xml/script/script_enum.xml** configuration file; In the Solaris or SUSE Linux OS, you can change **encoding** configuration item in the **installation path of the NMS/server/cbb/trans/core/conf/xml/script/script_enum.xml** configuration file.
- By default, the name of a script file contains the NE name. To exclude the NE name from a script file name, in the Windows OS, you can change the **scriptname** configuration item in the **installation path of the NMS/server/cbb/trans/core/conf/xml/script/script_enum.xml** configuration file. In the Solaris or SUSE Linux OS, you can change the **scriptname** configuration item in the **installation path of the NMS/server/cbb/trans/core/conf/xml/script/script_enum.xml** configuration file.
- The data are exported from the U2000 database.
- The imported script files update the data on the U2000 only, with no impact on the data on the NEs.

Comparison of Two Data Maintenance Methods

The characteristics of the two data maintenance methods determine their application scenarios. [Table 5-1](#) lists the characteristics and application scenarios of the three methods.

Table 5-1 Characteristics and application scenarios of two data maintenance methods

Method	Characteristics	Application Scenario
Backing up and restoring all data in the U2000 databases	● Backs up the structure and contents of the U2000 database. ● The data is in the binary mode. ● Backs up all data of the U2000 database. ● The processing speed is fast. ● The backup file is big.	● This requires a large storage medium space. If you want to back up the U2000 database in a scheduled manner, large-size disk is recommended. ● Backup data of an OS cannot be used for data restoration of another version or type of OS. ● Backup data of a database cannot be used for data restoration of another version or type of database.

Method	Characteristics	Application Scenario
Backing up and restoring the U2000 network configuration data by using the script files	● Exports the configuration data in the U2000 to a txt file that is similar to the MML format. This is done to save data. You can directly understand the configuration contents of the txt file. ● Backs up only some of the data, including the basic configuration data, port naming data and user-defined data. ● The processing speed is slow. ● The backup file is small.	● This method is usually used to upgrade the U2000. The new U2000 version is compatible with the scripts of the old version. ● This method is usually used to back up and restore the basic configuration data for a single NE. This method also restores the user-defined data.

5.3 Suggestions on Data Backup and Restoration

This topic provides suggestions on backup and restoration of U2000 data.

- When you install the U2000 for the first time, back up the U2000 databases. Back up the U2000 databases once, if you do not expand the databases. If the hard disk is large (if the available space exceeds 10 GB), you can back up the U2000 databases on a quarterly basis.
- Before backing up the data, upload the NE data, and perform the search of the protection subnets and trails.
- To avoid a situation in which data occupies too much disk space, clean the data that is previously backed up, on a regular basis.
- Before restoring U2000 databases, you must shut down the U2000 server and ensure that the databases are not used by other users.

5.4 Backing Up U2000 Data to a Local Server

This topic describes how to back up the U2000 data to a local server. The U2000 data backup is essential to restore the U2000 database safely and quickly.

[5.4.1 Periodically Backing Up the U2000 Data to a Local Server Through the U2000 Client](#)

This topic describes how to enable the periodically backup of the U2000 database to the local server. After this configuration, the database can be safely and quickly restored after a fault occurs.

[5.4.2 Immediately Backing Up the U2000 Database to a Local Server Through the U2000 Client](#)

When a fault occurs on the system, you can quickly restore system data by using the backup data of the database.

[5.4.3 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.

5.4.1 Periodically Backing Up the U2000 Data to a Local Server Through the U2000 Client

This topic describes how to enable the periodically backup of the U2000 database to the local server. After this configuration, the database can be safely and quickly restored after a fault occurs.

Prerequisite

- The database is running.
- Ensure that all users have been logged out of the NMS maintenance suite client.
- If you need to create a backup path in the Solaris OS or the SUSE Linux OS, log in to the OS as the **root** user, and then run the following commands to create a backup path and assign read, write, and execute rights to the backup path:

```
# mkdir backup path
```

```
# chmod -R 775 backup path
```

Context

- The time of executing the scheduled tasks of different types cannot be the same, neither can the involved NEs. Otherwise, task execution fails because of conflicts in obtaining resources.
- The U2000 does not support multiple periodic backup tasks at the same time. The difference between the time points to start scheduled tasks must be greater than the maximum running period of the tasks.
- It is recommended that you set the scheduled backup time to the time when network service traffic is light, such as at midnight.

Procedure

- 1 Log in to the U2000 client.

NOTE

The default user name is **admin** and password is null. When you log in to the system for the first time, the system requires you to change the password.

- 2 Choose **Administration > Task Schedule > Task Management** from the main menu.
- 3 Click **New**. The **New Task** dialog box is displayed.
- 4 Choose **Task Type > Backup**. Select **DB Backup** as the task type and enter a name for the scheduled task. Select **Once** or **Period** as the run type. Then click **Next**.
- 5 In **Time Setting**, set the planed start time of the task. If **Period** is selected, in **Period Setting**, set the planed period and execution times of the task. Then, click **Next**.

**CAUTION**

If multiple scheduled backup tasks are configured, ensure that times set for these tasks do not overlap; otherwise, backup fails.

- 6 Select **Back up the data to the local server** and enter a backup path on the local server. Then click **Finish**.

----End

Result

On the **Task Management** tab page, choose **Task Type > Backup > DB Backup** from the service tree. Then, the created task is displayed.

5.4.2 Immediately Backing Up the U2000 Database to a Local Server Through the U2000 Client

When a fault occurs on the system, you can quickly restore system data by using the backup data of the database.

Prerequisite

You must be an NM user with "NM maintainer" authority or higher.

Context

The backup process cannot be canceled once it is started.

Back up the database file to the default path as follows. The backed up data is generated in a folder named by time:

- On Solaris and SUSE Linux, back up the database file to the **installation path of the NMS/server/var/backup**.
- On Windows, back up the database file to the **installation path of the NMS\server\var\backup**.

Procedure

- 1 Log in to the U2000 client.

**NOTE**

The default user name is **admin** and password is null. When you log in to the system for the first time, the system requires you to change the password.

- 2 Choose **Administration > Back Up/Restore NMS Data > Database Backup** from the main menu.
- 3 Set the backup path on the server, and then click **Backup**. The U2000 atabase backup starts and a dialog box is displayed showing the backup progress.

 NOTE

Customizing a backup path helps to avoid the affect of system reinstallation and disk formatting on backup data. This improves the maintainability of the system.

The backup path should be short, and cannot contain any space, punctuation, or Chinese character.

----End

5.4.3 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 [C.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
```

- 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
```

5.5 Backing Up U2000 Data to a Remote Server

This topic describes how to back up the U2000 data to a remote server. The U2000 data backup is essential to restore the U2000 database safely and quickly.

5.5.1 Periodically Backing Up the U2000 Database to a Remote Server Through the U2000 Client

This topic describes how to enable periodical backup of the U2000 database to a remote server. After this configuration, the database can be safely and quickly restored after a fault occurs.

5.5.2 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.

5.5.1 Periodically Backing Up the U2000 Database to a Remote Server Through the U2000 Client

This topic describes how to enable periodical backup of the U2000 database to a remote server. After this configuration, the database can be safely and quickly restored after a fault occurs.

Prerequisite

- The database is running.
- All users have been logged out of the NMS maintenance suite (MSuite) client.
- 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 time of executing the scheduled tasks of different types cannot be the same, neither can the involved NEs. Otherwise, task execution fails because of conflicts in obtaining resources.
- The U2000 does not support multiple periodic backup tasks at the same time. The difference between the time points to start scheduled tasks must be greater than the maximum running period of the tasks.
- It is recommended that you set the scheduled backup time to the time when network service traffic is light, such as at midnight.

Procedure

- 1 Log in to the U2000 client.



NOTE

The default user name is **admin** and password is null. When you log in to the system for the first time, the system requires you to change the password.

- 2 Choose **Administration > Task Schedule > Task Management** from the main menu.
- 3 Click **New**. The **New Task** dialog box is displayed.
- 4 Choose **Task Type > Backup**. Select **DB Backup** as the task type and enter a name for the scheduled task. Select **Once** or **Period** as the run type. Then click **Next**.
- 5 In **Time Setting**, set the planed start time of the task. If **Period** is selected, in **Period Setting**, set the planed period and execution times of the task. Then, click **Next**.



CAUTION

If multiple scheduled backup tasks are configured, ensure that times set for these tasks do not overlap; otherwise, backup fails.

- 6 Select **Back up the data to the remote server** and enter a backup path on the remote server. Then click **Finish**.

----End

Result

On the **Task Management** tab page, choose **Task Type > Backup > DB Backup** from the service tree. Then, the created task is displayed.

5.5.2 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 [C.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.

- 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 where 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.

5.6 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.

5.6.1 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.

5.6.2 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.

5.6.1 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.9.9 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 [C.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 [C.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.9.8 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.

5.6.2 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.9.9 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 [C.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 [C.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.9.8 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.

5.7 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.

[5.7.1 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.

[5.7.2 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.

5.7.1 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.9.12 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 [C.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 [C.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.9.11 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.

5.7.2 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.9.12 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
```

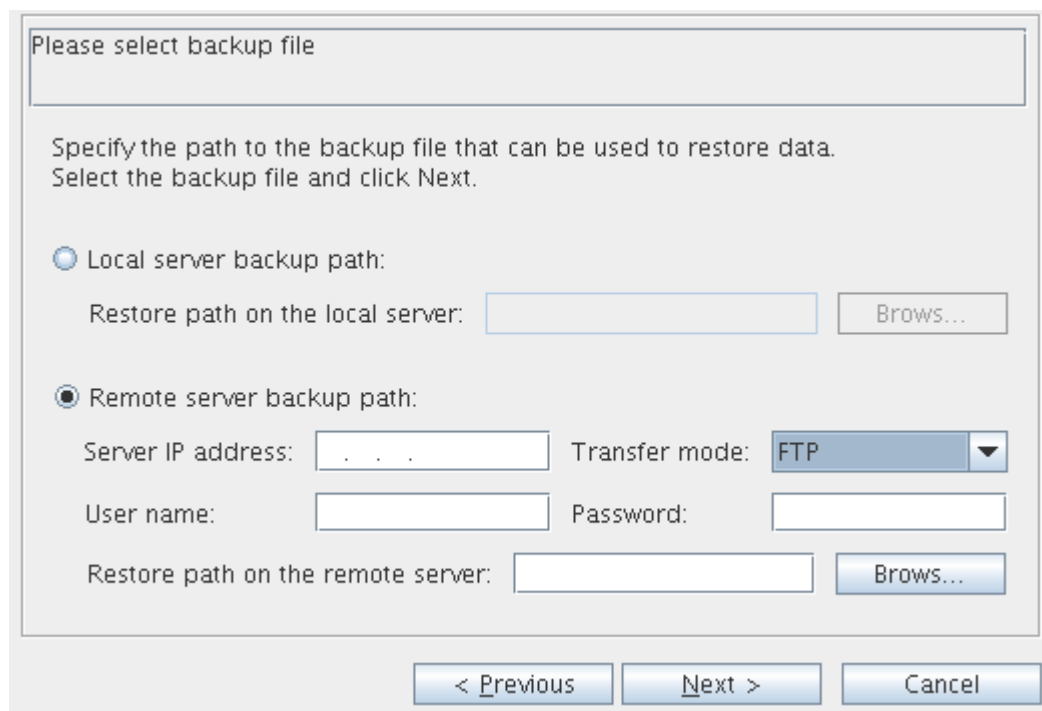
Procedure

- 1 Log in to the MSuite client. For details, see [C.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 [C.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.9.11 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.

5.8 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.

[5.8.1 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.

[5.8.2 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.

5.8.1 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.9.15 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.7.4 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 [C.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 [C.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.9.30 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.9.14 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.

5.8.2 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.9.15 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.7.4 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 [C.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 [C.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.9.30 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.9.14 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.

5.9 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.

5.9.1 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.

5.9.2 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.

5.9.1 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.9.18 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 [5.12 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 [C.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

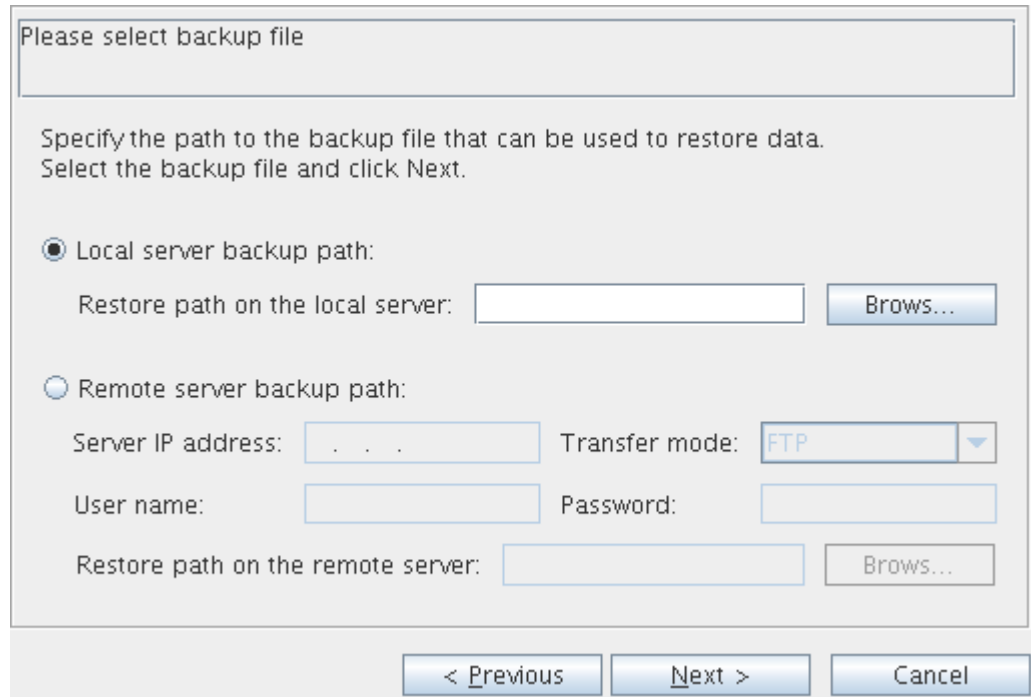
Data Restore-Text Mode is only used to locate and rectify the fault. This mode is not recommended during routine database restore.

- 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 [C.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.9.17 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.

5.9.2 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.9.18 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 [5.12 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 [C.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 [C.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.9.17 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.

5.10 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.

[5.10.1 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.

[5.10.2 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.

5.10.1 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.9.21 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 [5.12 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 [C.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 [C.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.9.20 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.

5.10.2 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.9.21 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



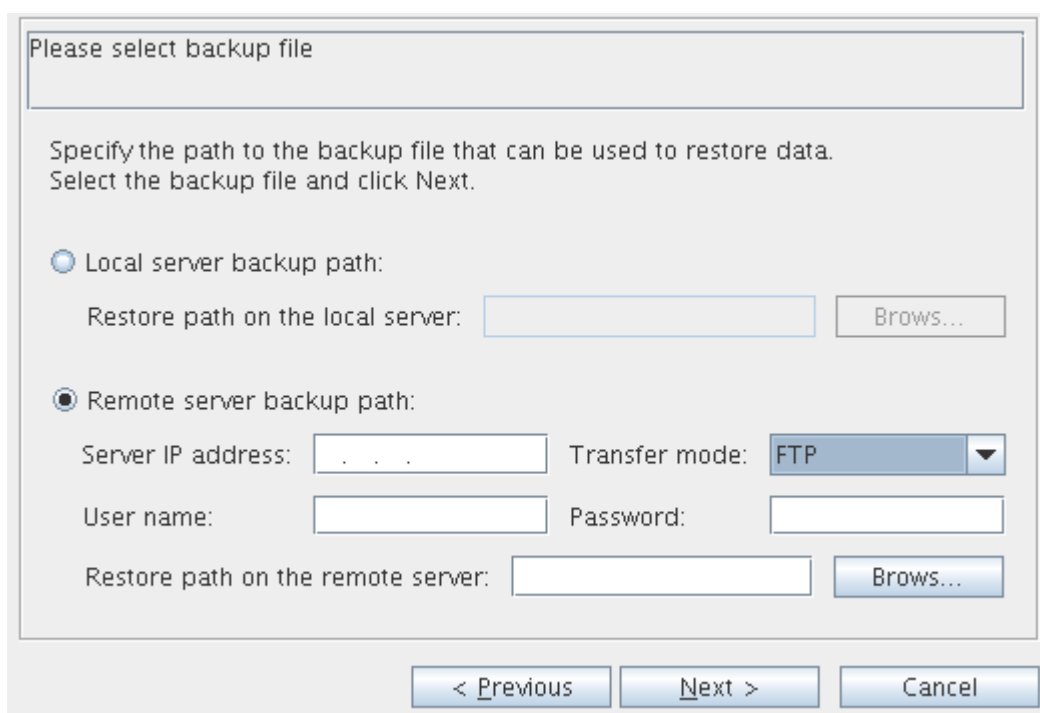
CAUTION

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 [5.12 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 [C.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.



- 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 [C.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.9.20 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.

5.11 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.

5.11.1 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.

5.11.2 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.

5.11.1 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.9.24 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.7.4 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 [5.12 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 [C.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 [C.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.9.30 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 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.

5.11.2 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.9.24 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.7.4 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 [5.12 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 [C.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.

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 [C.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.9.30 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 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.

5.12 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 [C.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 [5.9 Restoring U2000 High Availability System \(Windows\) Data](#).
 - For details about restoring data for the High Availability System (Solaris), see [5.10 Restoring U2000 High Availability System \(Solaris\) Data](#).
 - For details about restoring data for the High Availability System (SUSE Linux-Distributed), see [5.11 Restoring U2000 High Availability System \(SUSE Linux-Distributed\) Data](#).
- 3 Connect the primary and secondary sites. For details, see [C.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.

5.13 Backing Up and Restoring the U2000 Network Configuration Data by Using Scripts

This topic describes how to back up and restore the U2000 network configuration data by using scripts.

**CAUTION**

Not all U2000 data can be backed up or restored by using scripts. Instead, backing up and restoring all data in the U2000 database is recommended.

Using scripts to back up and restore data makes the following impacts:

- NBIs are affected. The upper-layer OSS must use physical IDs or logical IDs of NEs as indexes to interwork with the U2000. During U2000 upgrade, physical IDs of NEs are constant and logical IDs are assigned by the U2000 again. Physical IDs are recommended if the U2000 is interconnected to an upper-layer OSS. If the upper-layer OSS uses logical IDs as indexes, NEs must be uploaded after data restoration. Fibers/cables, subnets, and optical NEs have only logical IDs. If the upper-layer OSS uses data about the fibers/cables, subnets, or optical NEs, the fibers/cables, subnets, or optical NEs must be uploaded again.
- Only basic information is stored in scripts, whereas other information must be obtained by uploading NEs. Therefore, you must manually restore customized information that is stored on neither NEs nor scripts; otherwise, the information will be lost. Information that requires manual restoration includes but is not limited to:
 - Customized information (background and sound configurations) on clients
 - Alarm performance template configurations
 - Security information, such as NMS user name and password
 - Path naming rule
 - ACL
- The following information cannot be restored manually or using scripts. It is recommended that you dump the information before restoration by using the dumping function of the U2000.
 - History alarm
 - History performance
 - U2000 operation log
 - Abnormal event

5.13.1 Script Files

When you upgrade the U2000, you can upgrade the configuration data with zero data loss by importing and exporting the scripts. Script files that contain the basic data are required for importing and exporting scripts.

5.13.2 Immediately Backing Up the U2000 Data by Script

Before upgrading the U2000, you must export the data from the database to script files and save these files to import the data back to the U2000 after the upgrade.

5.13.3 Backing Up the U2000 Data Through Script Exporting in a Scheduled Manner

In routine maintenance, you can use the scheduled task function to export network configuration data as script files in a scheduled manner to ensure timely backup of customized information. In addition, this function can be performed without any manual intervention and thus reduces maintenance costs.

5.13.4 Restoring the U2000 Data by Using the Script

After upgrading the U2000, you can restore the U2000 network layer configuration data from the backup script files.

5.13.1 Script Files

When you upgrade the U2000, you can upgrade the configuration data with zero data loss by importing and exporting the scripts. Script files that contain the basic data are required for importing and exporting scripts.

Script File Type

Table 5-2 lists the types of the script files in the .txt format that the U2000 provides and the contents of the data.

Table 5-2 Script files the U2000 provides

Script File Type	Naming Rule	Contained Data	Whether the Import or Export Feature Is Supported
Networkwide Configuration File	None	The networkwide configuration file is the whole set of the following script files. When the network-wide configuration file is exported, the NE port naming file, NE configuration file, NE list file, network layer information file, and other scripts are exported. When the network-wide configuration file is imported, the NE configuration file and the NE port naming file are imported in sequence according to the NEs contained in the NE list file. The network layer information file is also imported.	This file can be imported and exported.
NE Port Naming File	NEPort_extension ID-basic ID_NE name_coding format.txt	This file contains the naming information about every port on the NE.	This file can be imported and exported.

Script File Type	Naming Rule	Contained Data	Whether the Import or Export Feature Is Supported
NE Configuration File	NEData_extension ID-basic ID_NE name_coding format.txt	This file contains the configuration information that is similar to the command lines. The configuration information contains all data that is required to recreate an NE and to ensure that the NE is functioning normally. The version and manufacturing information of the board are listed at the end of the file.	This file can be imported and exported.
NE List File	NWNeList_U2000 name_coding format.txt	This file contains information about NEs, U2000, and their physical location. When the NE list file is imported or exported, the NE port naming file and the NE configuration file are imported or exported in sequence according to the NE list file.	This file can be imported and exported.

Script File Type	Naming Rule	Contained Data	Whether the Import or Export Feature Is Supported
NM Computer Information File	NMInfo_U2000 name_coding format.txt	This file contains the configuration information about the U2000 server. The configuration information is as follows: ● Hardware information such as the operating system name and its version, operating system patch version, physical memory, CPU count and frequency ● Network information such as the host name and IP address ● Database information such as the database name and its version	This file can be exported but cannot be imported. NOTE It can be used to import third-party software such as MDS.

Script File Type	Naming Rule	Contained Data	Whether the Import or Export Feature Is Supported
Service Actualization Script	NWSvcData_U2000 name_coding format.txt	This file provides service actualization data scripts for the transport service actualization system. The service actualization data scripts are as follows: ● NE attributes ● Board installation ● Board protection ● Protection relationship ● Service configuration ● Protection subnets ● Trail configuration	This file can be exported but cannot be imported.
Network Layer Information File	NWCfg_U2000 name_coding format.txt	This file contains information on the network layer configuration, including the following: ● Fiber cable connections ● Protection subnets ● Trail configuration	This file can be imported and exported.
Network Modeling and Design Information File	None	This file contains information on MDS network modeling and design.	This file can be imported and exported.
CEAS	NEDData_extension ID-basic ID_NE name_coding format.txt	This file provides scripts for the operation that is performed on multiple NEs in batches.	This file can be exported but cannot be imported.

In addition, the U2000 provides the script files in the .xml format for the network planning and design, containing the network-wide configuration file, NE configuration file, network layer information file, and ASON information file. The ASON information file can be imported and exported, but other types of script files in the .xml format can be exported only.

 NOTE

- The default coding format in a script file is UTF-8. To change the coding format of the script file, you can change **encoding** configuration item in the **installation path of the NMS/server/cbb/trans/core/conf/xml/script/script_enum.xml** configuration file.
- By default, the name of a script file contains the NE name. To exclude the NE name from a script file name, you can change the **scriptname** configuration item in the **installation path of the NMS/server/cbb/trans/core/conf/xml/script/script_enum.xml** configuration file.

Main Usage

The main usage of the script files is as follows:

- Realizing the upgrade of the configuration data with zero loss during the U2000 upgrade. This is an important method for the U2000 upgrade. This is the main usage of the script files.
- After the network data is modified, restoring the customized information of the U2000, such as the trail name, fiber name, port name, and the customer information.
- By modifying the script files, realizing the division and combination of the U2000 data and realizing the import of the desired data only, such as the NE list (with no configuration data), fiber connection, protection subnet, or trail.
- Supporting the simplified implementation of the project design.

Compatibility

- The scripts exported from the U2000 of an earlier version can be imported to the U2000 of a later version. But an error may occur if the scripts exported from the U2000 of a later version is imported to the U2000 of an earlier version. The U2000 of an earlier version does not support the features and functions that are added and the parameters that are modified in the U2000 of a later version. After the scripts are imported, an error message is displayed. But this does not affect the import of other information.
- The scripts generated on Windows and on UNIX are compatible.

Application

During the network adjustment, such as adding or deleting a node in the network, if the fiber connection is deleted, the protection subnet and trail carried on the fiber are deleted from the network layer of the U2000. After the network adjustment, if the source and sink ports of the trail are not changed, you can find the trail again by performing the trail search. But the original customized information of the trail, such as the trail name, customized information of the trail, and remarks, cannot be restored through the search.

To restore the customized information of the trail, you need:

1. Before the network adjustment, export the network layer information file.
2. After the network adjustment, import the network layer information file.

**NOTE**

- When the source and sink ports of the trail are not changed after the network adjustment, you can use the scripts to restore the customized information. Otherwise, you need restore the customized information manually.
- When the network layer information file is imported after the network adjustment, errors may be displayed for part of the data, because certain objects, such as NEs, boards, and ports, are changed. This does not affect the restoration of the customized information.

5.13.2 Immediately Backing Up the U2000 Data by Script

Before upgrading the U2000, you must export the data from the database to script files and save these files to import the data back to the U2000 after the upgrade.

Prerequisite

- You must be an NM user with "NM maintainer" authority or higher.
- Before you export the script files, you must check the consistency of the configuration data to ensure that the configuration data in the U2000 is consistent with that in the NE.

Procedure

- 1 Log in to the U2000 client.

**NOTE**

The default user name is **admin** and password is null. When you log in to the system for the first time, the system requires you to change the password.

- 2 Choose **Administration > Back Up/Restore NMS Data > Import/Export Script File** from the main menu.
- 3 Click the **Export** option button.
- 4 Click the **TXT** or **XML** option button.
- 5 Select a script file type from the **Script File Type** field. For details, see [5.13.1 Script Files](#).

**NOTE**

- To export the networkwide script file, select **Networkwide Configuration File**. Export the following files to a specified directory: **NWCfg_NM Name.txt**, **NWNeList_NM Name.txt**, **NEPort_Port ID-Basic ID_NE Name.txt**, and **NEData_Extended ID-Basic ID_NE Name.txt**.
- The following script types are available for the export: **Networkwide Configuration File**, **NE Port Naming File**, **NE Configuration File**, **NE List File**, **NM Computer Information File**, **Service Actualization Script**, **Network Layer Information File**, **Network Modeling and Design Information File**, and **CEAS**.

- 6 Select the NE for which you want to export script files from the **Export NE List**.

**NOTE**

Specify the NE only when you export the **NE Configuration File**, **NE List File**, **NE Port Naming File**, **Networkwide Configuration File** and **CEAS**.

- 7 Click **Create File Directory** to create a directory where the exported script files are to be saved.

**NOTE**

The script file is saved on the U2000 server. On Windows, the backup directory is **installation path of the NMS\server\script**. On Solaris and SUSE Linux, the backup directory is **installation path of the NMS/server/script**. You can create a new directory under it.

- 8 Enter the directory name and click **OK**.
- 9 Select the created directory and click **Apply**.
- 10 In the **Confirm** dialog box, click **OK**.
A progress bar appears showing the status of the export.

----End

5.13.3 Backing Up the U2000 Data Through Script Exporting in a Scheduled Manner

In routine maintenance, you can use the scheduled task function to export network configuration data as script files in a scheduled manner to ensure timely backup of customized information. In addition, this function can be performed without any manual intervention and thus reduces maintenance costs.

Prerequisite

You must be an NM user with "NM maintainer" authority or higher.

Context

- The time of executing the scheduled tasks of different types cannot be the same, neither can the involved NEs. Otherwise, task execution fails because of conflicts in obtaining resources.
- The U2000 does not support multiple periodic backup tasks at the same time. The difference between the time points to start scheduled tasks must be greater than the maximum running period of the tasks.
- It is recommended that you set the scheduled backup time to the time when network service traffic is light, such as at midnight.

Procedure

- 1 Log in to the U2000 client.

 NOTE

The default user name is **admin** and password is null. When you log in to the system for the first time, the system requires you to change the password.

- 2 Choose **Administration > Task Schedule > Task Management** from the main menu.
- 3 Click **New**. The **New Task** dialog box is displayed.
- 4 Select **Script Export** as the task type and enter a name for the scheduled task. Select **Period** as the run type. Then click **Next**.
- 5 In **Time Setting**, set the planed start time of the task.
- 6 In **Period Setting**, set the execution interval and execution times of the task. Then, click **Next**.
- 7 Select the NEs and the type of the script file to be exported. For details, see [5.13.1 Script Files](#). Then click **Finish**. Then the created scheduled task is displayed in the **Task Management** window.

----End

5.13.4 Restoring the U2000 Data by Using the Script

After upgrading the U2000, you can restore the U2000 network layer configuration data from the backup script files.

Prerequisite

- The NMS subsystem deployment during data restoration must be the same as the that during data backup.
- You must be an NM user with "NM maintainer" authority or higher.
- You must have the license for the U2000 script import.

Context



CAUTION

Before importing the script file, you need to back up the U2000 database, and then initialize the U2000 database. Then, import the configuration file. It is recommended that you import the network-wide configuration file. You can restore the data from a backup file if you failed to import the script file.

Procedure

- 1 Log in to the U2000 client.



NOTE

The default user name is **admin** and password is null. When you log in to the system for the first time, the system requires you to change the password.

- 2 Choose **Administration > Back Up/Restore NMS Data > Import/Export Script File** from the main menu.
- 3 Click the **Import** option button.
- 4 Click the **TXT** or **XML** option button.
- 5 Select the script file type from the **Script File Type** field.



NOTE

Service Actualization Script and **NM Computer Information File** are not supported.

- 6 In the **Operation Directory List**, select the directory where the script file is to be imported is located.
- 7 Select the script file to import from the **Import File List**.
- 8 In the **Import Subnet List**, select the sunbets to be imported. All subnets are required to be selected.
- 9 Click **Apply**. The system prompts you twice that the import of the configuration script will result in data inconsistency between the U2000 and the NE.
- 10 Click **OK**. A progress bar appears showing the status of the import.

----End

5.14 Managing the U2000 Database

This topic describes how to manage the U2000 database. Managing the U2000 database includes initializing the U2000 database and checking the database status.

5.14.1 U2000 Database List

This topic describes the list of databases and function for the U2000. The database files of the U2000 server are used to store data or store the log information that is generated during the running of the database.

5.14.2 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.

5.14.3 Checking the Database Status

This topic describes how to check the database status. The NMS is unavailable if the database capacity exceeds the standard value. It is recommended that you check the database status periodically to ensure the normal running of the NMS.

5.14.1 U2000 Database List

This topic describes the list of databases and function for the U2000. The database files of the U2000 server are used to store data or store the log information that is generated during the running of the database.

Table 5-3 shows the descriptions of databases for the U2000.

Table 5-3 U2000 database list

Database Name	Function
MCDB	Distribution Manager Database
InventoryDB	Inventory Manage system Database
ReportDB	Report Manage system Database
BMSDB	Access Service Management Database
nemgr_sdhDB	SDH NE Management Database
nemgr_rtnDB	RTN NE Management Database
ason_sdh_db	ASON SDH Management Database
ason_wdm_db	ASON WDM Management Database
nemgr_ngwdmDB (nemgr_otnDB)	OTN NE Management Database
TransPerfDB	Transmits Perfomance Manage system Database
nemgr_wdmDB	WDM NE Management Database

Database Name	Function
nemgr_extDB	Extended NE Management Database
nemgr_ngwdmaDB (nemgr_naotnDB)	NAOTN NE Management Database
nemgr_nawdmDB	NAWDM NE Management Database
nemgr_marineDB	Marine NE Management Database
ason_naotn_db	ASON NAOTN Management Database
ason_otn_db	ASON OTN Management Database
OAMSDB	OAMS Management Database
nemgr_ptnDB	PTN/ATN Service Management Database
TNCOMMONDB	Service Management Base Component Database
TNSDHDB	SDH Service Management Database
TNOTNDB	WDM Service Management Database
TNETHDB	MSTP Service Management Database
TNIPDB	IP Service Management Database
TNCPSDB	Composite Service Management Database
IPCommonDB	IP Common Application Database
IPBaseDB	IP Base Service Database
RouterMgrDB	Router Manage System Database
SgMgrDB	Service Gateway Manage System Database
GctlDB	General configuration template Database
DmsBatchConfigDB	IP domain Batch Config Database
DmsNetAclDB	IP domain NetAcl Database
FrameSWMgrDB	Switch NE Manager(Frame) Database
BoxSwitchMgrDB	Switch NE Manager(Box) Database
SecurityMgrDB	Security NE Database
SecServiceDB	Security Service Database
PMSDB	Perfomance Manage system Database
XFTPDB	XFTP Database
EnpowerDB	Environment Power Database
ALARMDB	Database of FaultService
IMAPEAMDB	Database of EAMService

Database Name	Function
IMAPLOGDB	Database of LogService
IMAPSMDB	Database of SecurityService
IMAPTEMPDB	Temporary Database
IMAP_DB	Common Database
IMAPTMDB	Database of TopoService

5.14.2 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.9.9 How to End the Processes of the U2000 Single-Server System on Windows](#).
 - For the Single-Server System (Solaris), see [A.9.12 How to End the Processes of the U2000 Single-Server System on Solaris](#).
 - For the Single-Server System (SUSE Linux-Distributed), see [A.9.15 How to End the Processes of the U2000 Single-Server System \(SUSE Linux-Distributed\)](#).
 - For the High Availability System (Windows), see [A.9.18 How to End the U2000 Processes of the High Availability System \(Windows\)](#).
 - For the High Availability System (Solaris), see [A.9.21 How to End the U2000 Processes of the High Availability System \(Solaris\)](#).
 - For the High Availability System (SUSE Linux-Distributed), see [A.9.24 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.7.4 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.7.3 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. For more information, see [9.3.3 Locking a 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 [C.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. For more information, see [9.3.4 Unlocking a Resource Group](#).

----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. For more information, see [1 Starting the U2000 System](#).

5.14.3 Checking the Database Status

This topic describes how to check the database status. The NMS is unavailable if the database capacity exceeds the standard value. It is recommended that you check the database status periodically to ensure the normal running of the NMS.

Prerequisite

- The U2000 server runs in the normal state.
- The system monitoring process runs in the normal state.
- The System Monitor communicates well with the U2000 server.
- You have a valid user account and password of the U2000.

Context

If **Data Used Rate** or **Log Used Rate** of the database exceeds the preset alarm threshold, the system monitoring process sends an alarm to the NMS server and the related record on the System Monitor turns red.

Procedure

- 1 **Optional:** In the Windows OS, choose **Start > Programs > Network Management System > U2000 System Monitor** or double-click the shortcut icon on the desktop to start the System Monitor.
- 2 **Optional:** In the Solaris OS, on the **Java Desktop System, Release 3**, double-click the **U2000 System Monitor** shortcut icon.
- 3 **Optional:** In the SUSE Linux OS, on the local client desktop, double-click the **U2000 System Monitor** shortcut icon.
- 4 In the **Login** dialog box, enter the required user name and password to access the System Monitor window.
- 5 Click **Login** to log in to the System Monitor of the U2000.
- 6 Click the **Database** tab and view the data space, remaining data space, data space usage, log space, remaining log space, and log space usage of the database.

----End

5.15 Setting Alarm/Event Timing Dump

The U2000 automatically dumps alarms or events based on the specified period. Dumped alarms/events are deleted from the database, thereby preventing insufficiency of database space.

Context

The alarm/event timing dump is performed everyday and the alarm/event overflow dump is performed every 10 minutes. In this way, these two actions may be performed at the same time. As performing these two actions deletes the data of one table, if these two actions are performed at the same time, task execution failure alarm is generated. Therefore, you need to set the start time of these two actions to be different. For example, the start time of the alarm/event timing dump is set to 2007-01-01 10:05:00 whereas the start time of the alarm/event overflow dump is set to 2007-01-01 10:00:00. The interval between two actions is five minutes, so they can be performed at different time.

Procedure

- 1 Choose **Administration > Task Schedule > Task Management** from the main menu.
- 2 In the **Task Management** window, choose **Database Capacity Management** in the navigation tree.
- 3 In the **Task Management** window, double-click the **Alarm/Event Log Dump** task in the task list.

The screenshot shows a configuration window for the 'Alarm/Event Log Dump' task. It has two tabs: 'Common Parameters' (selected) and 'Extended Parameters'. The 'Basic Information' section contains the following fields:

- Task name: Alarm/Event Log Dump
- Run type: Period (dropdown menu)
- Start time: 01/01/2007 13:00:00 (calendar/time picker) with a checkbox for DST.
- Task type: Alarm/Event Log Dump

The 'Period Information' section contains the following fields:

- No. of periods: 1 (text input) with a dropdown menu set to 'days'.
- No. of run times: 0 (text input) with a note: '{Zero indicates No. of Run times is not limited.}'

At the bottom right, there are 'OK' and 'Cancel' buttons.

- 4 In the **Attribute** dialog box, modify common and extended parameters.
- 5 Click **OK**.

----End

5.16 Setting U2000 Log Timing Dumping

By setting U2000 log dump, you can periodically or instantly dump security logs, operation logs, and system logs of the U2000. The dumped logs are saved in files and deleted from the database. This prevents database space insufficiency.

Context

Each of the types **Operation Log Dump**, **Security Log Dump** and **System Log Dump** has a default system task that is provided by the U2000. You are not allowed to delete this system task, but you can modify its setting. In addition, you cannot create new tasks of these three types.

Procedure

- 1 Choose **Administration > Task Schedule > Task Management** from the main menu.
- 2 In the **Task Type** navigation tree, choose **Database Capacity Management > Alarm/Event Log Dump**, **Database Capacity Management > Operation Log Dump**, **Database Capacity Management > Security Log Dump** or **Database Capacity Management > System Log Dump**.
- 3 Double-click the task in the task list.



NOTE

In the task list, right-click the log dump task and choose **Run At Once**. The log dump task is performed instantly.

- 4 In the displayed **Attribute** dialog box, set the parameters on the **Common Parameters** and **Extended Parameters** tabs.
- 5 Click **OK**.

----End

5.17 Dumping Performance Data

This topic describes how to dump performance data. The performance data can be dumped in two modes, namely, automatic dumping and manual dumping.

5.17.1 Dumping Performance Data Manually

This topic describes how to dump performance data manually. This operation enables you to configure the user-defined conditions to dump the performance data manually.

5.17.2 Dumping Performance Data Automatically

This topic describes how to dump performance data automatically. This operation enables you to configure the default condition to automatically dump the performance data.

5.17.1 Dumping Performance Data Manually

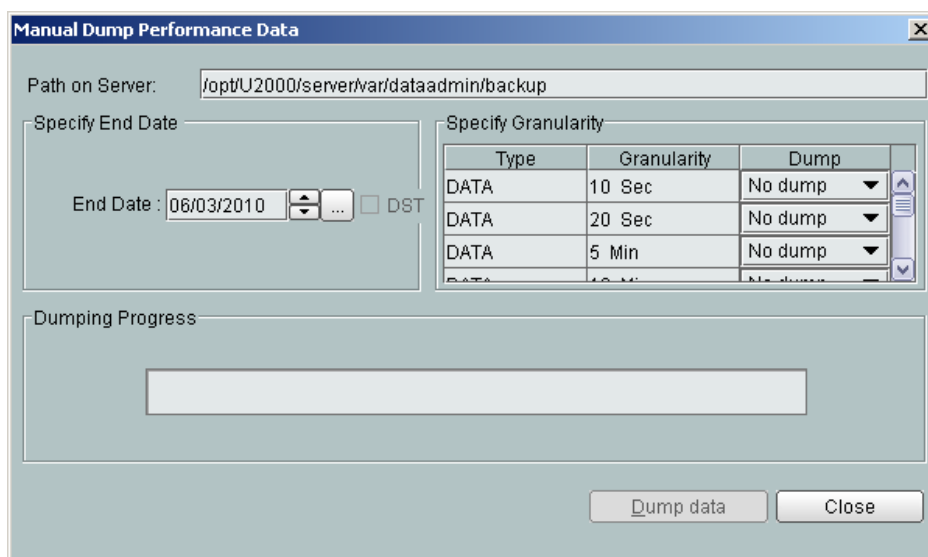
This topic describes how to dump performance data manually. This operation enables you to configure the user-defined conditions to dump the performance data manually.

Prerequisite

- Performance data for at least one day exists.
- There is sufficient memory to save the dumped performance data.

Procedure

- 1 Choose **Performance > Performance Dump Management > Manual Dump Performance Data** from the Main Menu.
- 2 In the **Path on the server** text box, enter the path to save the dumped performance data.
- 3 In the **Specify the end date** area, click  to select the end date to dump the performance data.



- 4 In the **Specify Granularity** area, in the **Dump** drop-down list, select the dump mode for different granularities.

Granularities are 5 minutes, 10 minutes, 15 minutes, 30 minutes, 1 hour, and 1 day.

Dump can be classified as no dump, dump to file, and delete.

- 5 Click **Dump data** to dump the performance data.

The progress bar displays the status of the number of total records and the number of dumped records.

- 6 A dialog box is displayed, prompting that the operation succeeds. Click **OK**.

----End

5.17.2 Dumping Performance Data Automatically

This topic describes how to dump performance data automatically. This operation enables you to configure the default condition to automatically dump the performance data.

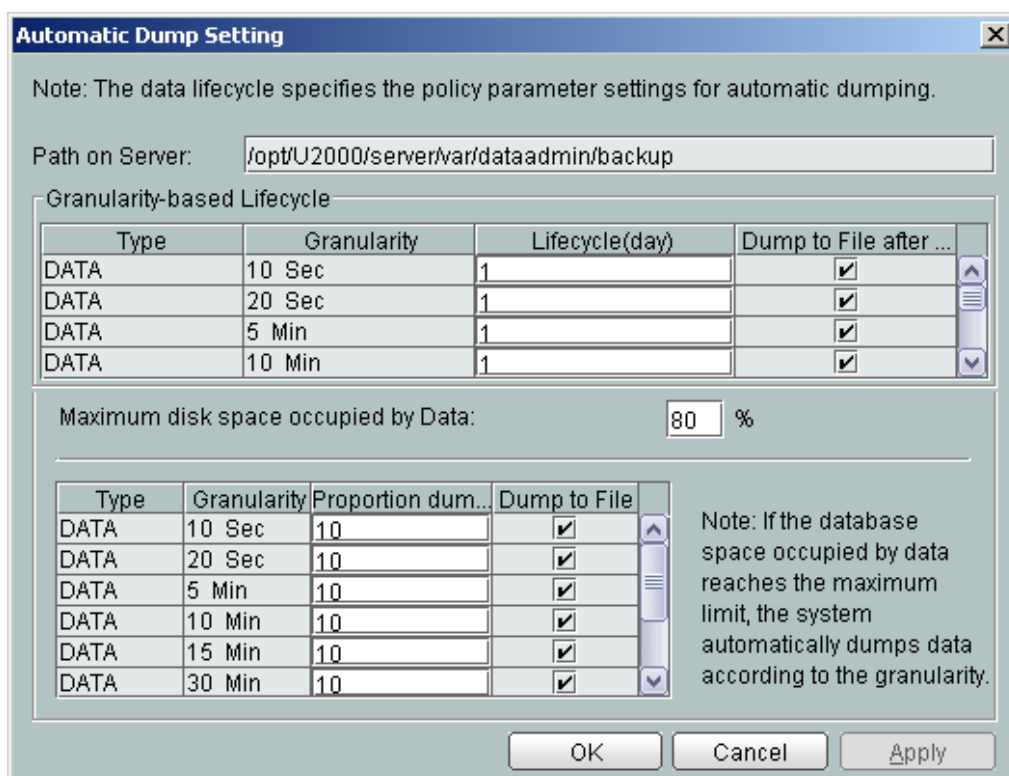
Prerequisite

- Performance data for at least one day exists.
- There is sufficient memory to save the dumped performance data.

Procedure

- 1 Choose **Performance > Performance Dump Management > Automatic Dump Setting** from the Main Menu.
- 2 In the **Path on Server** text box, enter the path to save the dumped performance data.
- 3 In the **Granularity-based Lifecycle** area, in the **Lifecycle(day)** text box, enter the number of days according to the granularity.

Granularities are 10 seconds, 20 seconds, 5 minutes, 10 minutes, 15 minutes, 30 minutes, 1 hour, and 1 day.



The dialog box titled "Automatic Dump Setting" contains a note: "Note: The data lifecycle specifies the policy parameter settings for automatic dumping." Below this, the "Path on Server" is set to "/opt/U2000/server/var/dataadmin/backup". The "Granularity-based Lifecycle" section features a table with columns: Type, Granularity, Lifecycle(day), and Dump to File after The table lists four entries for "DATA" with granularities of 10 Sec, 20 Sec, 5 Min, and 10 Min, each with a lifecycle of 1 day and the "Dump to File after ..." checkbox checked. Below this table, a field for "Maximum disk space occupied by Data:" is set to 80 %. Another table lists granularities from 10 Sec to 30 Min, each with a "Proportion dum..." field set to 10 and the "Dump to File" checkbox checked. A note on the right states: "Note: If the database space occupied by data reaches the maximum limit, the system automatically dumps data according to the granularity." At the bottom are "OK", "Cancel", and "Apply" buttons.

Type	Granularity	Lifecycle(day)	Dump to File after ...
DATA	10 Sec	1	☒
DATA	20 Sec	1	☒
DATA	5 Min	1	☒
DATA	10 Min	1	☒

Maximum disk space occupied by Data: 80 %

Type	Granularity	Proportion dum...	Dump to File
DATA	10 Sec	10	☒
DATA	20 Sec	10	☒
DATA	5 Min	10	☒
DATA	10 Min	10	☒
DATA	15 Min	10	☒
DATA	30 Min	10	☒

Note: If the database space occupied by data reaches the maximum limit, the system automatically dumps data according to the granularity.

- 4 Select **Dump to File after Lifecycle** check box to save the dumped performance data from the database to a file or from one file to another file in **Path on Server** path.



NOTE

If you do not select the **Dump to file after lifecycle** check box, the performance data is deleted without being saved.

- 5 In the **Proportion dumped(%)** text box, enter the percentage of performance data to be dumped according to the granularity.

Granularities are 5 minutes, 10 minutes, 15 minutes, 30 minutes, 1 hour, and 1 day.

**NOTE**

For dumping the performance data from database to file, **Maximum disk space occupied by Data** specifies the percentage of performance data retained in the database.

- 6 Select **Dump to File** check box to save the dumped performance data from the database to a file or from one file to another file mentioned in **Path on Server** path.

If you do not select the **Dump to file** check box, the performance data is deleted from the database without being saved.

- 7 Click **Apply** or **OK**.

----End

Example

- If the number of days in the **Lifecycle(day)** text box is 2 days for 15 minutes granularity, the latest 2 days performance data is stored and the remaining data is dumped.
- For performance data dump from database to file, if the performance data for the last 2 days exceeds the percentage of performance data in **Maximum disk space occupied by Data** and if the percentage of performance data in **Proportion dumped(%)** text box is 10, the oldest 10 percent performance data is dumped from the database.

6 Managing U2000 Files and Disks

About This Chapter

This topic describes how to manage the system files and disks of the U2000.

[6.1 U2000 File System Overview](#)

This topic describes the system architecture of the U2000, which is based on the client/server model, and the file system of the U2000.

[6.2 Single-Server System \(Windows\)](#)

This topic describes how to manage the system files and disks of the U2000 in the Single-Server System (Windows).

[6.3 Single-Server System \(Solaris\)](#)

This topic describes how to manage the system files and disks of the U2000 in the Single-Server System (Solaris).

[6.4 Single-Server System \(SUSE Linux-Distributed\)](#)

This topic describes how to manage the system files and disks of the U2000 in the Single-Server System (SUSE Linux-Distributed).

[6.5 High Availability System \(Windows\)](#)

This topic describes how to manage the system files and disks of the U2000 in the High Availability System (Windows).

[6.6 High Availability System \(Solaris\)](#)

This topic describes how to manage the system files and disks of the U2000 in the High Availability System (Solaris).

[6.7 High Availability System \(SUSE Linux-Distributed\)](#)

This topic describes how to manage the system files and disks of the U2000 in the High Availability System (SUSE Linux-Distributed).

6.1 U2000 File System Overview

This topic describes the system architecture of the U2000, which is based on the client/server model, and the file system of the U2000.

6.1.1 System Architecture Overview

This topic describes the system architecture of the U2000.

6.1.2 File System of the Server

This topic describes the file system structure that is displayed after the software of the master and slave servers of the U2000 is installed.

6.1.3 File System of the Client

This topic describes the file system structure that is displayed after the U2000 client is installed.

6.1.1 System Architecture Overview

This topic describes the system architecture of the U2000.

The system architecture of the U2000 is based on the client/server model. The details are as follows:

- The client provides the graphical user interface (GUI) for you to maintain and perform operations on network elements (NEs), in addition to monitoring the status of the U2000.
- The server communicates with NEs and stores the data of operations and maintenance on NEs.
- The client and server of the U2000 communicate with each other through the data communication network (DCN).

6.1.2 File System of the Server

This topic describes the file system structure that is displayed after the software of the master and slave servers of the U2000 is installed.

The U2000 server software can run in the Windows, Solaris and SUSE Linux operating system (OS) and integrates the database software. The file systems of the master and slave servers of the U2000 are the same. The following table shows the directory structure.

Table 6-1 Major directory architecture for the U2000 server software in the Windows OS

Default Directory Name in Window	Description
D:\U2000	Saves the files related to the U2000 software.
D:\U2000\client	Saves the files related to the client software.
D:\U2000\webblct	Serves as the directory used by the Web LCT.
D:\U2000\common	Saves the third-party software that can run independently.
D:\U2000\notify	Saves the files related to the remote notification service.
D:\U2000\server	Saves the files and subdirectories related to the U2000 server.

Default Directory Name in Window	Description
D:\U2000\uninstall	Serves as the directory used by the CAU.
D:\U2000\server\bin	Saves the executable files of the U2000 server program.
D:\U2000\server\conf	Saves the U2000 configuration file.
D:\U2000\server\var\backup	Saves the U2000 database backup file.
D:\U2000\server\var\dbdata	Saves the temporary database data.
D:\U2000\server\dump	Saves dumped logs.
D:\U2000\server\etc\conf \license	Saves the U2000 license file.
D:\U2000\server\log	Saves log files created from the U2000 server commissioning information.
D:\U2000\server\var	Saves the output data in the running of the U2000.
D:\U2000\server\etc	Saves the static data.
D:\U2000\server\var\share	Saves the sharing data.
D:\U2000\server\tools	Saves the files related to the tools.

Table 6-2 Directory structure of the U2000 server software in the Solaris or SUSE Linux OS

Default Directory Name	Description
/opt/U2000	Serves as the NMS installation directory.
/opt/U2000/client	Saves the files related to the client software.
/opt/U2000/weblct	Serves as the directory used by the Web LCT.
/opt/U2000/common	Saves the third-party software that can run independently.
/opt/U2000/notify	Saves the files related to the remote notification service.
/opt/U2000/server	Saves the files and subdirectories related to the U2000 server.
/opt/U2000/uninstall	Serves as the directory used by the CAU.
/opt/U2000/server/bin	Saves the executable files of the U2000 server program.
/opt/U2000/server/conf	Saves the U2000 configuration file.
/opt/U2000/server/var/ backup	Saves the U2000 database backup file.
/opt/U2000/server/var/ dbdata	Saves the temporary database data.
/opt/U2000/server/dump	Saves dumped logs.

Default Directory Name	Description
/opt/U2000/server/etc/conf/license	Saves the U2000 license file.
/opt/U2000/server/log	Saves log files created from the U2000 server commissioning information.
/opt/U2000/server/var	Saves the output data in the running of the U2000.
/opt/U2000/server/etc	Saves the static data.
/opt/U2000/server/var/share	Saves the sharing data.
/opt/U2000/server/tools	Saves the files related to the tools.

6.1.3 File System of the Client

This topic describes the file system structure that is displayed after the U2000 client is installed.

The U2000 client software can run in the Solaris or Windows OS. The following table shows the directory structure of the client file system.

Table 6-3 Directory structure of the U2000 client software in the Windows OS

Default Directory Name in Windows	Description
D:\U2000\client	Saves the files related to the client software.
D:\U2000\weblct	Serves as the directory used by the Web LCT.
D:\U2000\common	Saves the third-party software that can run independently.
D:\U2000\notify	Saves the files related to the remote notification service.
D:\U2000\client\bin	Saves the executable files of the U2000 client application.
D:\U2000\client\log	Saves the log files containing the uploading information and abnormal information of the client.
D:\U2000\client\lib	Saves the SDK information.
D:\U2000\client\patch	Saves the patches and patch version information of the U2000 client.
D:\U2000\client\report	Serves as the directory for exporting reports.
D:\U2000\client\thirdparty	Saves the third-party software.

Table 6-4 Directory structure of the U2000 client software in the Solaris OS

Default Directory Name in Solaris	Description
/opt/U2000/client	Saves the files related to the client software.
/opt/U2000/common	Saves the third-party software that can run independently.
/opt/U2000/client/bin	Saves the executable files of the U2000 client application.
/opt/U2000/client/log	Saves the log files containing the uploading information and abnormal information of the client.
/opt/U2000/client/lib	Saves the SDK information.
/opt/U2000/client/patch	Saves the patches and patch version information of the U2000 client.
/opt/U2000/client/report	Serves as the directory for exporting reports.
/opt/U2000/client/thirdparty	Saves the third-party software.

6.2 Single-Server System (Windows)

This topic describes how to manage the system files and disks of the U2000 in the Single-Server System (Windows).

6.2.1 Checking the Usage of the Server Disk

This topic describes how to check the usage of the server disk. Disk anomalies can lead to data loss, affecting the normal running of the NMS. It is recommended that you check the disk status regularly. In this manner, you can repair or replace the disk in time when discovering any disk fault.

6.2.2 Cleaning Up the U2000 Server Disk Space

To ensure sufficient disk space for the server, you need to delete the outdated and useless backup files and trash files to clean up the disk space. Otherwise, the insufficiency of disk space may cause a running error of the U2000 server.

6.2.3 Cleaning Up the U2000 Client Disk Space

To ensure the sufficient disk space for running the client, you need to clean up the disk space by deleting useless backup files and trash files. Otherwise, the insufficiency of disk space may cause a running error of the U2000 client.

6.2.1 Checking the Usage of the Server Disk

This topic describes how to check the usage of the server disk. Disk anomalies can lead to data loss, affecting the normal running of the NMS. It is recommended that you check the disk status regularly. In this manner, you can repair or replace the disk in time when discovering any disk fault.

Procedure

- 1 In the **My Computer** window, right-click a disk and choose **Properties** from the shortcut menu.
- 2 In the dialog box that is displayed, click the **Tools** tab.
- 3 In the **Error-checking** area, click **Check Now**.
- 4 In the **Check Disk operation** dialog box, select the required check disk option and click **Start**.

----End

Reference Standard

Hardware errors prompts do not exist in the displayed information.

Exception Handling

If a disk is faulty, contact the device supplier to repair or replace the disk.

6.2.2 Cleaning Up the U2000 Server Disk Space

To ensure sufficient disk space for the server, you need to delete the outdated and useless backup files and trash files to clean up the disk space. Otherwise, the insufficiency of disk space may cause a running error of the U2000 server.

Context

Do not delete useful files, especially operating system files. Otherwise, the U2000 server may not run stably.

Procedure

- 1 Log in to Windows as the administrator user.
- 2 Delete the outdated and useless files:
 - Delete the outdated and useless alarm dump files. The default path is **installation path of the NMS\server\dump**.
 - Delete the outdated and useless log dump files. The default path is **installation path of the NMS\server\dump**.
 - Delete the outdated and useless database backup files. The default path is **installation path of the NMS\server\var\backup**.
 - Delete the outdated and useless U2000 running logs. The default path is **installation path of the NMS\serve\log**.
 - Delete other outdated and useless files, such as installation files and patch files of earlier versions.

----End

6.2.3 Cleaning Up the U2000 Client Disk Space

To ensure the sufficient disk space for running the client, you need to clean up the disk space by deleting useless backup files and trash files. Otherwise, the insufficiency of disk space may cause a running error of the U2000 client.

Context

Before you delete a file, ensure that the file is no more needed. Otherwise, the U2000 client may not run stably.

Procedure

- 1 Empty the **Recycle Bin**.
- 2 Delete the files in **D:\U2000\client\log**.
- 3 Delete other useless files.

----End

6.3 Single-Server System (Solaris)

This topic describes how to manage the system files and disks of the U2000 in the Single-Server System (Solaris).

6.3.1 Checking the Usage of the Server Disk

This topic describes how to check the usage of the server disk. Disk anomalies can lead to data loss, affecting the normal running of the NMS. It is recommended that you check the disk status regularly. In this manner, you can repair or replace the disk in time when discovering any disk fault.

6.3.2 Cleaning Up the U2000 Server Disk Space

To ensure sufficient disk space for the server, you need to delete the outdated and useless backup files and trash files to clean up the disk space. Otherwise, the insufficiency of disk space may cause a running error of the U2000 server.

6.3.3 Cleaning Up the U2000 Client Disk Space

To ensure the sufficient disk space for running the client, you need to clean up the disk space by deleting useless backup files and trash files. Otherwise, the insufficiency of disk space may cause a running error of the U2000 client.

6.3.1 Checking the Usage of the Server Disk

This topic describes how to check the usage of the server disk. Disk anomalies can lead to data loss, affecting the normal running of the NMS. It is recommended that you check the disk status regularly. In this manner, you can repair or replace the disk in time when discovering any disk fault.

Procedure

- Check the disk status.
 1. Log in to the Solaris OS as the nmsuser user.

2. Open a terminal window. Then, run the following commands to switch to the **root** user:

```
% su - root
Password:password of the root user
```

3. Run the following command to view the physical status of the current server disk:

```
# iostat -E
```

The terminal displays:

```
sdl      Soft Errors: 0 Hard Errors: 0 Transport Errors: 0 Vendor: SEAGATE
Product: ST373307LSUN72G  Revision: 0507 Serial No: 3HZ9JBYN000 07518
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 displayed information varies according to the actual condition of the intended workstation, and thus may be different from the preceding information.

----End

Reference Standard

Hardware errors prompts do not exist in the displayed information.

Exception Handling

If a disk is faulty, contact the device supplier to repair or replace the disk.

6.3.2 Cleaning Up the U2000 Server Disk Space

To ensure sufficient disk space for the server, you need to delete the outdated and useless backup files and trash files to clean up the disk space. Otherwise, the insufficiency of disk space may cause a running error of the U2000 server.

Context

Do not delete useful files, especially operating system files. Otherwise, the U2000 server may not run stably.

Procedure

- 1 Log in to Solaris as the **root** user.
- 2 Delete the outdated and useless files:
 - Delete the outdated and useless alarm dump files. The default path is **/opt/U2000/server/dump**.
 - Delete the outdated and useless log dump files. The default path is **/opt/U2000/server/dump**.
 - Delete the outdated and useless database backup files. The default path is **/opt/U2000/server/var/backup**.
 - Delete the outdated and useless U2000 running logs. The default path is **/opt/U2000/server/log**.

- Delete other outdated and useless files, such as installation files and patch files of earlier versions.

----End

6.3.3 Cleaning Up the U2000 Client Disk Space

To ensure the sufficient disk space for running the client, you need to clean up the disk space by deleting useless backup files and trash files. Otherwise, the insufficiency of disk space may cause a running error of the U2000 client.

Context

Before you delete a file, ensure that the file is no more needed. Otherwise, the U2000 client may not run stably.

Procedure

- 1 Empty the **Trash**.
- 2 Delete the files in **/opt/U2000/client/log**.
- 3 Delete other useless files.

----End

6.4 Single-Server System (SUSE Linux-Distributed)

This topic describes how to manage the system files and disks of the U2000 in the Single-Server System (SUSE Linux-Distributed).

6.4.1 Checking the Usage of Server Disks

This topic describes how to check the usage of server disks. Disk anomalies can lead to data loss, affecting the normal running of the NMS. It is recommended that you regularly check the disk status. In this manner, you can repair or replace the disk in time when discovering any disk fault.

6.4.2 Cleaning Up the U2000 Server Disk Space

To ensure sufficient disk space for the server, you need to delete the outdated and useless backup files and trash files to clean up the disk space. Otherwise, the insufficiency of disk space may cause a running error of the U2000 server.

6.4.3 Cleaning Up the U2000 Client Disk Space

To ensure the sufficient disk space for running the client, you need to clean up the disk space by deleting useless backup files and trash files. Otherwise, the insufficiency of disk space may cause a running error of the U2000 client.

6.4.1 Checking the Usage of Server Disks

This topic describes how to check the usage of server disks. Disk anomalies can lead to data loss, affecting the normal running of the NMS. It is recommended that you regularly check the disk status. In this manner, you can repair or replace the disk in time when discovering any disk fault.

Procedure

- 1 Log in to the SUSE Linux OS as the **nmsuser** user.
- 2 Open a terminal window. Then, run the following commands to switch to the **root** user:

```
% su - root
Password:password of the root user
```

- 3 Run the following command to view the physical status of the current server disk:

```
# df -h
```

The terminal displays:

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/sda1	31G	9.6G	21G	32%	/
udev	7.9G	192K	7.9G	1%	/dev
/dev/sda6	55G	19G	37G	35%	/opt
/dev/sda3	16G	2.9G	13G	20%	/usr
/dev/sda5	21G	1.8G	19G	9%	/var
tmpfs	4.0K	0	4.0K	0%	/dev/vx
/dev/vx/dsk/datadg/lvapp	49G	12G	35G	25%	/opt/U2000
/dev/vx/dsk/datadg/lvoracle	29G	4.5G	23G	17%	/opt/oracle

NOTE

The displayed information varies according to the actual condition of the intended workstation, and thus may be different from the preceding information.

----End

Reference Standard

Hardware errors prompts do not exist in the displayed information.

Exception Handling

If a disk is faulty, contact the device supplier to repair or replace the disk.

6.4.2 Cleaning Up the U2000 Server Disk Space

To ensure sufficient disk space for the server, you need to delete the outdated and useless backup files and trash files to clean up the disk space. Otherwise, the insufficiency of disk space may cause a running error of the U2000 server.

Context

Do not delete useful files, especially operating system files. Otherwise, the U2000 server may not run stably.

Procedure

- 1 Log in to SuSE Linux as the **root** user.
- 2 Delete the outdated and useless files:
 - Delete the outdated and useless alarm dump files. The default path is **/opt/U2000/server/dump**.

- Delete the outdated and useless log dump files. The default path is **/opt/U2000/server/dump**.
- Delete the outdated and useless database backup files. The default path is **/opt/U2000/server/var/backup**.
- Delete the outdated and useless U2000 running logs. The default path is **/opt/U2000/server/log**.
- Delete other outdated and useless files, such as installation files and patch files of earlier versions.

----End

6.4.3 Cleaning Up the U2000 Client Disk Space

To ensure the sufficient disk space for running the client, you need to clean up the disk space by deleting useless backup files and trash files. Otherwise, the insufficiency of disk space may cause a running error of the U2000 client.

Context

Before you delete a file, ensure that the file is no more needed. Otherwise, the U2000 client may not run stably.

Procedure

- 1 Empty the **Trash**.
- 2 Delete the files in **/opt/U2000/client/log**.
- 3 Delete other useless files.

----End

6.5 High Availability System (Windows)

This topic describes how to manage the system files and disks of the U2000 in the High Availability System (Windows).

6.5.1 Checking Server Disks

This topic describes how to check the usage and status of the U2000 server disks.

6.5.2 Clearing Disk Space

This topic describes how to clear disk space. Clearing disk space in time facilitates the normal running of the U2000 client and server.

6.5.1 Checking Server Disks

This topic describes how to check the usage and status of the U2000 server disks.

6.5.1.1 Checking the Disk Usage of the U2000 Server

This topic describes how to check the disk usage of the U2000 server through the System Monitor or Veritas Enterprise Administrator. With this operation, you can learn the information such as the remaining space and used proportion of a disk.

6.5.1.2 Checking the Status of Server Disks

This topic describes how to check the status of server disks. If the disk status is abnormal, the data may be lost and the U2000 cannot be normally used. Therefore, you need to check the disk status periodically. When a disk fault is located, clear it or replace the disk in time.

6.5.1.3 Checking the Disk Group Status of the U2000 Server

This topic describes how to check the disk group status of the U2000 server.

6.5.1.4 Checking the Disk Volume Status of the U2000 Server

This topic describes how to check the disk volume status of the U2000 server.

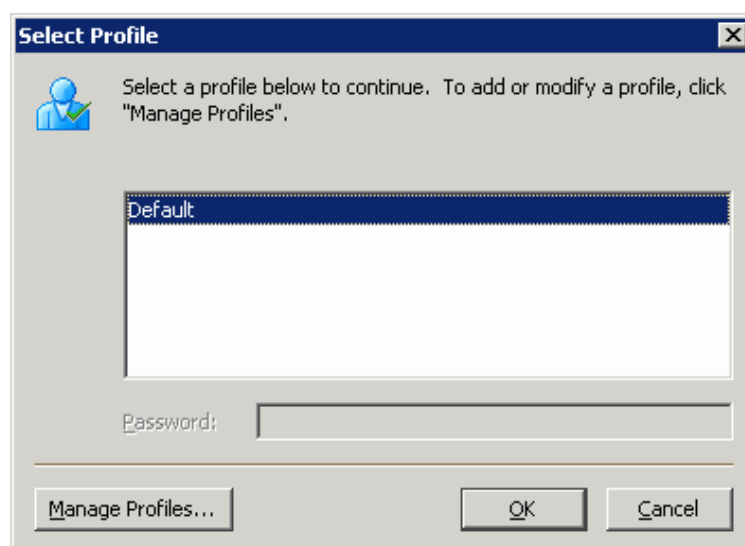
6.5.1.1 Checking the Disk Usage of the U2000 Server

This topic describes how to check the disk usage of the U2000 server through the System Monitor or Veritas Enterprise Administrator. With this operation, you can learn the information such as the remaining space and used proportion of a disk.

Procedure

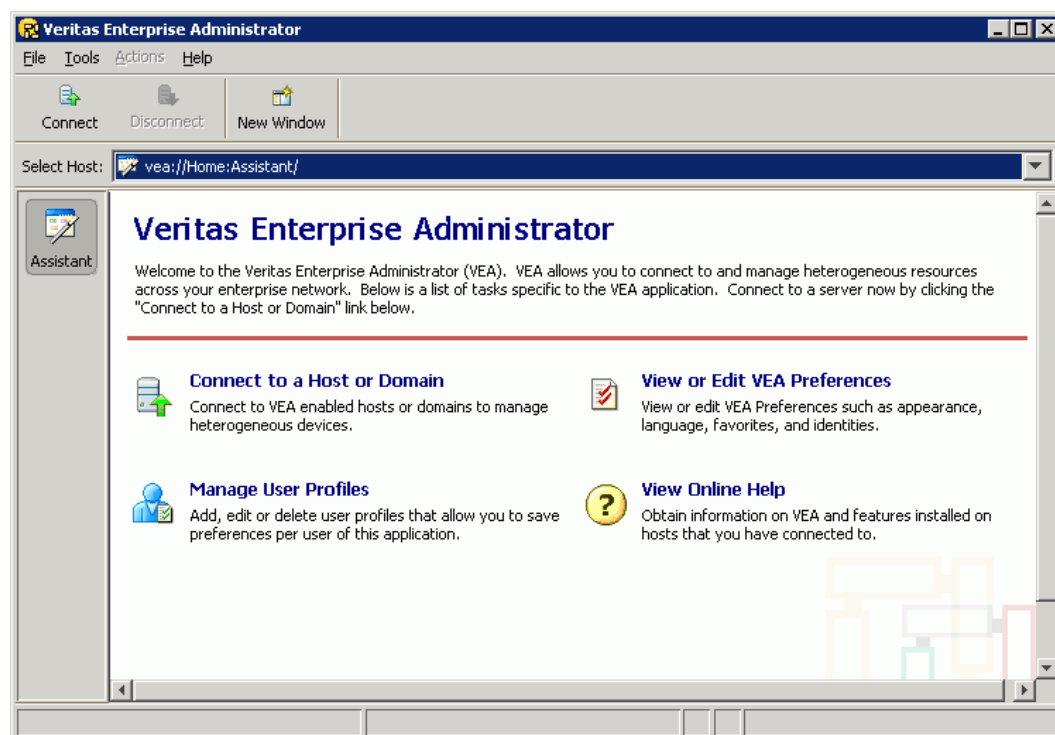
- To check the disk usage through the System Monitor, do as follows:
 1. Log in to the U2000 System Monitor.
 2. Click the **Disk** tab to check the information such as the remaining space and used proportion of a disk.
- Access the Veritas Enterprise Administrator (VEA) window to view the associated information.
 1. Log in to the OS as the administrator.
 2. Choose **Start > All Programs > Symantec > Veritas Storage Foundation > Veritas Enterprise Administrator**.

Figure 6-1 Selecting profile



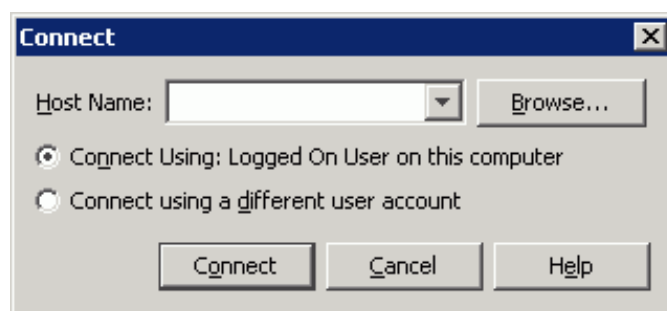
3. In the **Select Profile** window, select **default**, and then click **OK**.

Figure 6-2 VEA login window



4. Click **Connect**.

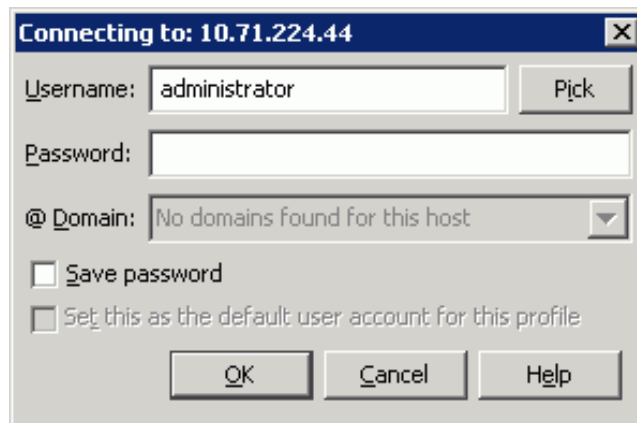
Figure 6-3 Connection



5. In the **Connect** window, enter an IP address in the **Host Name** field, and then click **Connect**.

 NOTE

If the IP address of the primary site is entered, the information about the primary site is displayed. If the IP address of the secondary site is entered, the information about the secondary site is displayed.

Figure 6-4 Accessing the login window

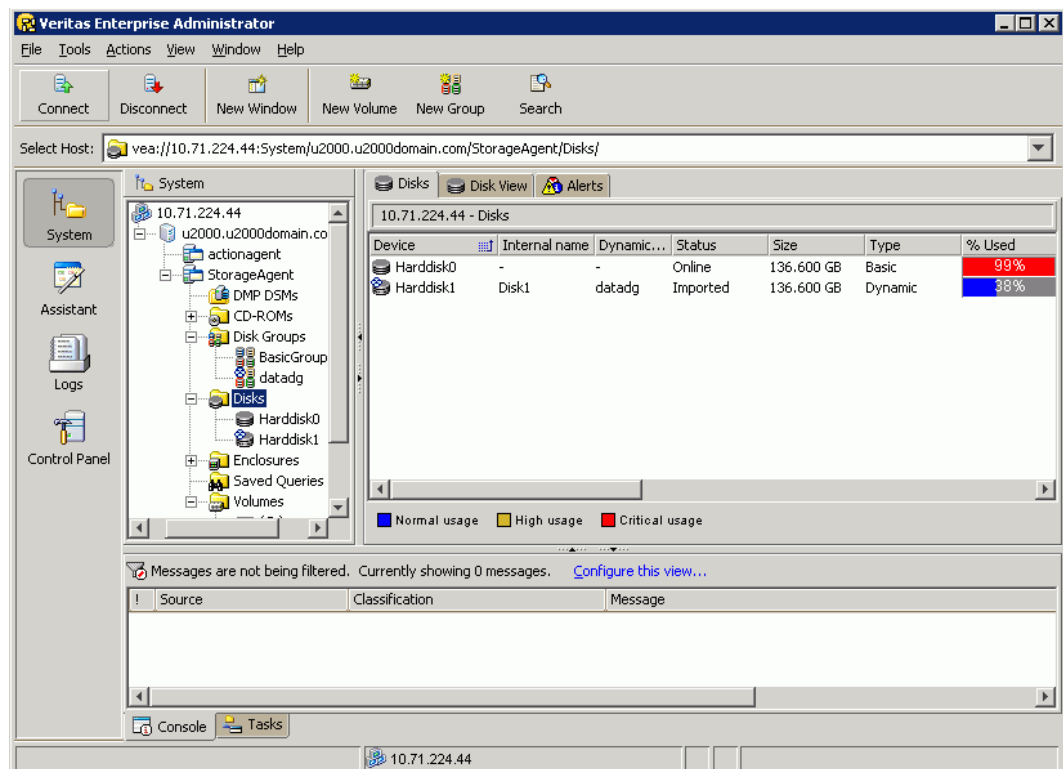
6. In the **Connecting to xxxx** dialog box, enter the user name and password, and then click **OK**.

 NOTE

- Here, **xxxx** indicates the IP address selected in the previous step.
- The user name to be entered is in the format of administrator.

7. In the **Connection Successful** dialog box, click **OK**.
8. In the navigation tree of the VEA window, choose **StorageAgent > Disk**. The information about the usage of the current server disks is displayed in the right pane.

You need to focus on the information in the **Size** and **Used** columns.

Figure 6-5 Viewing the usage of server disks

----End

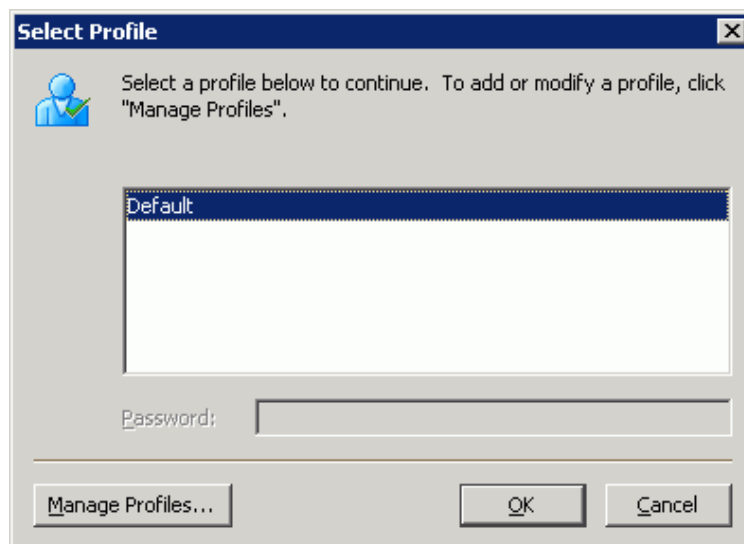
6.5.1.2 Checking the Status of Server Disks

This topic describes how to check the status of server disks. If the disk status is abnormal, the data may be lost and the U2000 cannot be normally used. Therefore, you need to check the disk status periodically. When a disk fault is located, clear it or replace the disk in time.

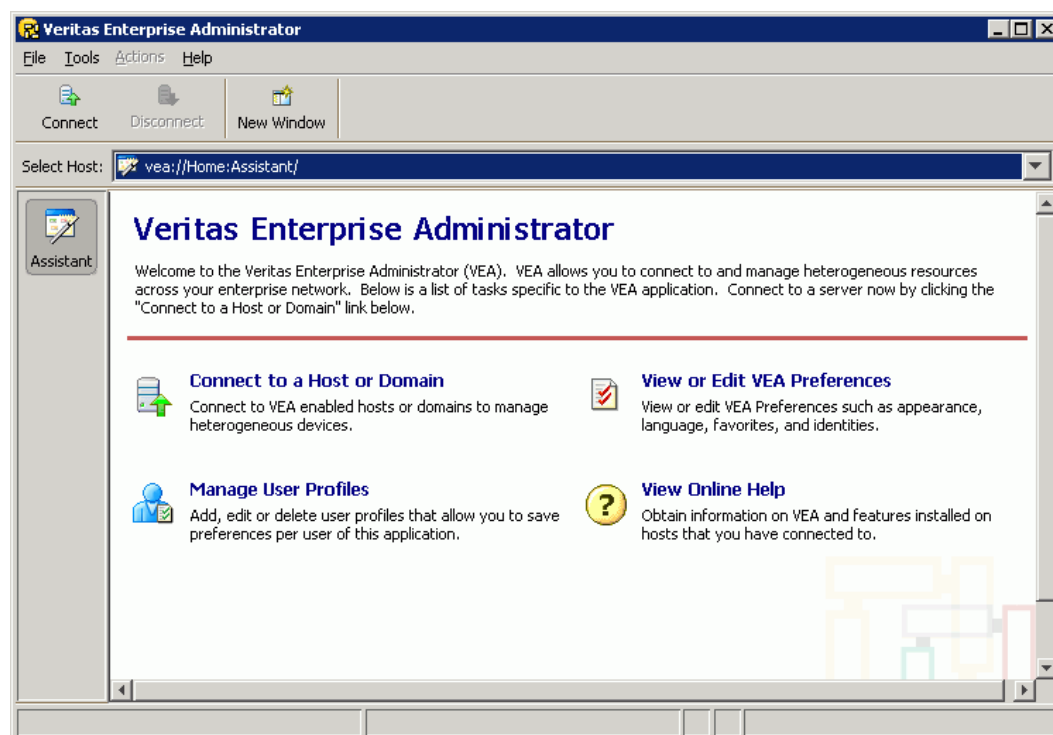
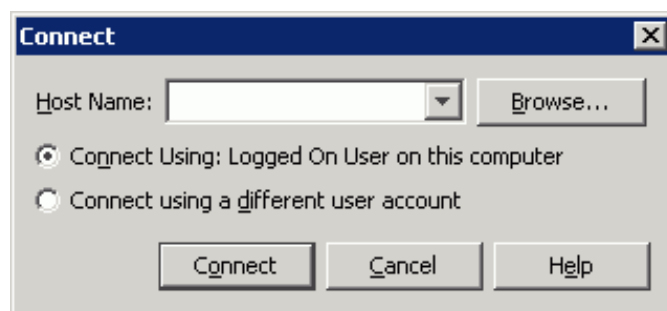
Procedure

- 1 Log in to the OS as the administrator.
- 2 Choose **Start > All Programs > Symantec > Veritas Storage Foundation > Veritas Enterprise Administrator**.

Figure 6-6 Selecting profile

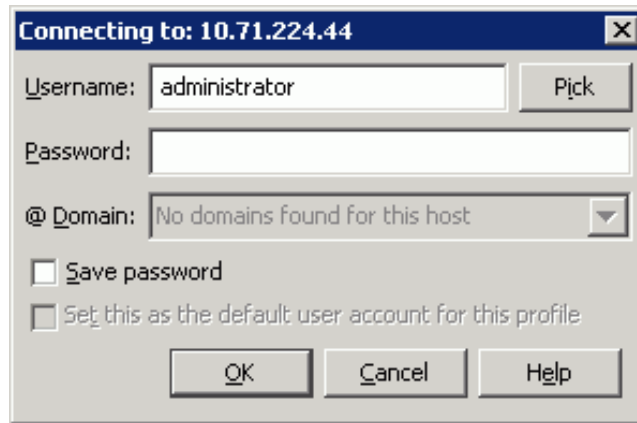


- 3 In the **Select Profile** window, select **default**, and then click **OK**.

Figure 6-7 VEA login window**4 Click Connect.****Figure 6-8** Connection**5 In the Connect window, enter an IP address in the Host Name field, and then click Connect.****NOTE**

If the IP address of the primary site is entered, the information about the primary site is displayed. If the IP address of the secondary site is entered, the information about the secondary site is displayed.

Figure 6-9 Accessing the login window



- 6 In the **Connecting to xxxx** dialog box, enter the user name and password, and then click **OK**.

 NOTE

- Here, **xxxx** indicates the IP address selected in the previous step.
- The user name to be entered is in the format of administrator.

- 7 In the **Connection Successful** dialog box, click **OK**.
- 8 In the navigation tree of the VEA window, choose **StorageAgent > Disk**. The information about the usage of the current server disks is displayed in the right pane.

You need to focus on the information in the **Status** column.

----End

Result

The disk status is considered as normal in the following situation: **Online** or **Imported** is displayed in the **Status** column.

Follow-up Procedure

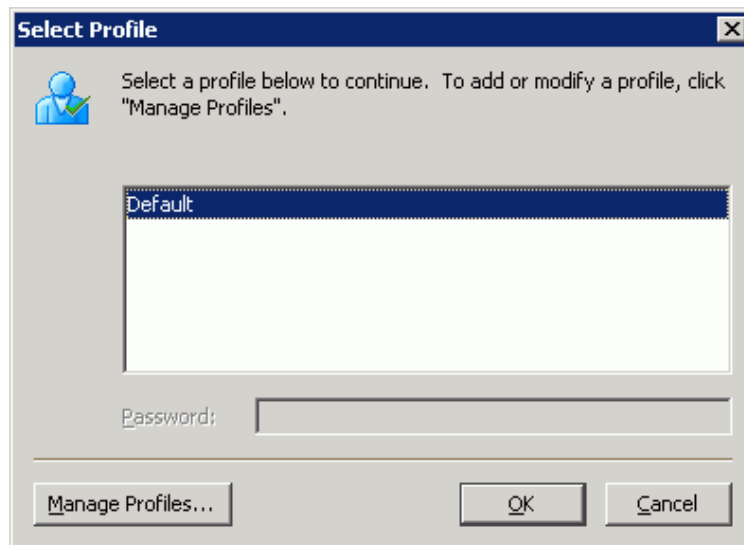
If a disk fault occurs, contact the equipment supplier to repair or replace the disk in a timely manner.

6.5.1.3 Checking the Disk Group Status of the U2000 Server

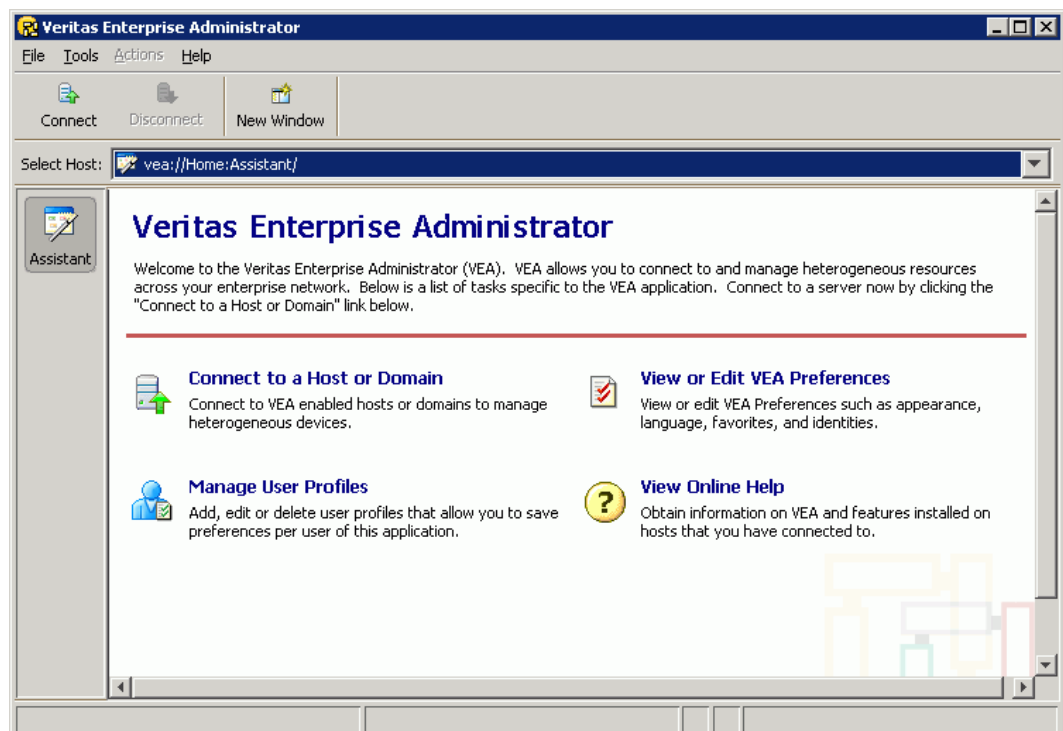
This topic describes how to check the disk group status of the U2000 server.

Procedure

- 1 Log in to the OS as the administrator.
- 2 Choose **Start > All Programs > Symantec > Veritas Storage Foundation > Veritas Enterprise Administrator**.

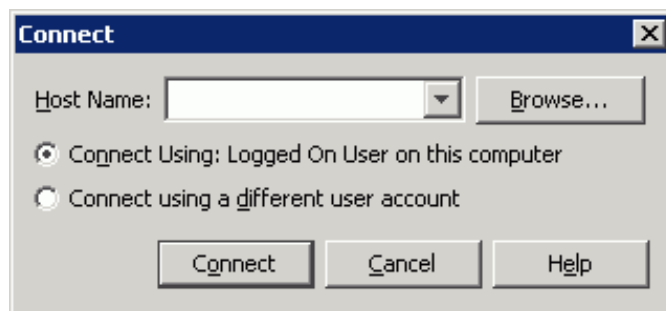
Figure 6-10 Selecting profile

- 3 In the **Select Profile** window, select **default**, and then click **OK**.

Figure 6-11 VEA login window

- 4 Click **Connect**.

Figure 6-12 Connection

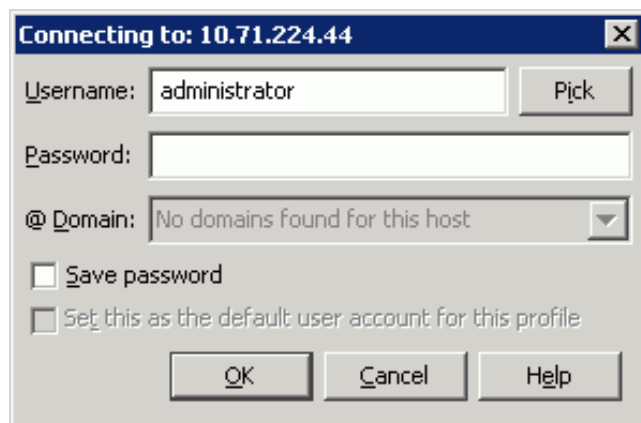


- 5 In the **Connect** window, enter an IP address in the **Host Name** field, and then click **Connect**.

 NOTE

If the IP address of the primary site is entered, the information about the primary site is displayed. If the IP address of the secondary site is entered, the information about the secondary site is displayed.

Figure 6-13 Accessing the login window



- 6 In the **Connecting to xxxx** dialog box, enter the user name and password, and then click **OK**.

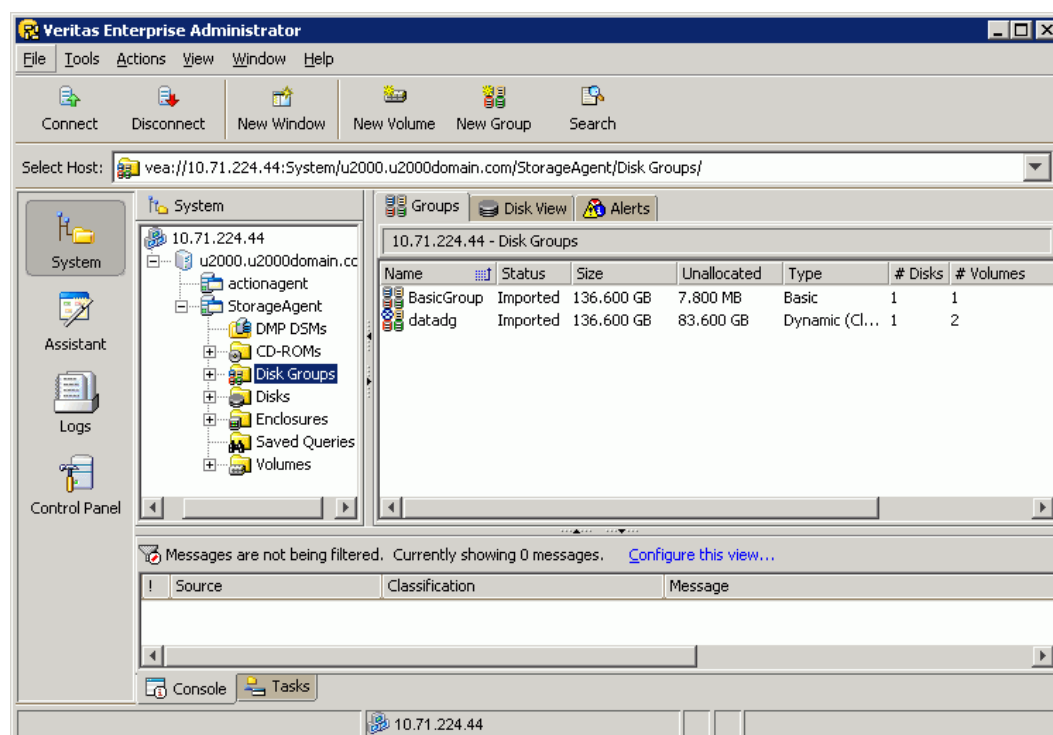
 NOTE

- Here, **xxxx** indicates the IP address selected in the previous step.
- The user name to be entered is in the format of administrator.

- 7 In the **Connection Successful** dialog box, click **OK**.

- 8 In the navigation tree of the VEA window, choose **StorageAgent > Disk Groups**. The information about the usage of the current server disk groups is displayed in the right pane.

You need to focus on the information in the **Status** column.

Figure 6-14 Viewing the disk group status

----End

Result

The disk group status is considered as normal in the following situations:

- **BasicGroup** and **datadg** are displayed in the **Name** column.
- **Imported** is displayed in the **Status** column.

Follow-up Procedure

If a disk group fault occurs, contact the local office or Customer Service Center of Huawei according to the warranty.

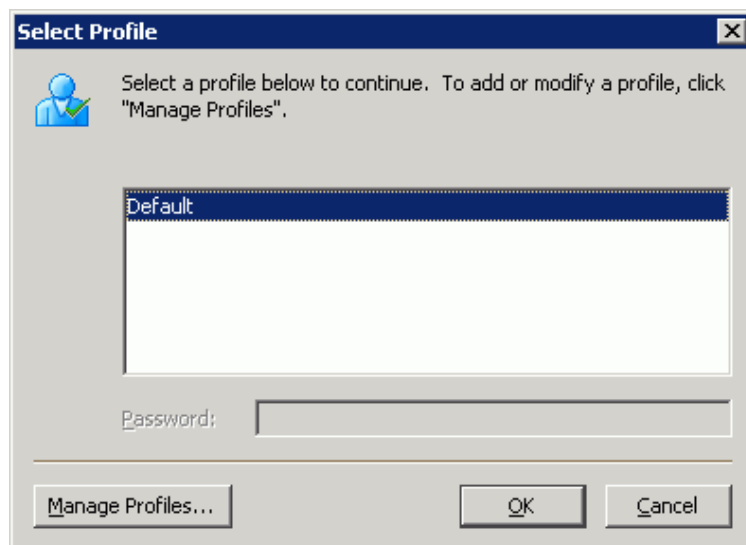
6.5.1.4 Checking the Disk Volume Status of the U2000 Server

This topic describes how to check the disk volume status of the U2000 server.

Procedure

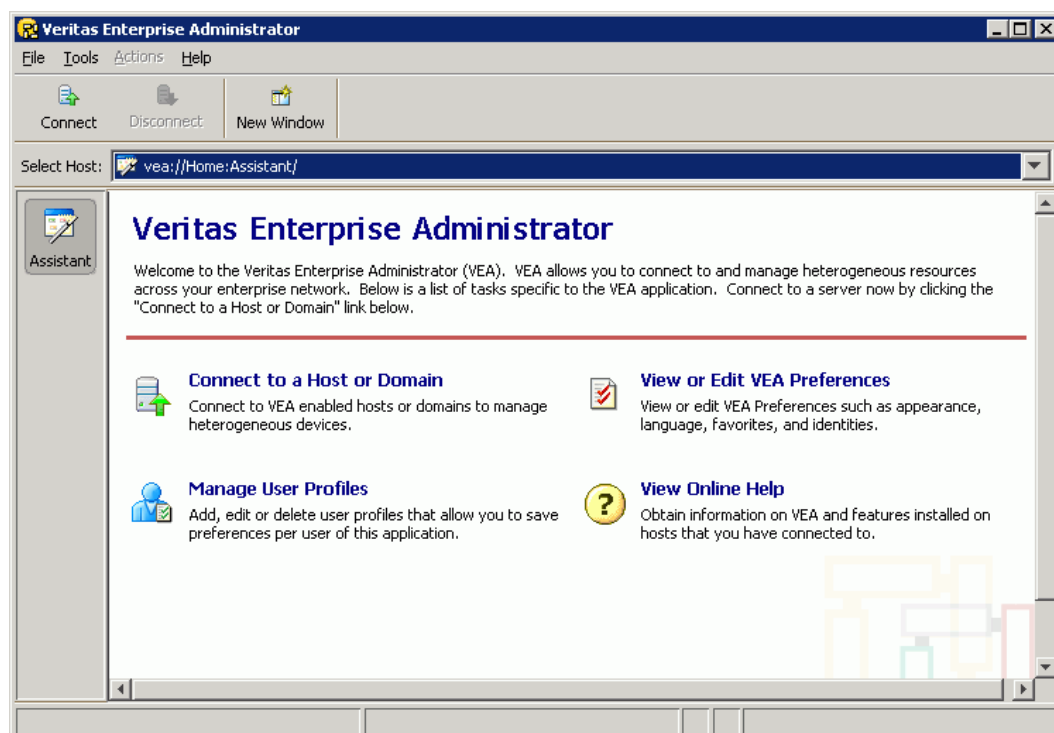
- 1 Log in to the OS as the administrator.
- 2 Choose **Start > All Programs > Symantec > Veritas Storage Foundation > Veritas Enterprise Administrator**.

Figure 6-15 Selecting profile

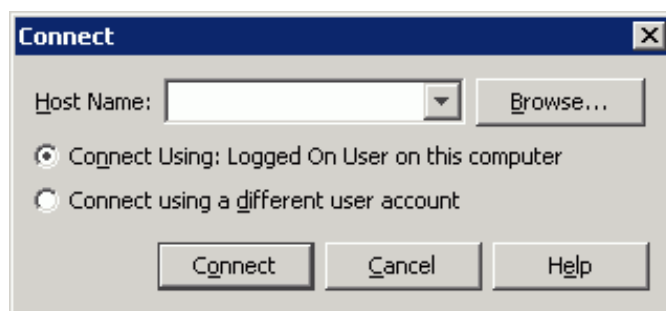


- 3 In the **Select Profile** window, select **default**, and then click **OK**.

Figure 6-16 VEA login window



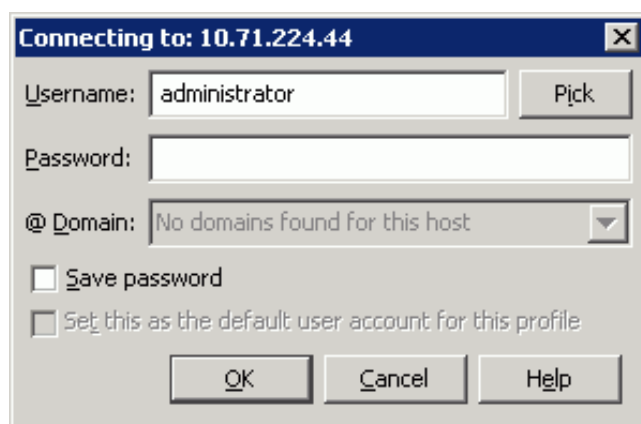
- 4 Click **Connect**.

Figure 6-17 Connection

- 5 In the **Connect** window, enter an IP address in the **Host Name** field, and then click **Connect**.

**NOTE**

If the IP address of the primary site is entered, the information about the primary site is displayed. If the IP address of the secondary site is entered, the information about the secondary site is displayed.

Figure 6-18 Accessing the login window

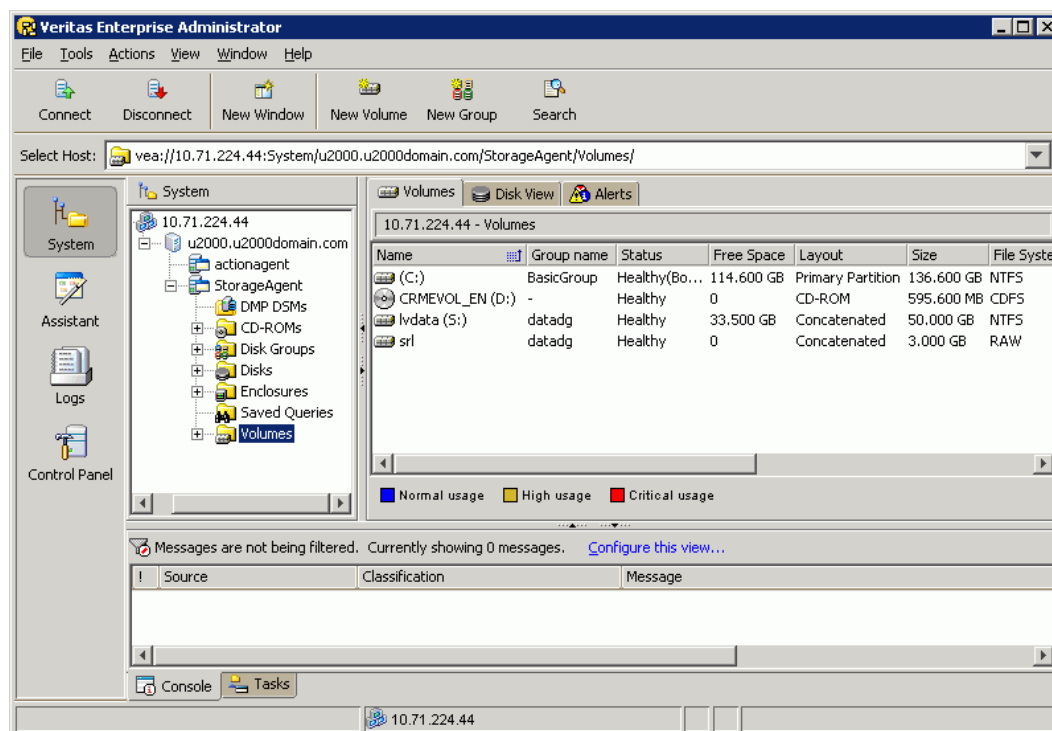
- 6 In the **Connecting to xxxx** dialog box, enter the user name and password, and then click **OK**.

**NOTE**

- Here, **xxxx** indicates the IP address selected in the previous step.
- The user name to be entered is in the format of administrator.

- 7 In the **Connection Successful** dialog box, click **OK**.
- 8 In the navigation tree of the VEA window, choose **StorageAgent > Volumes**. The status of the current server disk groups is displayed in the right pane.

You need to focus on the information in the **Status** column.

Figure 6-19 Viewing the disk volume status

----End

Result

The disk volume status is considered as normal in the following situation:

- The disk volumes used by the U2000 exist. Currently, the disk volumes used in the U2000 include:
 - (C:)
 - (D:)
 - Lvdata(S:)
 - srl
- For all disk volumes, **Healthy** must be displayed in the **Status** column.

Follow-up Procedure

If a disk volume fault occurs, contact the local office or Customer Service Center of Huawei according to the warranty.

6.5.2 Clearing Disk Space

This topic describes how to clear disk space. Clearing disk space in time facilitates the normal running of the U2000 client and server.

6.5.2.1 Cleaning Up the U2000 Server Disk Space

To ensure sufficient disk space for the server, you need to delete the outdated and useless backup files and trash files to clean up the disk space. Otherwise, the insufficiency of disk space may cause a running error of the U2000 server.

6.5.2.2 Cleaning Up the U2000 Client Disk Space

To ensure the sufficient disk space for running the client, you need to clean up the disk space by deleting useless backup files and trash files. Otherwise, the insufficiency of disk space may cause a running error of the U2000 client.

6.5.2.1 Cleaning Up the U2000 Server Disk Space

To ensure sufficient disk space for the server, you need to delete the outdated and useless backup files and trash files to clean up the disk space. Otherwise, the insufficiency of disk space may cause a running error of the U2000 server.

Context

Do not delete useful files, especially operating system files. Otherwise, the U2000 server may not run stably.

Procedure

- 1 Log in to Windows as the administrator user.
- 2 Delete the outdated and useless files:
 - Delete the outdated and useless alarm dump files. The default path is **installation path of the NMS\server\dump**.
 - Delete the outdated and useless log dump files. The default path is **installation path of the NMS\server\dump**.
 - Delete the outdated and useless database backup files. The default path is **installation path of the NMS\server\var\backup**.
 - Delete the outdated and useless U2000 running logs. The default path is **installation path of the NMS\serve\log**.
 - Delete other outdated and useless files, such as installation files and patch files of earlier versions.

----End

6.5.2.2 Cleaning Up the U2000 Client Disk Space

To ensure the sufficient disk space for running the client, you need to clean up the disk space by deleting useless backup files and trash files. Otherwise, the insufficiency of disk space may cause a running error of the U2000 client.

Context

Before you delete a file, ensure that the file is no more needed. Otherwise, the U2000 client may not run stably.

Procedure

- 1 Empty the **Recycle Bin**.

- 2 Delete the files in **D:\U2000\client\log**.
- 3 Delete other useless files.

----End

6.6 High Availability System (Solaris)

This topic describes how to manage the system files and disks of the U2000 in the High Availability System (Solaris).

6.6.1 Checking Server Disks

This topic describes how to check the usage and status of the U2000 server disks.

6.6.2 Clearing Disk Space

This topic describes how to clear disk space. Clearing disk space in time facilitates the normal running of the U2000 client and server.

6.6.1 Checking Server Disks

This topic describes how to check the usage and status of the U2000 server disks.

6.6.1.1 Checking the Disk Usage of the U2000 Server

This topic describes how to check the disk usage of the U2000 server through the System Monitor or command lines. With this operation, you can learn the information such as the remaining space and used proportion of the disk.

6.6.1.2 Checking the Disk Status of the U2000 Server

If the disk status is abnormal, the data may be lost and the U2000 cannot be normally used. Therefore, you need to check the disk status periodically. If any fault of the disk is found, clear it or replace the disk in time.

6.6.1.3 Checking the Disk Group Status of the U2000 Server

Check whether the disk group status is normal.

6.6.1.4 Checking the Disk Volume Status of the U2000 Server

This section describes how to query the disk volume status.

6.6.1.5 Viewing the Disk Mirroring Status

This topic describes how to check the disk mirroring status after the system data is imported to the application server.

6.6.1.6 Monitoring the Mounting Status of File Systems

This topic describes how to use the VCS client to monitor the mounting status of the U2000 file system and Sybase file system.

6.6.1.1 Checking the Disk Usage of the U2000 Server

This topic describes how to check the disk usage of the U2000 server through the System Monitor or command lines. With this operation, you can learn the information such as the remaining space and used proportion of the disk.

Procedure

- To check the disk usage through the System Monitor, do as follows:

1. Log in to the U2000 System Monitor.
2. Click the **Disk** tab to check the information such as the remaining space and used proportion of the disk.
- To check the disk usage through command lines, do as follows:
 1. Log in to the Solaris OS as the **root** user.
 2. Run the following commands on the primary and secondary sites to check the disk usage:

df -k

The following information is displayed:

Filesystem	kbytes	used	avail	capacity
Mounted on				
/dev/vx/dsk/bootdg/rootvol	9260525	3990038	5177882	44%
/proc	0	0	0	0%
fd	0	0	0	0%
mnttab	0	0	0	0%
swap	10831272	8	10831264	1%
dmpfs	10831264	0	10831264	0%
dmpfs	10831264	0	10831264	0%
swap	10833744	2480	10831264	1%
/dev/vx/dsk/bootdg/ftp	4133838	9	4092491	1%
/dev/vx/dsk/bootdg/opt	30983686	661511	30012339	3%

----End

6.6.1.2 Checking the Disk Status of the U2000 Server

If the disk status is abnormal, the data may be lost and the U2000 cannot be normally used. Therefore, you need to check the disk status periodically. If any fault of the disk is found, clear it or replace the disk in time.

Procedure

- Check the disk status on Veritas.
 1. Log in to the Solaris operating system as user **nmsuser**.
 2. Open a terminal window, and run the following commands to switch to user root:


```
$ su - root
Password: password_of_user_root
```
 3. Run the following commands on the master server of the primary and secondary sites:


```
# vxdisk list
```

In the case of two hard disks, the terminal displays the following information:

DEVICE	TYPE	DISK	GROUP	STATUS
clt0d0s2	auto:sliced	rootdisk	datadg	online
clt1d0s2	auto:sliced	rootmirror	datadg	online

In the case of four hard disks, the terminal displays the following information:

DEVICE	TYPE	DISK	GROUP	STATUS
clt0d0s2	auto:slice	rootdisk	rootdg	online
clt1d0s2	auto:slice	rootmirror	rootdg	online
clt2d0s2	auto:slice	datadisk	datadg	online
clt3d0s2	auto:slice	datamirror	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.

4. Run the following commands to switch to non-root user:

```
# exit
```

- Check the disk status on Solaris.

1. Log in to the Solaris operating system as user **nmsuser**.
2. Open a terminal window, and run the following commands to switch to user root:

```
$ su - root  
Password: password_of_user_root
```

3. Run the following commands to view the physical status of the disk on the current server:

```
# iostat -E
```

The terminal displays:

```
sd1          Soft Errors: 0 Hard Errors: 0 Transport Errors: 0  
Vendor: HITACHI Product: H101414SCSUN146G Revision: SA25 Serial No:  
0848E3PKSA  
Size: 146.80GB <146800115712 bytes>  
Media Error: 0 Device Not Ready: 0 No Device: 0 Recoverable: 0  
Illegal Request: 0 Predictive Failure Analysis: 0  
sd2          Soft Errors: 3 Hard Errors: 4 Transport Errors: 0  
Vendor: TSSTcorp Product: CD/DVDW TS-T632A Revision: SR03 Serial No:  
Size: 0.00GB <0 bytes>  
Media Error: 0 Device Not Ready: 4 No Device: 0 Recoverable: 0  
Illegal Request: 3 Predictive Failure Analysis: 0  
sd3          Soft Errors: 0 Hard Errors: 0 Transport Errors: 0  
Vendor: HITACHI Product: H101414SCSUN146G Revision: SA25 Serial No:  
0848E42GTA  
Size: 146.80GB <146800115712 bytes>  
Media Error: 0 Device Not Ready: 0 No Device: 0 Recoverable: 0  
Illegal Request: 0 Predictive Failure Analysis: 0  
sd4          Soft Errors: 0 Hard Errors: 0 Transport Errors: 0  
Vendor: HITACHI Product: H101414SCSUN146G Revision: SA25 Serial No:  
0848E3PAAA  
Size: 146.80GB <146800115712 bytes>  
Media Error: 0 Device Not Ready: 0 No Device: 0 Recoverable: 0  
Illegal Request: 0 Predictive Failure Analysis: 0  
sd5          Soft Errors: 0 Hard Errors: 0 Transport Errors: 0  
Vendor: HITACHI Product: H101414SCSUN146G Revision: SA25 Serial No:  
0848E46GKA  
Size: 146.80GB <146800115712 bytes>  
Media Error: 0 Device Not Ready: 0 No Device: 0 Recoverable: 0  
Illegal Request: 0 Predictive Failure Analysis: 0  
sd6          Soft Errors: 0 Hard Errors: 0 Transport Errors: 0  
Vendor: HITACHI Product: H101414SCSUN146G Revision: SA25 Serial No:  
0848E46GDA  
Size: 146.80GB <146800115712 bytes>  
Media Error: 0 Device Not Ready: 0 No Device: 0 Recoverable: 0  
Illegal Request: 0 Predictive Failure Analysis: 0  
sd7          Soft Errors: 0 Hard Errors: 0 Transport Errors: 0  
Vendor: HITACHI Product: H101414SCSUN146G Revision: SA25 Serial No:  
0848E46GUA  
Size: 146.80GB <146800115712 bytes>  
Media Error: 0 Device Not Ready: 0 No Device: 0 Recoverable: 0  
Illegal Request: 0 Predictive Failure Analysis: 0
```

 NOTE

The output information may be different from that displayed on the terminal according to the actual situation of the workstation.

4. Run the following commands to switch to non-root user:

```
# exit
```

----End

Reference Standard

If the following standards are met, it indicates that the disk status is normal:

- After you run the **vxdisk list** command, the disk status is **online**.
- After you run the **iostat -E** command, if the **Hard Errors** information of the disk is **0**, it indicates that the physical status of the disk is normal.

Troubleshooting

If a disk fails, contact the equipment supplier to repair or replace the disk in a timely manner.

6.6.1.3 Checking the Disk Group Status of the U2000 Server

Check whether the disk group status is normal.

Procedure

- 1 Open a terminal window, and run the following commands to switch to user root:

```
% su - root  
Password:password_of_user_root
```

- 2 Run the following commands on both the primary and secondary sites:

```
# vxdg list
```

The screen output is similar to the following:

NAME	STATE	ID
datadg	enabled	997585324.1237.Primary

----End

Reference Standards

If the following standards are met, the disk group status is normal:

- If over two disks are available on the workstation, two disk groups should be displayed, including **rootdg** and **datadg**. Otherwise, there is a problem with the disk groups.
- If only two disks are available on the workstation, only one disk group, that is, **datadg**, should be displayed. Otherwise, there is a problem with the disk group.
- The **STATE** of each disk group should be **enabled**. Otherwise, there is a problem with the disk groups.

Troubleshooting

If a fault of the disk group occurs, contact the local office or Customer Service Center of Huawei according to the warranty.

6.6.1.4 Checking the Disk Volume Status of the U2000 Server

This section describes how to query the disk volume status.

Procedure

- 1 Log in to the Solaris OS as the **nmsuser** user.
- 2 Open a terminal window, and run the following commands to switch to the **root** user:
% **su - root**
Password: **password_of_user_root**
- 3 Run the following commands to check whether the disk volume status is normal, according to the disk volume information:

vxprint -v

The terminal displays:

Disk group: rootdg

TY	NAME	ASSOC	KSTATE	LENGTH	PLOFFS	STATE	TUTILO	PUTILO
v	opt	fsgen	ENABLED	167781888	-	ACTIVE	-	-
v	rootvol	root	ENABLED	20982912	-	ACTIVE	-	-
v	swapvol	swap	ENABLED	33560448	-	ACTIVE	-	-
v	usr	fsgen	ENABLED	20982912	-	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 disks that are actually configured.

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

----End

Reference Standards

If the following standards are met, it indicates that the disk volume status is normal:

- Disk volumes used by the U2000 exist. Currently, disk volumes used by the U2000 is lv_nms_data.
- For all the disk volumes, **KSTATE** must be **ENABLED**.
- For all the disk volumes, **STATE** must be **ACTIVE**.

Troubleshooting

1. If the problem persists, run the following command to record the details of all the disk volumes, and contact the local office or Customer Service Center of Huawei according to the warranty.

vxprint -l VolumeName

Table 6-5 describes the meanings of the fields that are displayed:

Table 6-5 Field description for disk volume status

Field Name	Description
Disk group	The disk group to which this disk volume belongs.
Volume	Disk volume name.
info	Disk volume length.
type	Disk volume type.
state	Disk volume state. Normally, it should be ACTIVE, and kernel be ENABLED
assoc	Association of disk volumes, rvg refers to the RVG to which this disk volume belongs, which is datarvg normally.
plexes	The plex contained in this disk volume.
policies	Disk volume management policy.
flags	Disk volume flag.
logging	Disk volume log. Normally, the type is DCM.
recovery	Disk volume recovery mode.
device	Disk volume number and trail.
perms	Disk volume owner and authority.

For example, to query the details of the disk volume **lv_nms_data**, you can run the following command:

```
# vxprint -l lv_nms_data
```

The terminal displays:

```
Disk group: datadg
```

```
Volume:   lv_nms_data
info:     len=83886080
type:     usetype=fsgen
state:    state=ACTIVE kernel=ENABLED cdsrecovery=0/0 (clean)
assoc:    rvg=datarvg
          plexes=lv_nms_data-01,lv_nms_data-02
          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=1001 bdev=295/1001 cdev=295/1001 path=/dev/vx/dsk/datadg/
lv_nms_data
perms:    user=root group=root mode=0666
.....
```

6.6.1.5 Viewing the Disk Mirroring Status

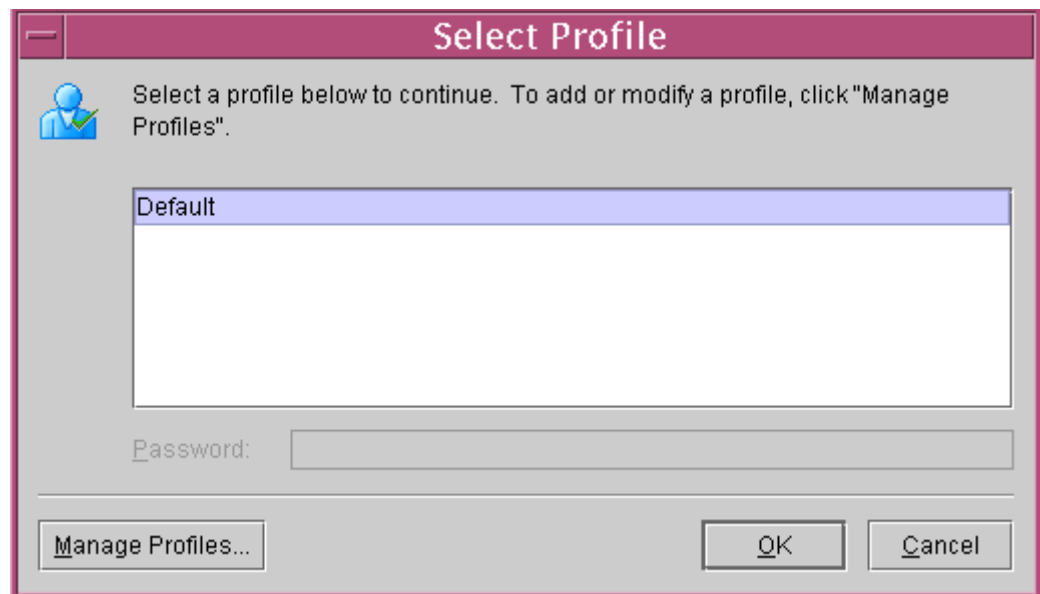
This topic describes how to check the disk mirroring status after the system data is imported to the application server.

Procedure

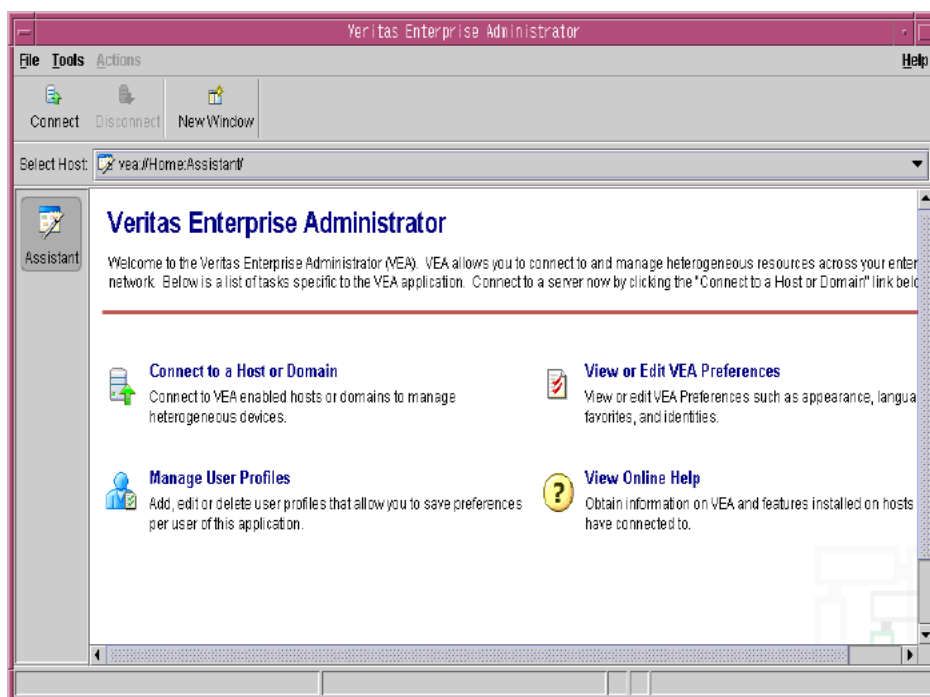
- 1 Log in to the Veritas Enterprise Administrator (VEA) client.
 1. Run the following command to start the VEA client:

`# vea&`
 2. In the dialog box shown in [Figure 6-20](#), click **OK**.

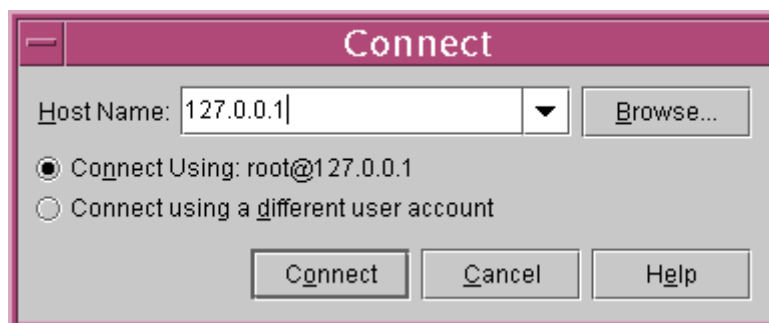
Figure 6-20 Selecting profile



3. In the dialog box shown in [Figure 6-21](#), click **Connect**.

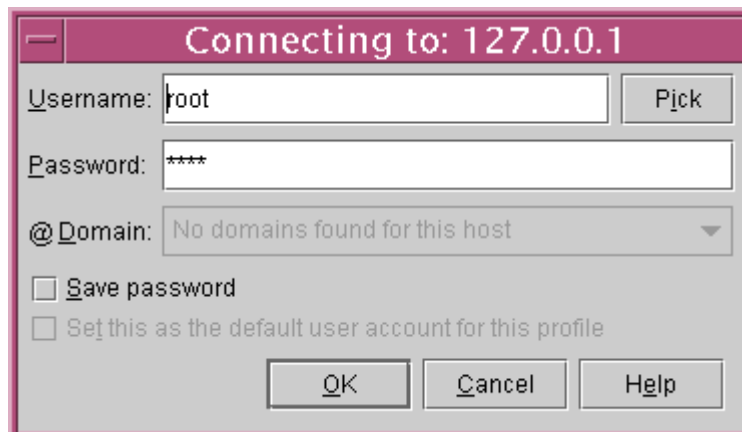
Figure 6-21 Logging in VEA

4. In the dialog box shown in [Figure 6-22](#), enter **127.0.0.1**, and then click **Connect**.

Figure 6-22 Connect the server

5. In the dialog box shown in [Figure 6-23](#), enter the valid user name and password of the server. Then, click **OK**.

Figure 6-23 Entering user name and password

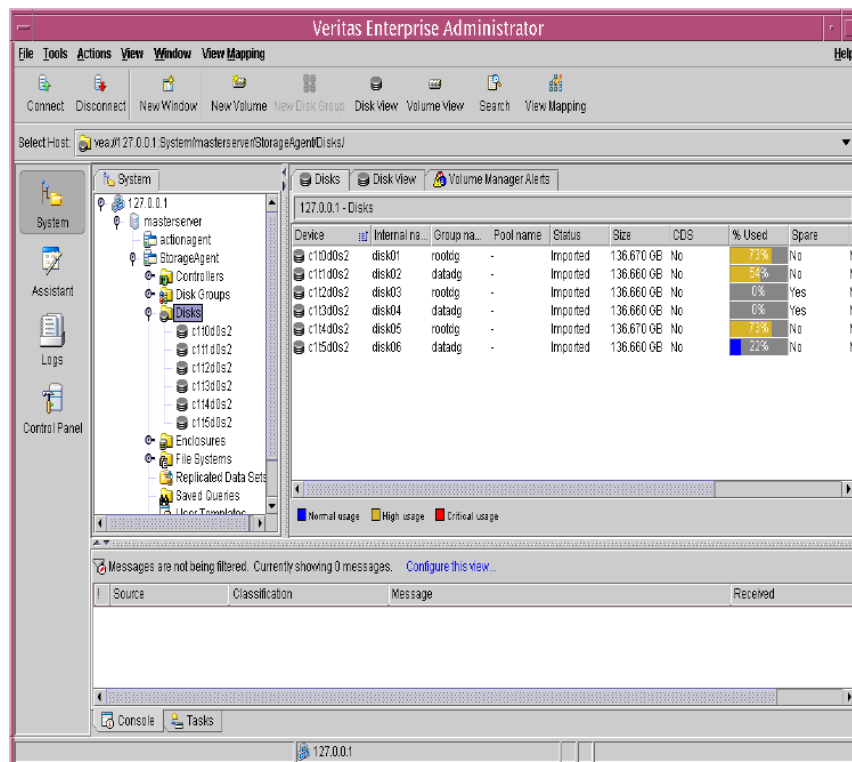


NOTE

The user name and password to be entered here are the user name and password of the **root** user.

- 2 In the window shown in **Figure 6-24**, choose **Disks** under the server node (such as **127.0.0.1**) from the **Management Console** navigation tree.

Figure 6-24 Viewing the disk mirroring result



 NOTE

The disk names and quantity vary according to the model of the server. Thus, you need to check the disk mirroring on the related server.

----End

Result

The first disk is encapsulated into the **rootdg** disk group, whereas the second disk is encapsulated into the **datadg** disk group. The third disk serves as the mirroring disk for the first disk, whereas the fourth for the second. The fifth disk serves as the hot backup disk and the sixth disk serves as the cold backup disk.

6.6.1.6 Monitoring the Mounting Status of File Systems

This topic describes how to use the VCS client to monitor the mounting status of the U2000 file system and Sybase file system.

Procedure

- 1 Log in to the Solaris OS as the **nmsuser** user.
- 2 Open a terminal window, and run the following commands to switch to user root:

```
% su - root Password:password_of_user_root
```
- 3 Run the following command to view the mounting status of the U2000 file system and the Sybase file system.

df -k

The screen output is similar to the following:

Filesystem	kbytes	used	avail	capacity	Mounted on
/dev/vx/dsk/bootdg/rootvol	20174017	13589154	6383123	69%	/
/devices	0	0	0	0%	/devices
ctfs	0	0	0	0%	/system/contract
proc	0	0	0	0%	/proc
mnttab	0	0	0	0%	/etc/mnttab
swap	21862280	1656	21860624	1%	/etc/svc/volatile
objfs	0	0	0	0%	/system/object
/dev/vx/dsk/bootdg/usr	10091716	4375109	5615690	44%	/usr
/platform/SUNW,SPARC-Enterprise-T5220/lib/libc_psr/libc_psr_hwcap2.so.1	20174017	13589154	6383123	69%	/platform/sun4v/lib/
libc_psr.so.1					
/platform/SUNW,SPARC-Enterprise-T5220/lib/sparcv9/libc_psr/libc_psr_hwcap2.so.1	20174017	13589154	6383123	69%	/platform/sun4v/lib/sparcv9/
libc_psr.so.1					
/dev/vx/dsk/bootdg/var	7065437	2507779	4487004	36%	/var
swap	21863384	2760	21860624	1%	/tmp
swap	21860672	48	21860624	1%	/var/run
swap	21860624	0	21860624	0%	/dev/vx/dmp
swap	21860624	0	21860624	0%	/dev/vx/rdmp
/dev/vx/dsk/bootdg/opt	50430351	6720986	43205062	14%	/opt
/dev/vx/dsk/datadg/lv_database	15482443	3277157	12050462	22%	/opt/sybase
/dev/vx/dsk/datadg/lv_nms	41287586	6716001	34158710	17%	/opt/U2000

If the file system information about `/dev/vx/dsk/datadg/lv_database` and `/dev/vx/dsk/datadg/lv_nms` is displayed, it indicates that the mounting status of the U2000 file system and the Sybase file system is normal.

----End

6.6.2 Clearing Disk Space

This topic describes how to clear disk space. Clearing disk space in time facilitates the normal running of the U2000 client and server.

6.6.2.1 Cleaning Up the U2000 Server Disk Space

To ensure sufficient disk space for the server, you need to delete the outdated and useless backup files and trash files to clean up the disk space. Otherwise, the insufficiency of disk space may cause a running error of the U2000 server.

6.6.2.2 Cleaning Up the U2000 Client Disk Space

To ensure the sufficient disk space for running the client, you need to clean up the disk space by deleting useless backup files and trash files. Otherwise, the insufficiency of disk space may cause a running error of the U2000 client.

6.6.2.1 Cleaning Up the U2000 Server Disk Space

To ensure sufficient disk space for the server, you need to delete the outdated and useless backup files and trash files to clean up the disk space. Otherwise, the insufficiency of disk space may cause a running error of the U2000 server.

Context

Do not delete useful files, especially operating system files. Otherwise, the U2000 server may not run stably.

Procedure

- 1 Log in to Solaris as the **root** user.
- 2 Delete the outdated and useless files:
 - Delete the outdated and useless alarm dump files. The default path is `/opt/U2000/server/dump`.
 - Delete the outdated and useless log dump files. The default path is `/opt/U2000/server/dump`.
 - Delete the outdated and useless database backup files. The default path is `/opt/U2000/server/var/backup`.
 - Delete the outdated and useless U2000 running logs. The default path is `/opt/U2000/server/log`.
 - Delete other outdated and useless files, such as installation files and patch files of earlier versions.

----End

6.6.2.2 Cleaning Up the U2000 Client Disk Space

To ensure the sufficient disk space for running the client, you need to clean up the disk space by deleting useless backup files and trash files. Otherwise, the insufficiency of disk space may cause a running error of the U2000 client.

Context

Before you delete a file, ensure that the file is no more needed. Otherwise, the U2000 client may not run stably.

Procedure

- 1 Empty the **Trash**.
- 2 Delete the files in **/opt/U2000/client/log**.
- 3 Delete other useless files.

----End

6.7 High Availability System (SUSE Linux-Distributed)

This topic describes how to manage the system files and disks of the U2000 in the High Availability System (SUSE Linux-Distributed).

[6.7.1 Checking Server Disks](#)

This topic describes how to check the usage and status of U2000 server disks.

[6.7.2 Clearing Disk Space](#)

This topic describes how to clear disk space. Clearing disk space in time facilitates the normal running of the U2000 client and server.

6.7.1 Checking Server Disks

This topic describes how to check the usage and status of U2000 server disks.

[6.7.1.1 Checking the Usage of U2000 Server Disks](#)

This topic describes how to check the usage of U2000 server disks through the System Monitor or command lines. With this operation, you can learn the remaining space and used proportion of the disks.

[6.7.1.2 Checking the Status of Server Disks](#)

This topic describes how to check the status of server disks. The abnormal disk status can lead to data loss, affecting the normal running of the NMS. It is recommended that you regularly check the disk status. If you discover any disk fault, repair or replace the disk in time.

[6.7.1.3 Checking the Disk Group Status of the U2000 Server](#)

Check whether the disk group status is normal.

[6.7.1.4 Checking the Disk Volume Status of the U2000 Server](#)

This section describes how to query the disk volume status.

[6.7.1.5 Viewing the Disk Mirroring Status](#)

This topic describes how to check the disk mirroring status after the system data is imported to the application server.

6.7.1.6 Monitoring the Mounting Status of File Systems

This topic describes how to monitor the mounting status of the U2000 file system and Oracle file system through the VCS client.

6.7.1.1 Checking the Usage of U2000 Server Disks

This topic describes how to check the usage of U2000 server disks through the System Monitor or command lines. With this operation, you can learn the remaining space and used proportion of the disks.

Procedure

- To check the disk usage through the System Monitor, do as follows:
 1. Log in to the U2000 System Monitor.
 2. Click the **Disk** tab to view the information such as the remaining space and used proportion of the disks.
- To check the disk usage through command lines, do as follows:
 1. Log in to the SuSE Linux OS as the **root** user.
 2. Run the following commands on the primary and secondary sites to check the disk usage:

df -h

Information similar to the following is displayed:

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/sda1	31G	9.6G	21G	32%	/
udev	7.9G	192K	7.9G	1%	/dev
/dev/sda6	55G	19G	37G	35%	/opt
/dev/sda3	16G	2.9G	13G	20%	/usr
/dev/sda5	21G	1.8G	19G	9%	/var
tmpfs	4.0K	0	4.0K	0%	/dev/vx
/dev/vx/dsk/datadg/lvapp	49G	12G	35G	25%	/opt/U2000
/dev/vx/dsk/datadg/lvoracle	29G	4.5G	23G	17%	/opt/oracle

----End

6.7.1.2 Checking the Status of Server Disks

This topic describes how to check the status of server disks. The abnormal disk status can lead to data loss, affecting the normal running of the NMS. It is recommended that you regularly check the disk status. If you discover any disk fault, repair or replace the disk in time.

Procedure

- 1 Log in to the SUSE Linux OS as the **nmsuser** user.
- 2 Open a terminal window. Then, run the following commands to switch to the **root** user:

```
$ su - root
```

```
Password:root user password
```

- 3 Run the following command on the primary and secondary sites:

```
# vxdisk list
```

If two disks are used, the following information is displayed:

DEVICE	TYPE	DISK	GROUP	STATUS
sda	auto:none	-	-	online invalid,
sdb	auto:none	-	-	online invalid,
sdc	auto:sliced	disk03	datadg	online

**NOTE**

The equipment name displayed in the **DEVICE** column varies according to the actual condition of the intended workstation, and thus may be different from the preceding information.

- Run the following command to switch to the non-root user:

```
# exit
```

```
----End
```

Reference Standard

The disk status can be concluded to be normal in the following situation:

After you run the **vxdisk list** command, the status of all disks is **online**.

Exception Handling

If a disk is faulty, contact the equipment supplier to repair or replace the disk in time.

6.7.1.3 Checking the Disk Group Status of the U2000 Server

Check whether the disk group status is normal.

Procedure

- Open a terminal window, and run the following commands to switch to user root:

```
% su - root
Password:password_of_user_root
```

- Run the following commands on both the primary and secondary sites:

```
# vx dg list
```

The screen output is similar to the following:

NAME	STATE	ID
datadg	enabled	997585324.1237.Primary

```
----End
```

Reference Standards

If the following standards are met, the disk group status is normal:

- If over two disks are available on the workstation, two disk groups should be displayed, including **rootdg** and **datadg**. Otherwise, there is a problem with the disk groups.
- If only two disks are available on the workstation, only one disk group, that is, **datadg**, should be displayed. Otherwise, there is a problem with the disk group.
- The **STATE** of each disk group should be **enabled**. Otherwise, there is a problem with the disk groups.

Troubleshooting

If a fault of the disk group occurs, contact the local office or Customer Service Center of Huawei according to the warranty.

6.7.1.4 Checking the Disk Volume Status of the U2000 Server

This section describes how to query the disk volume status.

Procedure

- 1 Log in to the SUSE Linux OS as the **nmsuser** user.
- 2 Open a terminal window, and run the following commands to switch to the **root** user:

```
% su - root
Password:password_of_user_root
```
- 3 Run the following commands to check whether the disk volume status is normal, according to the disk volume information:

```
# vxprint -v
```

The terminal displays:

```
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	-	-

----End

Reference Standards

If the following standards are met, it indicates that the disk volume status is normal:

- Disk volumes used by the U2000 exist. Currently, disk volume used by the U2000 is lvapp.
- For all the disk volumes, **KSTATE** must be **ENABLED**.
- For all the disk volumes, **STATE** must be **ACTIVE**.

Troubleshooting

1. If the problem persists, run the following command to record the details of all the disk volumes, and contact the local office or Customer Service Center of Huawei according to the warranty.

```
# vxprint -l VolumeName
```

Table 6-6 describes the meanings of the fields that are displayed:

Table 6-6 Field description for disk volume status

Field Name	Description
Disk group	The disk group to which this disk volume belongs.
Volume	Disk volume name.
info	Disk volume length.
type	Disk volume type.
state	Disk volume state. Normally, it should be ACTIVE, and kernel be ENABLED
assoc	Association of disk volumes, rvg refers to the RVG to which this disk volume belongs, which is datarvg normally.
plexes	The plex contained in this disk volume.
policies	Disk volume management policy.
flags	Disk volume flag.
logging	Disk volume log. Normally, the type is DCM.
recovery	Disk volume recovery mode.
device	Disk volume number and trail.
perms	Disk volume owner and authority.

For example, to query the details of the disk volume **lvapp**, you can run the following command:

```
# vxprint -l lvapp
```

The terminal displays:

```
Disk group: datadg
```

```
Volume:    lvapp
info:      len=83886080
type:      usetype=fsgen
state:     state=ACTIVE kernel=ENABLED cdsrecovery=0/0 (active)
assoc:     rvg=datarvg
           plexes=lv_nms_data-01,lv_nms_data-02,lv_nms_data-03
           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=30005 bdev=310/30005 cdev=310/30005 path=/dev/vx/dsk/datadg/
           lv_nms_data
perms:     user=root group=root mode=0666
guid:      {fc6b83b0-5c89-11db-92ae-002128053518}
```


6.7.1.5 Viewing the Disk Mirroring Status

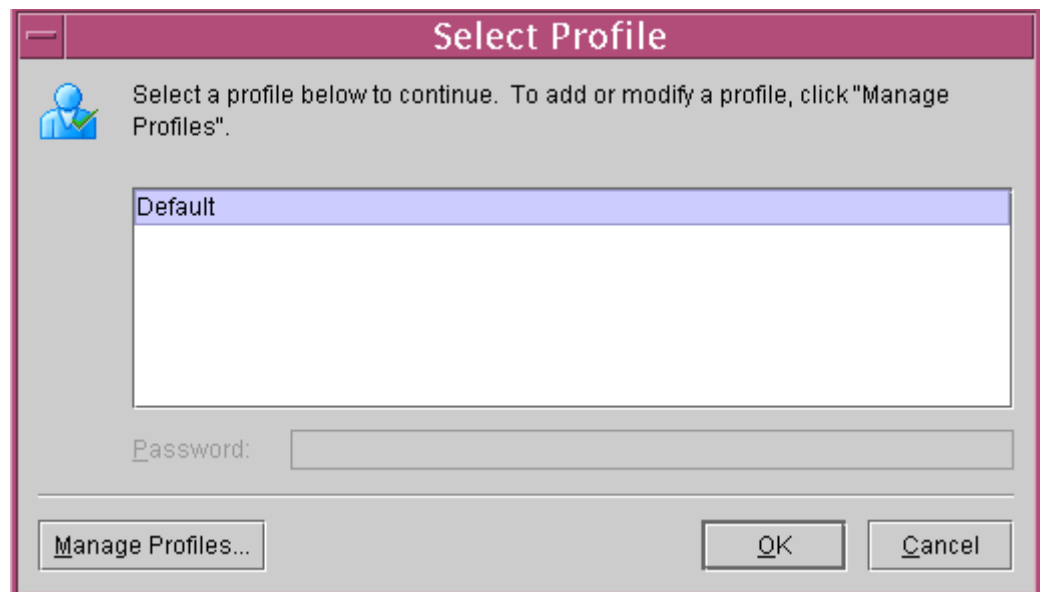
This topic describes how to check the disk mirroring status after the system data is imported to the application server.

Procedure

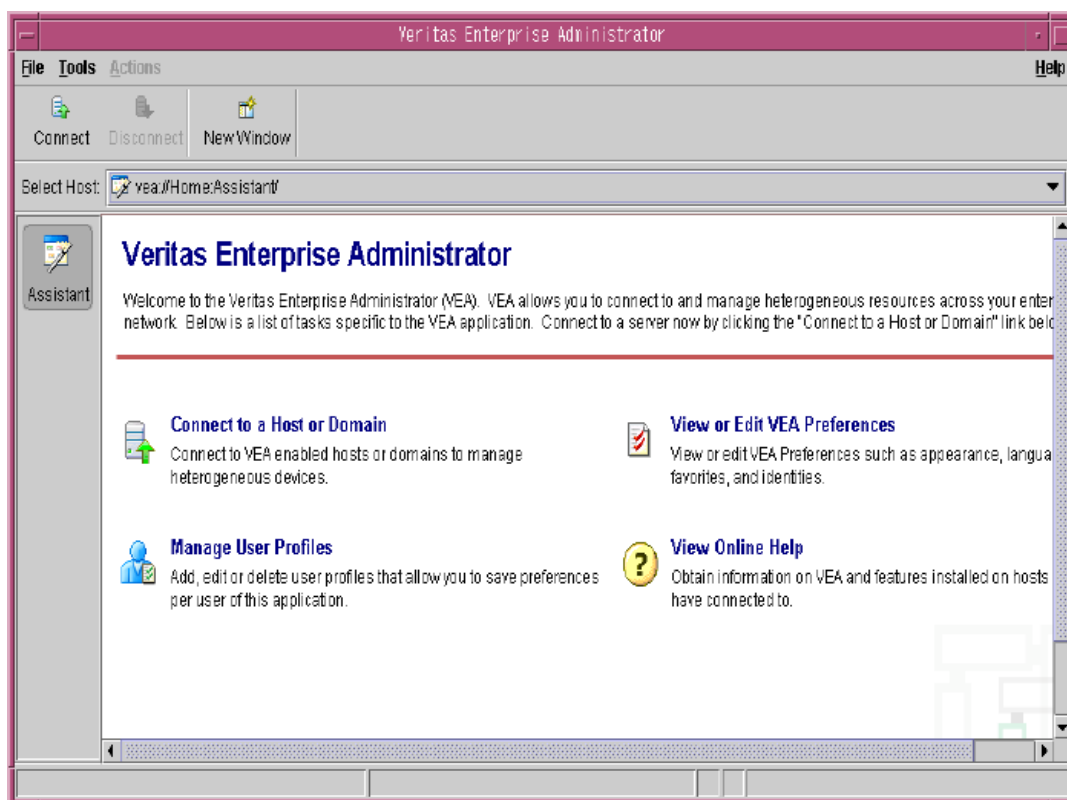
- 1 Log in to the Veritas Enterprise Administrator (VEA) client.
 1. Run the following command to start the VEA client:

vea&
 2. In the dialog box shown in [Figure 6-25](#), click **OK**.

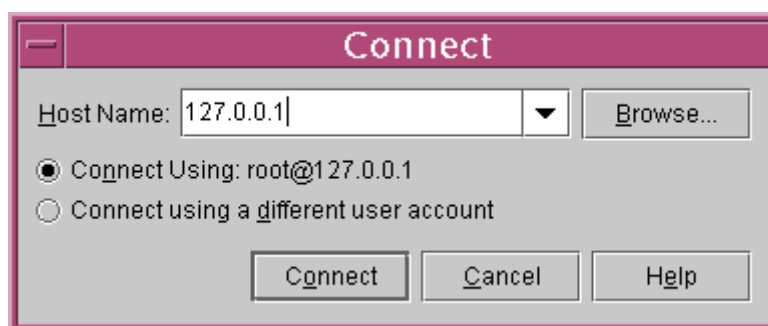
Figure 6-25 Selecting a profile



3. In the dialog box shown in [Figure 6-26](#), click **Connect**.

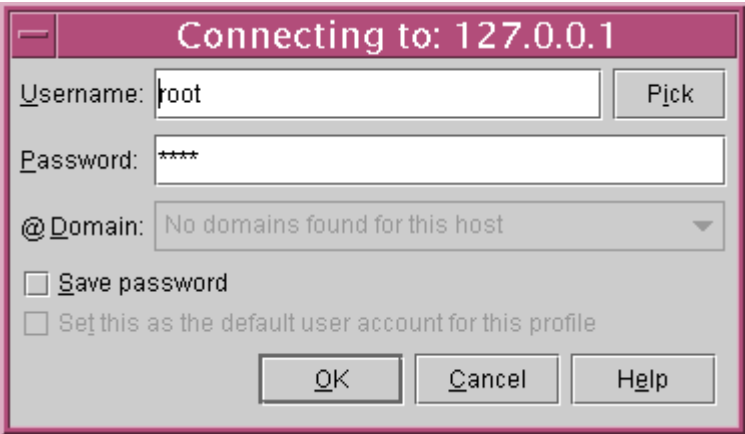
Figure 6-26 Logging in to the VEA

4. In the dialog box shown in [Figure 6-27](#), enter **127.0.0.1**, and then click **Connect**.

Figure 6-27 Connecting to the server

5. In the dialog box shown in [Figure 6-28](#), enter the valid user name and password of the server. Then, click **OK**.

Figure 6-28 Entering the user name and password

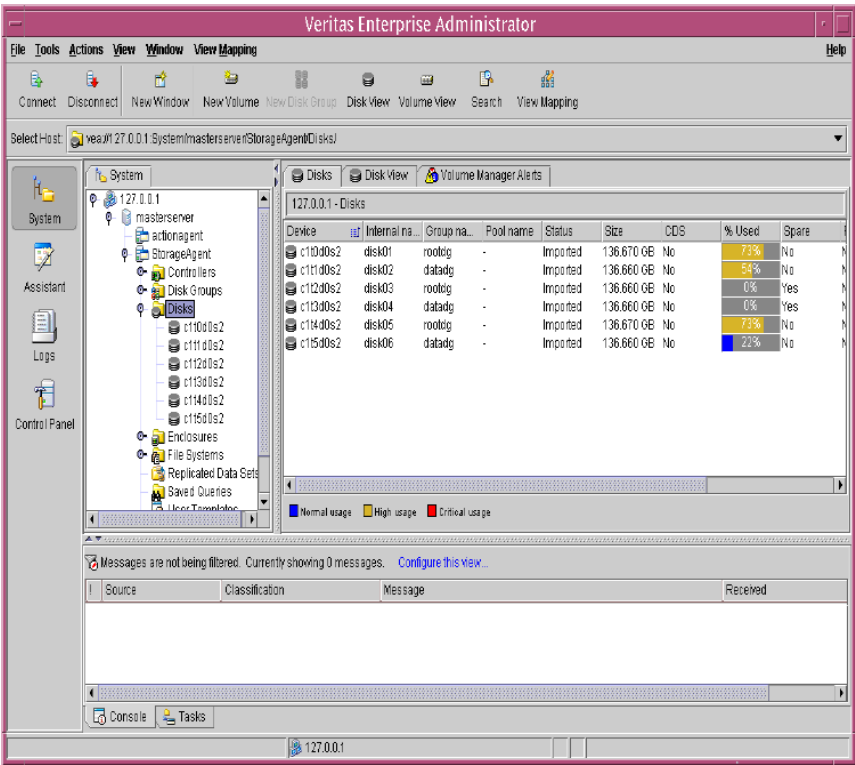


 NOTE

The user name and password to be entered here is the user name and password of the **root** user.

- 2 In the window shown in **Figure 6-29**, choose **Disks** under the server node (such as **127.0.0.1**) from the **Management Console** navigation tree.

Figure 6-29 Viewing the disk mirroring result



 NOTE

The disk names and quantity vary according to the model of the server. Thus, you need to check the disk mirroring relations of the server.

----End

Result

The first disk is encapsulated into the **rootdg** disk group and the second disk is encapsulated into the **datadg** disk group. The third disk mirrors the first disk and the fourth mirrors the second. The fifth disk serves as the hot standby disk and the sixth disk serves as the cold standby disk.

6.7.1.6 Monitoring the Mounting Status of File Systems

This topic describes how to monitor the mounting status of the U2000 file system and Oracle file system through the VCS client.

Procedure

- 1 Log in to the SUSE Linux OS as the **nmsuser** user.
- 2 Open a terminal window. Then, run the following commands to switch to the **root** user:

```
$ su -root
```

```
Password:root user password
```

- 3 Run the following command to view the mounting status of the U2000 file system and Oracle file system:

```
# df -k
```

The following information is displayed:

Filesystem	1K-blocks	Used	Available	Use%	Mounted on
/dev/sda2	55G 24G	29G	46%	/,	
udev	7.9G 180K	7.9G	1%	/dev,	
tmpfs	4.0K 0	4.0K	0%	/dev/vx,	
/dev/vx/dsk/datadg/lvapp,	9.7G 9.7G	0	100%	/opt/U2000,	
/dev/vx/dsk/datadg/lvoracle,	20G 5.3G	13G	29%	/opt/oracle,	
/dev/vx/dsk/datadg/lvdata,	20G 17G	1.4G	93%	/opt/oracle/oradb/data	

If the file system information about **/dev/vx/dsk/datadg/lvoracle** and **/dev/vx/dsk/datadg/lvapp** is displayed, it indicates that the mounting status of the Oracle file system and U2000 file system is normal.

----End

6.7.2 Clearing Disk Space

This topic describes how to clear disk space. Clearing disk space in time facilitates the normal running of the U2000 client and server.

6.7.2.1 Cleaning Up the U2000 Server Disk Space

To ensure sufficient disk space for the server, you need to delete the outdated and useless backup files and trash files to clean up the disk space. Otherwise, the insufficiency of disk space may cause a running error of the U2000 server.

6.7.2.2 Cleaning Up the U2000 Client Disk Space

To ensure the sufficient disk space for running the client, you need to clean up the disk space by deleting useless backup files and trash files. Otherwise, the insufficiency of disk space may cause a running error of the U2000 client.

6.7.2.1 Cleaning Up the U2000 Server Disk Space

To ensure sufficient disk space for the server, you need to delete the outdated and useless backup files and trash files to clean up the disk space. Otherwise, the insufficiency of disk space may cause a running error of the U2000 server.

Context

Do not delete useful files, especially operating system files. Otherwise, the U2000 server may not run stably.

Procedure

- 1 Log in to SuSE Linux as the **root** user.
- 2 Delete the outdated and useless files:
 - Delete the outdated and useless alarm dump files. The default path is **/opt/U2000/server/dump**.
 - Delete the outdated and useless log dump files. The default path is **/opt/U2000/server/dump**.
 - Delete the outdated and useless database backup files. The default path is **/opt/U2000/server/var/backup**.
 - Delete the outdated and useless U2000 running logs. The default path is **/opt/U2000/server/log**.
 - Delete other outdated and useless files, such as installation files and patch files of earlier versions.

----End

6.7.2.2 Cleaning Up the U2000 Client Disk Space

To ensure the sufficient disk space for running the client, you need to clean up the disk space by deleting useless backup files and trash files. Otherwise, the insufficiency of disk space may cause a running error of the U2000 client.

Context

Before you delete a file, ensure that the file is no more needed. Otherwise, the U2000 client may not run stably.

Procedure

- 1 Empty the **Trash**.

2 Delete the files in **/opt/U2000/client/log**.

3 Delete other useless files.

----End

7 Log Management

About This Chapter

The log records the operations and important system events on the U2000. You can use log management to query and collect statistics on logs.

[7.1 Getting to Know Log Management](#)

You can understand conceptual knowledge of log management such as log management functions and log types. The knowledge helps you to perform log operations.

[7.2 Managing Operation Logs](#)

You can query and collect statistics on operation logs of the U2000 to understand the operation status of the U2000.

[7.3 Managing System Logs](#)

You can query and collect statistics on system logs of the U2000 to understand the running status of the U2000.

[7.4 Managing Security Logs](#)

You can query and collect statistics on security logs of the U2000 to understand the security operation status of the U2000.

[7.5 Managing NE Logs](#)

You can use this function of The U2000 to query, dump, and synchronize logs on the U2000 after the logs of the managed NEs are synchronized. The U2000 also provides the function of collecting statistics on NE log commands.

[7.6 Setting Log Templates](#)

By setting log templates, you can save the specific query and statistical conditions in log templates. This helps you to query and collect statistics on logs conveniently.

[7.7 Setting a Log Forwarding Server](#)

You can set a log forwarding server to forward the U2000 logs to a third-party server.

[7.8 Managing Log Data](#)

By dumping logs, you can periodically or manually clear the log information that is not required, preventing the log information from occupying many resources. By exporting logs to files, you can view logs and identify faults.

[7.9 Managing NE Syslog](#)

Syslog management provides the occurrence time, severity, and cause of a fault on a NE, which helps you analyze and solve the problem.

[7.10 Transferring NE Logs to Log Servers](#)

The Syslog protocol allows you to transfer the logs of an NE to the log servers, in the format defined by the Syslog protocol.

7.1 Getting to Know Log Management

You can understand conceptual knowledge of log management such as log management functions and log types. The knowledge helps you to perform log operations.

7.1.1 Log Management Function

In log management, the system, security, and operation logs that are generated during U2000 running are recorded. You can query and collect statistics on logs to understand the U2000 running status, system security status, or specific user operation. In addition, you can save log results to a file or print the log results for future browse.

7.1.2 Log Types

The U2000 has operation logs, system logs, security logs and NE logs. The four types of logs record different log information.

7.1.1 Log Management Function

In log management, the system, security, and operation logs that are generated during U2000 running are recorded. You can query and collect statistics on logs to understand the U2000 running status, system security status, or specific user operation. In addition, you can save log results to a file or print the log results for future browse.

U2000 log management includes the functions such as querying logs, collecting statistics on logs, managing log templates, saving logs, and printing logs.

7.1.2 Log Types

The U2000 has operation logs, system logs, security logs and NE logs. The four types of logs record different log information.

7.1.2.1 Security Logs

This topic describes the meaning, path, and parameters of security logs. In security logs, the maintenance personnel can view security information that the U2000 records. In addition, by collecting statistics on security logs, you can count the number of statistics items based on the statistics conditions.

7.1.2.2 Operation Logs

This topic describes the meaning, path, and parameters of operation logs. In operation logs, the maintenance personnel can view the user operation information that the U2000 records. In addition, by collecting statistics on operation logs, you can count the number of statistics items based on the statistics conditions.

7.1.2.3 NE Syslog

U2000 NE logs record the operations on the managed NEs. The U2000 NE syslog running logs record the running information about U2000 NEs. The NE syslog operation logs and NE syslog running logs help you to know the NE running information.

7.1.2.4 System Logs

This topic describes the meaning, path, and parameters of system logs. In system logs, the maintenance personnel can view the system operation information that the U2000 records. In addition, you can collect statistics on system logs based on the log severity or source.

7.1.2.1 Security Logs

This topic describes the meaning, path, and parameters of security logs. In security logs, the maintenance personnel can view security information that the U2000 records. In addition, by collecting statistics on security logs, you can count the number of statistics items based on the statistics conditions.

Description

Security logs record the security operations that the user performs in the U2000, for example, login, logout, locking, and unlocking.

Path

Security logs are stored in the database. You can query them through the client. The entry for querying security logs through the client is **Administration > Log Management > Query Security Logs**.

Security logs can be dumped to a file from the database. The navigation path is **Administration > Task Schedule > Task Management**. By default, the dump path of the security logs is **\$installation path of the NMS/dump/ThresholdExport/Log(Solaris/Linux), %installation path of the NMS%\dump\ThresholdExport\Log(Windows)**.

After the security logs are dumped, the U2000 generates the relative folder and log file.

- Folder: The folder is named in the format YYMMDD in the dump path. "YYMMDD" indicates the date when the security logs are dumped.
- Log file: The following two files are generated in the folder: **YYMMDDHHMMSS-security-log-dateThreshold_info.xml** and **YYMMDDHHMMSS-security-log-dateThreshold-Number.FileName extension**. The file with the suffix **_info.xml** saves the configuration information of the dumped logs, and the file with the suffix **-Number.FileName extension** saved the dumped logs.

 NOTE

Security logs can be dumped to a .csv or .xml file, and the file can be compressed to a .zip package.

Parameters

Parameter Name	Parameter Meaning
Security Event	Event that is related to U2000 security.
Risk Level	Level of risks caused by the operations that are performed on the U2000. There are three risk levels: Warning, Minor, and Risk.
Operation User	U2000 user.
User Type	Type of an U2000 user.
Operation Time	Time when an operation is performed. It is accurate to second.
Operation Terminal	IP address of the host where an operation is performed.

Parameter Name	Parameter Meaning
Operation Object	Object that an operation is performed on.
Operation Result	Result of an operation: succeeded, failed or partly succeeded.
Details	Other useful information about an operation.

7.1.2.2 Operation Logs

This topic describes the meaning, path, and parameters of operation logs. In operation logs, the maintenance personnel can view the user operation information that the U2000 records. In addition, by collecting statistics on operation logs, you can count the number of statistics items based on the statistics conditions.

Description

Operation logs record the information about the non-security operations that the user performs in the U2000, for example, muting and unmuting the alarm sound.

Path

Operation logs are stored in the database. You can query them through the client. The entry for querying operation logs through the client is **Administration > Log Management > Query Operation Logs**.

Operation logs can be dumped to a file from the database. The navigation path is **Administration > Task Schedule > Task Management**. By default, the dump path of the operation logs is **\$installation path of the NMS/dump/ThresholdExport/Log(Solaris/Linux), %installation path of the NMS%\dump\ThresholdExport\Log(Windows)**.

After the operation logs are dumped, the U2000 generates the relative folder and log file.

- Folder: The folder is named in the format YYMMDD in the dump path. "YYMMDD" indicates the date when the operation logs are dumped.
- Log file: The following two files are generated in the folder: **YYMMDDHHMMSS-operation-log-dateThreshold_info.xml** and **YYMMDDHHMMSS-operation-log-dateThreshold-Number.FileName extension**. The file with the suffix **_info.xml** saves the configuration information of the dumped logs, and the file with the suffix **-Number.FileName extension** saved the dumped logs.

NOTE

Operation logs can be dumped to a .csv or .xml file, and the file can be compressed to a .zip package.

Parameters

Parameter Name	Parameter Meaning
Operation Name	Name of an operation that a user performs on the U2000.

Parameter Name	Parameter Meaning
Risk Level	Levels of risks caused by the operations that are performed on the U2000: Warning, Minor, and Risk.
Operation User	U2000 user.
User Type	Type of an U2000 user.
Operation Time	Time when an operation executes. It is accurate to second.
Operation Category	Type of an U2000 operation.
Operation Terminal	IP address of the host where an operation is performed.
Operation Object	Object that an operation is performed on.
Operation Result	Result of an operation: succeeded, failed and partly succeeded.
Details	Other useful information about an operation.

7.1.2.3 NE Syslog

U2000 NE logs record the operations on the managed NEs. The U2000 NE syslog running logs record the running information about U2000 NEs. The NE syslog operation logs and NE syslog running logs help you to know the NE running information.

Description

NE syslog operation logs record the operations on the managed NEs. You can query the NE syslog operation logs through the U2000 client GUI. You do not need to query the NE syslog operation logs on each NE.

The NE syslog running logs record the running information of U2000 NEs. By obtaining all NE syslog running logs from NEs through the U2000, you can view the NE syslog running logs managed by the U2000 through the U2000, instead of viewing the NE syslog running logs on each NE.

Path

The entry for querying NE syslogs through the client is **Administration > NE Security Management > NE Syslog Run Log**.

NE syslog operation logs are saved in **client/report(Solaris/Linux) client\report (Windows)**. The path description is as follows.

Path	Description
client/report (Solaris/Linux) client\report (Windows)	NEs logs in this path record the NMS user operations on the U2000. The naming convention of NE logs is DevLog_year_month_day_hour_minute_second.a suffix. The suffix of the log file name supports the .csv, .html, .txt, and .xls formats.

NE syslog running logs are saved in **server/log/syslog(Solaris/Linux)** **server\log\syslog (Windows)**. The path description is as follows.

Path	Description
server/log/syslog(Solaris/Linux) server\log\syslog(Windows)	The NE syslog running logs in this directory record the results of operations performed on U2000 NEs. The NE syslog running log files are named in the format of year_month_day_hour_minute_second.a suffix. The suffix of a log file name can be .txt or .zip.

Parameters

Parameter Name	Parameter Meaning
NE Name	The name of the NE managed by the NMS.
Time	The specific time when an operation is performed. It is accurate to second.
User Name	The user name of the NE managed by the NMS.
Access Method	The access method of a NE user for NEs.
IP Address	The IP address of the host used to perform an operation.
User Command	The command used to perform operations on the NE.

Parameter Name	Parameter Meaning
Result	There are four kinds of operation results: Failed, Succeeded, Unknown, and - . NOTE ● Unknown: Other NE operation results reported in MML mode are displayed as Unknown except for succeeded and failed operation results. ● -: There is no Result in the NE operation logs reported in SNMP mode. Therefore, the NE operation logs reported in SNMP mode are displayed as -.
Memo	The remark for NE operation logs.
User Command Detail	The details of the commands used by the user.

Parameter Name	Parameter Meaning
NE Name	The name of the NE managed by the NMS.
IP Address	The IP address of the NE managed by the NMS.
Digest	The digest of the NE syslog running log.
Content	The details of the NE syslog running log.
Module Name	The name of the module corresponding to the NE syslog running log.
Level	The level of the NE syslog running log.
Sending Time	The time when the NE syslog running log is sent.

7.1.2.4 System Logs

This topic describes the meaning, path, and parameters of system logs. In system logs, the maintenance personnel can view the system operation information that the U2000 records. In addition, you can collect statistics on system logs based on the log severity or source.

Description

System logs record the operations or tasks that the U2000 performs automatically, for example, scheduled tasks and system tasks.

Path

System logs are stored in the database. You can query them through the client. The entry for querying system logs through the client is **Administration > Log Management > Query System Logs**.

System logs can be dumped to a file from the database. The navigation path is **Administration > Task Schedule > Task Management**. By default, the dump path of the system logs is **\$installation path of the NMS/dump/ThresholdExport/Log(Solaris/Linux), %installation path of the NMS%\dump\ThresholdExport\Log(Windows)**.

After the system logs are dumped, the U2000 generates the relative folder and log file.

- Folder: The folder is named in the format YYMMDD in the dump path. "YYMMDD" indicates the date when the system logs are dumped.
- Log file: The following two files are generated in the folder: **YYMMDDHHMMSS-system-log-dateThreshold_info.xml** and **YYMMDDHHMMSS-system-log-dateThreshold-Number.FileName extension**. The file with the suffix **_info.xml** saves the configuration information of the dumped logs, and the file with the suffix **-Number.FileName extension** saved the dumped logs.

 NOTE

System logs can be dumped to a .csv or .xml file, and the file can be compressed to a .zip package.

Parameters

Parameter Name	Parameter Meaning
Level	Levels of risks caused by the operations performed on the U2000: Warning, Minor, and Risk.
Source	Module where the U2000 performs an operation.
Time	Time when an operation is performed. It is accurate to second.
Basic Information	Information about basic operations.
Operation Result	Result of an operation: succeeded, failed or unkonwn.
Details	Other useful information about an operation.

7.2 Managing Operation Logs

You can query and collect statistics on operation logs of the U2000 to understand the operation status of the U2000.

7.2.1 Querying Operation Logs

You can query operation logs to know the operation records of the U2000.

7.2.2 Collecting Statistics on Operation Logs

You can know the operation status by collecting statistics and analyzing operation logs. For example, you can know the period during which a maximum number of operations are performed and the operations that are performed most frequently.

7.2.1 Querying Operation Logs

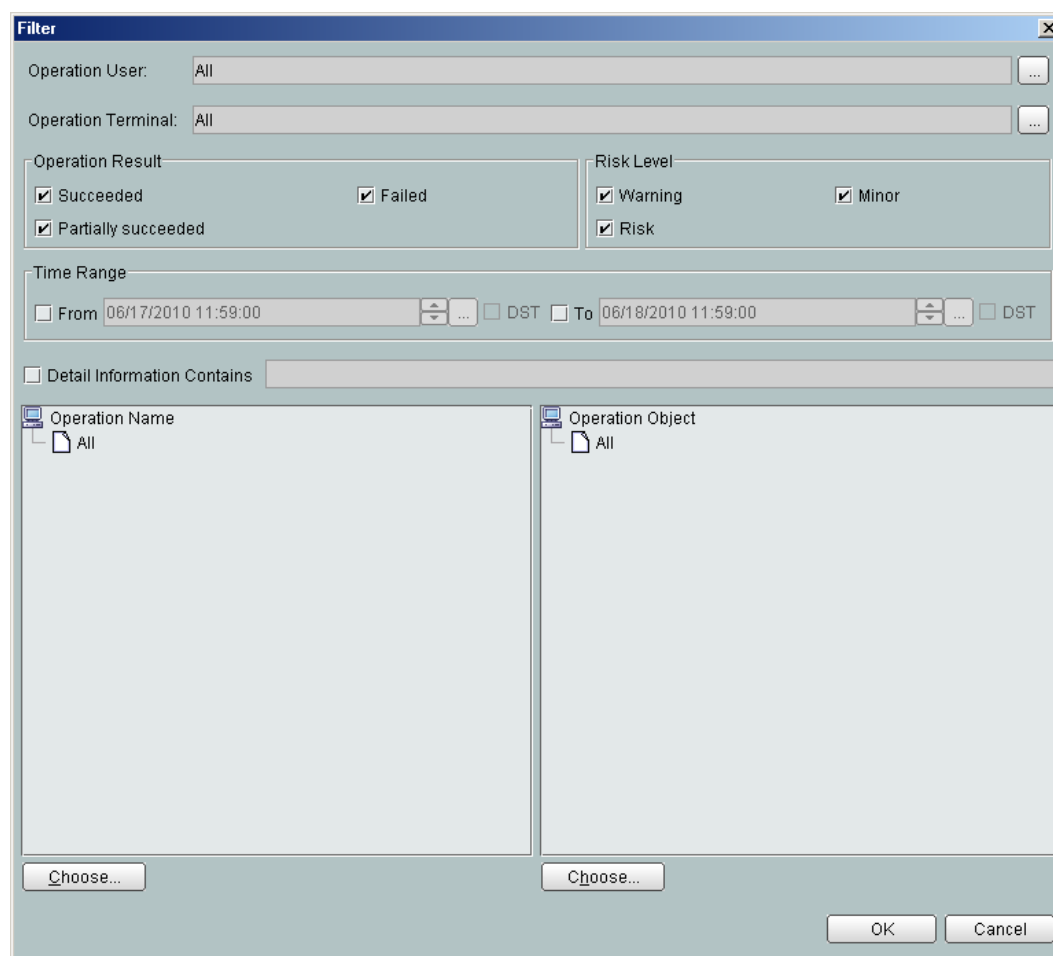
You can query operation logs to know the operation records of the U2000.

Context

- When you query operation logs by user name, only names of the users that have performed operations are displayed under **Available Operation User** in the **Select Operation User** dialog box.
- The statistical result is generated based on the existing data in the database. If the database is empty, there is no statistical result.

Procedure

- 1 Choose **Administration > Log Management > Query Operation Logs** from the main menu.
- 2 In the **Filter** window, set the filtering conditions, and then click **OK**.





NOTE

You can query logs in the **Query Operation Logs** window in the following ways:

- Click **Template Filter**, and then select **Open**. Select a template from the template list, and then click **Open** to use an existing template to query logs. If no template exists on the U2000, see [7.6 Setting Log Templates](#) to create a template.
- Set the query conditions in the **Filter** dialog box, and then click **OK** to query logs.

3 In the **Query Operation Logs** window, double-click a record to view the log details.

- Click a field in the header of the query result table to sort the query results by field.
- A white upward triangular icon  indicates that you can sort the results by field. A black upward triangular icon  indicates that the results are sorted in the ascending order by field. The black downward triangular icon  indicates that the results are sorted in the descending order by field.
- Click the **Device Name**, or **Access Method** field. Different from other table header fields, these fields are displayed in groups. Therefore, they are not sorted in alphabetic order.

----End

7.2.2 Collecting Statistics on Operation Logs

You can know the operation status by collecting statistics and analyzing operation logs. For example, you can know the period during which a maximum number of operations are performed and the operations that are performed most frequently.

Context

The statistical result is generated based on the existing data in the database. If the database is empty, there is no statistical result.

Procedure

- 1 Choose **Administration > Log Management > Operation Log Statistics** from the main menu.
- 2 In the **Statistic Filter** window, set the statistical items and statistical conditions, and then click **OK**.

Statistic Filter

Statistical Items Filter Condition

Statistic Row

Statistic Item
Operation User

Statistic Item
Operation Name

Statistic Column

Statistic Item
Operation Terminal

Example

Statistical Items	Statistic Column	Statistic Column
Statistics Result	2	2
Statistic Row	1	1
Statistic Row	1	1

OK Cancel

NOTE

You can also click **Cancel**, and then collect statistics in the **Operation Log Statistics** window in the following ways:

- Click **Template**, and then select **Open**. Select a template from the template list, and then click **Open** to use an existing template to collect statistics on operation logs. If no template exists on the U2000, see [7.6 Setting Log Templates](#) to create a template.
- Click **Statistic Filter**. Set **Statistical Items** and **Filter Condition** in the **Statistic Filter** window, and then click **OK** to collect statistics on operation logs.

----End

Result

In the **Operation Log Statistics** window, the statistical result is displayed.

Perform the following operations as required:

- Click **Print** to print the statistical result.
- Click **Save As** to save the statistical result.

7.3 Managing System Logs

You can query and collect statistics on system logs of the U2000 to understand the running status of the U2000.

7.3.1 Querying System Logs

You can query system logs to know the important events that occur when the U2000 is running.

7.3.2 Collecting Statistics on System Logs

You can know the system status by collecting statistics and analyzing the system log. For example, you can know the type of the services that raise the most alarms.

7.3.1 Querying System Logs

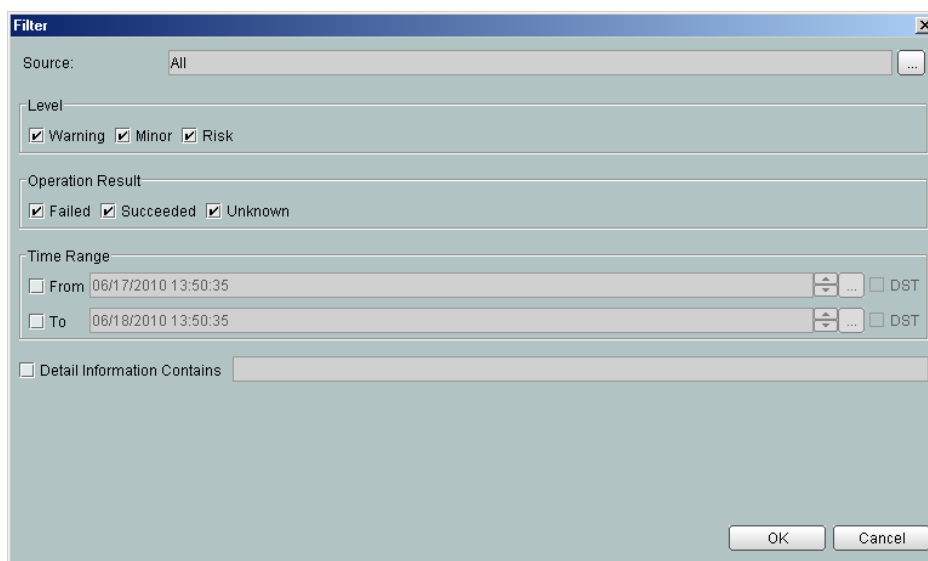
You can query system logs to know the important events that occur when the U2000 is running.

Context

The statistical result is generated based on the existing data in the database. If the database is empty, there is no statistical result.

Procedure

- 1 Choose **Administration > Log Management > Query System Logs** from the main menu.
- 2 In the **Filter** window, set the filtering conditions, and then click **OK**.



NOTE

You can query logs in the **Query System Logs** window in the following ways:

- Click **Template Filter**, and then select **Open**. Select a template from the template list, and then click **Open** to use an existing template to query logs. If no template exists on the U2000, see [7.6 Setting Log Templates](#) to create a template.
 - Set the query conditions in the **Filter** window, and then click **OK** to query logs.
- 3 In the **Query System Logs** window, double-click a record to view the log details.
 - Click a field in the header of the query result table to sort the query results by field.
 - A white upward triangular icon indicates that you can sort the results by field. A black upward triangular icon indicates that the results are sorted in the ascending order by

field. The black downward triangular icon ▼ indicates that the results are sorted in the descending order by field.

- Click the **Device Name**, or **Access Method** field. Different from other table header fields, these fields are displayed in groups. Therefore, they are not sorted in alphabetic order.

----End

7.3.2 Collecting Statistics on System Logs

You can know the system status by collecting statistics and analyzing the system log. For example, you can know the type of the services that raise the most alarms.

Context

The statistical result is generated based on the existing data in the database. If the database is empty, there is no statistical result.

Procedure

- 1 Choose **Administration > Log Management > System Log Statistics** from the main menu.
- 2 In the **Statistic Filter** window, set the statistical condition, and then click **OK**.

Statistic Filter

Statistical Items | Filter Condition

Statistic Row

Statistic Item
Level ▼

Statistic Column

Statistic Item
Source ▼

Example

Statistical Items	Statistic Column	Statistic Column
Statistics Result	2	2
Statistic Row	1	1
Statistic Row	1	1

OK Cancel



NOTE

You can also click **Cancel**, and then collect statistics in the **System Log Statistics** window in the following ways:

- Click **Template**, and then select **Open**. Select a template from the template list, and then click **Open** to use an existing template to collect statistics on system logs. If no template exists on the U2000, see [7.6 Setting Log Templates](#) to create a template.
- Click **Statistic Filter**. Set the statistical condition in the **Statistic Filter** window, and then click **OK** to collect statistics on system logs.

----End

Result

In the **System Log Statistics** window, the statistical result is displayed.

Perform the following operations as required:

- Click **Print** to print the statistical result.
- Click **Save As** to save the statistical result.

7.4 Managing Security Logs

You can query and collect statistics on security logs of the U2000 to understand the security operation status of the U2000.

[7.4.1 Querying Security Logs](#)

You can query security logs to know the security operations of the U2000.

[7.4.2 Collecting Statistics on Security Logs](#)

You can know the security operations by collecting statistics and analyzing security logs. For example, you can know the period during which maximum number of security operations are performed and the operations that are performed most frequently.

7.4.1 Querying Security Logs

You can query security logs to know the security operations of the U2000.

Context

The statistical result is generated based on the existing data in the database. If the database is empty, there is no statistical result.

Procedure

- 1 Choose **Administration > Log Management > Query Security Logs** from the main menu.
- 2 In the **Filter** window, set the filtering conditions, and then click **OK**.

NOTE

You can query logs in the **Query Security Logs** window in the following ways:

- Click **Template Filter**, and then select **Open**. Select a template from the template list, and then click **Open** to use an existing template to query logs.
- Set the query conditions in the **Filter** window, and then click **OK** to query logs.

3 In the **Query Security Logs** window, double-click a record to view the log details.

- Click a field in the header of the query result table to sort the query results by field.
- A white upward triangular icon indicates that you can sort the results by field. A black upward triangular icon indicates that the results are sorted in the ascending order by field. The black downward triangular icon indicates that the results are sorted in the descending order by field.
- Click the **Device Name**, or **Access Method** field. Different from other table header fields, these fields are displayed in groups. Therefore, they are not sorted in alphabetic order.

----End

7.4.2 Collecting Statistics on Security Logs

You can know the security operations by collecting statistics and analyzing security logs. For example, you can know the period during which maximum number of security operations are performed and the operations that are performed most frequently.

Context

The statistical result is generated based on the existing data in the database. If the database is empty, there is no statistical result.

Procedure

- 1 Choose **Administration > Log Management > Security Log Statistics** from the main menu.
- 2 In the **Statistic Filter** window, set the statistical items and filtering conditions, and then click **OK**.

Statistical Items	Statistic Column	Statistic Column
Statistics Result	2	2
Statistic Row	1	1
Statistic Row	1	1

NOTE

You can also click **Cancel**, and then collect statistics in the **Security Log Statistics** window in the following ways:

- Click **Template**, and then select **Open**. Select a template from the template list, and then click **Open** to use an existing template to collect statistics on security logs. If no template exists on the U2000, see [7.6 Setting Log Templates](#) to create a template.
- Click **Statistic Filter**. Set **Statistical Items** and **Filter Condition** in the **Statistic Filter** window, and then click **OK** to collect statistics on security logs.

----End

Result

In the **Security Log Statistics** window, the statistical result is displayed.

Perform the following operations as required:

- Click **Print** to print the statistical result.
- Click **Save As** to save the statistical result.

7.5 Managing NE Logs

You can use this function of The U2000 to query, dump, and synchronize logs on the U2000 after the logs of the managed NEs are synchronized. The U2000 also provides the function of collecting statistics on NE log commands.

7.5.1 Browsing the NE Syslog Running Logs

By obtaining all the NE syslog running logs through U2000 on the NE side, you can browse the NE syslog running logs of the NEs managed by the U2000 on the U2000, rather than query the running logs on each NE.

7.5.2 Synchronizing SNMP Device Logs

You can synchronize the SNMP device logs to the U2000. This helps you to view the SNMP device logs.

7.5.1 Browsing the NE Syslog Running Logs

By obtaining all the NE syslog running logs through U2000 on the NE side, you can browse the NE syslog running logs of the NEs managed by the U2000 on the U2000, rather than query the running logs on each NE.

Prerequisite

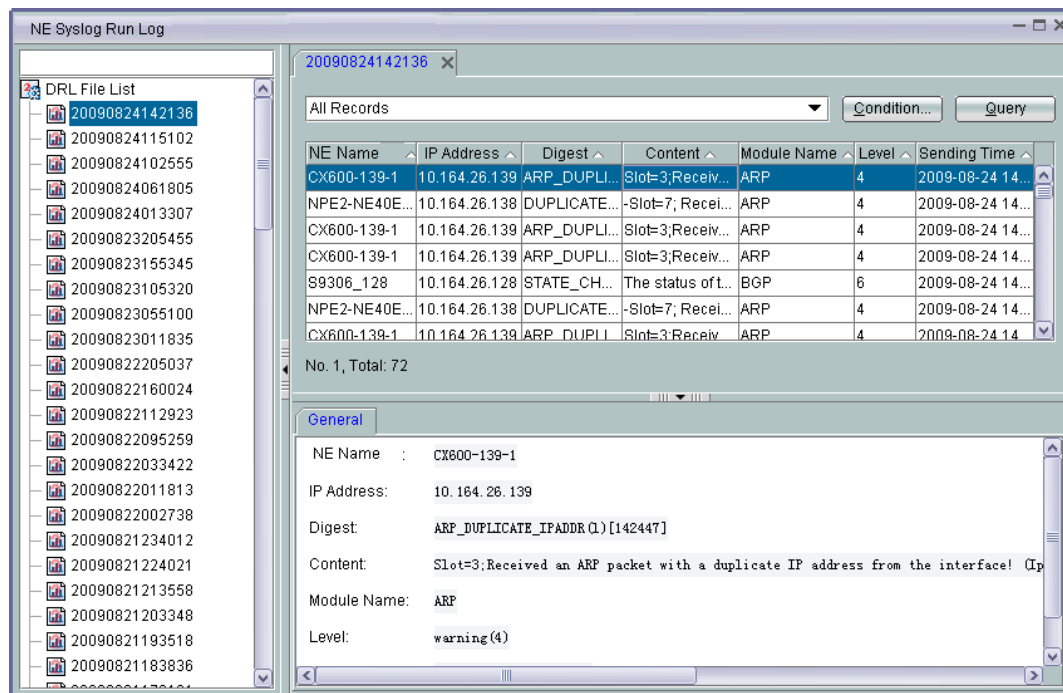
- You must be a U2000 user with the **Security Watcher** authority or higher.
- You must configure the information center on the NE side so that the NE syslog running logs can be sent to the U2000. For details about configure the information center on the NE side, refer to [7.9.4 Configuring the Information Center on the NEs](#).
- Configure the U2000 server as the receiver of NE logs. That is, set **Log Host IP Address** to the IP address of the U2000 server. For details, see [7.9.4.3 Adding the Syslog Host](#).

Context

admin can query the NE syslog running logs of all applicable NEs.

Procedure

- 1 Choose **Administration > NE Security Management > NE Syslog Run Log** from the main menu.
- 2 In the **DRL File List** navigation tree, double-click a NE syslog running log file, such as **20090824142136**. In the right-hand pane, click a record to view log details.

**NOTE**

- The files in the DRL file list are ordered by time.
- You can enter the file name in the text box above the **DRL File List** navigation tree to filter the DRL files. Only numbers from 0 to 9 are allowed. Then, the matched files are displayed in the **DRL File List** navigation tree.

3 Perform the following operations as required:

Click **Condition**. In the **Set Filter Condition** dialog box that is displayed, set the filter criteria for filtering out NE syslog running logs.

----End

7.5.2 Synchronizing SNMP Device Logs

You can synchronize the SNMP device logs to the U2000. This helps you to view the SNMP device logs.

Procedure

- 1 Choose **Administration > NE Security Management > Synchronize SNMP NE Logs of ALL Nes** from the main menu.
- 2 In the displayed dialog box, click **OK**.

----End

7.6 Setting Log Templates

By setting log templates, you can save the specific query and statistical conditions in log templates. This helps you to query and collect statistics on logs conveniently.

Context

The operations on the log query template and log statistics template are similar.

Procedure

- 1 Choose **Administration > Log Management** from the main menu.
- 2 Among the displayed menus, you can choose **Query Operation Logs**, **Query System Logs**, **Query Security Logs**, **Operation Log Statistics**, **System Log Statistics** and **Security Log Statistics**. The following takes the template for querying and collecting statistics on operation logs as an example.

Task	Operation
Create a template	1. Choose Administration > Log Management > Query Operation Logs. 2. In the Filter dialog box, click Cancel. 3. In the Query Operation Logs window, choose Template Filter > New. 4. In the Enter Template Name dialog box, enter the template name, and then click OK. 5. In the Filter dialog box, set the filtering conditions of template parameters, and then click OK.
Modify a template	If there is already a log query template or a log statistics template on the U2000, you can do as follows to modify the template: 1. In the Query Operation Logs window, choose Template Filter > Open. Select a template in the Open dialog box. 2. In the Query Operation Logs window, click Filter. 3. In the Filter dialog box, modify the query conditions in the log template, and then click OK. 4. In the Query Operation Logs window, choose Template Filter > Save.
Save As	You can do as follows to save and modify a log query or statistics template: In the Query Operation Logs window, choose Template Filter > Save As.

Task	Operation
Delete a template	If there is already a log query template or a log statistics template on the U2000, you can do as follows to delete the template: Delete the operations in the template. 1. In the Query Operation Logs window, choose Template Filter > Delete. 2. In the displayed Delete dialog box, select the specified template. 3. Click Delete.

----End

7.7 Setting a Log Forwarding Server

You can set a log forwarding server to forward the U2000 logs to a third-party server.

Context

The log forwarding server forwards only security logs and operation logs.

Procedure

- 1 Choose **Administration > Settings > Log Forwarding Server** from the main menu.



- 2 You can perform the following operations in the **Log Forwarding Server** window.

Task	Operation
Add	In the Create Log Forwarding Server dialog box, set the server that receives the logs. ● To enable the log forwarding function, select Yes from the Enable drop-down list. ● The IP address cannot be set to a loopback address. ● String Filter does not support wildcards. ● The switchover between the primary and secondary servers is supported when the value of Protocol is TCP. When the primary sever fails, the secondary server takes over the service and receives the logs. When the primary server is recovered, the service is switched back to the primary server. ● You can set a maximum of five servers to receive logs.
Modify	In the Log Forwarding Servers dialog box, select a server record, and then click Modify . In the displayed Modify Log Forwarding Server dialog box, set the server information of logs.
Delete	In the Log Forwarding Servers dialog box, select a server record, and then click Delete .
Refresh	To refresh the server information. NOTE After another user updates the information about the log forwarding server, you can click Refresh to obtain the updated information. The U2000 does not automatically update the information about the log forwarding server.
Cancel	To exit the Log Forwarding Server dialog box.

----End

7.8 Managing Log Data

By dumping logs, you can periodically or manually clear the log information that is not required, preventing the log information from occupying many resources. By exporting logs to files, you can view logs and identify faults.

7.8.1 Setting U2000 Log Timing Dumping

By setting U2000 log dump, you can periodically or instantly dump security logs, operation logs, and system logs of the U2000. The dumped logs are saved in files and deleted from the database. This prevents database space insufficiency.

7.8.2 Setting U2000 Log Overflow Dump

The U2000 supports log overflow dump. When the capacity of logs reaches the specified threshold, the U2000 periodically dump logs. Dumped logs are saved in files and deleted from the database. This prevents database space insufficiency.

7.8.3 Manually Dumping U2000 Logs

The U2000 supports the function of manually dumping logs. Dumped logs are saved in files and deleted from the database. This prevents database space insufficiency.

7.8.4 Setting U2000 Log Export

By setting U2000 log export, you can periodically or instantly export security logs, operation logs, and system logs of the U2000. The exported logs are saved in files. Thus, they cannot be deleted from the database.

7.8.1 Setting U2000 Log Timing Dumping

By setting U2000 log dump, you can periodically or instantly dump security logs, operation logs, and system logs of the U2000. The dumped logs are saved in files and deleted from the database. This prevents database space insufficiency.

Context

Each of the types **Operation Log Dump**, **Security Log Dump** and **System Log Dump** has a default system task that is provided by the U2000. You are not allowed to delete this system task, but you can modify its setting. In addition, you cannot create new tasks of these three types.

Procedure

- 1 Choose **Administration > Task Schedule > Task Management** from the main menu.
- 2 In the **Task Type** navigation tree, choose **Database Capacity Management > Alarm/Event Log Dump, Database Capacity Management > Operation Log Dump, Database Capacity Management > Security Log Dump** or **Database Capacity Management > System Log Dump**.
- 3 Double-click the task in the task list.

NOTE

In the task list, right-click the log dump task and choose **Run At Once**. The log dump task is performed instantly.

- 4 In the displayed **Attribute** dialog box, set the parameters on the **Common Parameters** and **Extended Parameters** tabs.
- 5 Click **OK**.

----End

7.8.2 Setting U2000 Log Overflow Dump

The U2000 supports log overflow dump. When the capacity of logs reaches the specified threshold, the U2000 periodically dump logs. Dumped logs are saved in files and deleted from the database. This prevents database space insufficiency.

Context

Each of the types **Operation Log Overflow Dump**, **Security Log Overflow Dump** and **System Log Overflow Dump** has a default system task that is provided by the U2000. You are not allowed to delete the system task, but you can modify its setting. In addition, you cannot create new tasks of these three types.

Procedure

- 1 Choose **Administration > Task Schedule > Task Management** from the main menu.
- 2 In the **Task Type** navigation tree, choose **Overflow Dump > Operation Log Overflow Dump**, **Overflow Dump > Security Log Overflow Dump** or **Overflow Dump > System Log Overflow Dump**. select the type of the log overflow dump task, and then double-click the selected log dump task in the right area.
- 3 Double-click the task in the task list.



NOTE

In the right area, right-click the log dump task and choose **Run At Once**. The log dump task is performed instantly.

- 4 In the **Attribute** dialog box, modify the parameters on the **Common Parameters** and **Extended Parameters** tabs.
- 5 Click **OK**.

----End

7.8.3 Manually Dumping U2000 Logs

The U2000 supports the function of manually dumping logs. Dumped logs are saved in files and deleted from the database. This prevents database space insufficiency.

Context

Each of the types **Operation Log Manual Dump**, **Security Log Manual Dump** and **System Log Manual Dump** has a default system task that is provided by the U2000. You are not allowed to delete the system task, but you can modify its setting. In addition, you cannot create new tasks of these three types.

Procedure

- 1 Choose **Administration > Task Schedule > Task Management** from the main menu.
- 2 In the navigation tree on the left of the **Task Management** window, choose **Manual Dump > Operation Log Manual Dump**, **Manual Dump > Security Log Manual Dump** or **Manual Dump > System Log Manual Dump**.
- 3 In the task list, right-click Manual Dump task and choose **Run**.

The **Attribute** dialog box is used to configure log export parameters. It contains the following sections:

- File**:
 - Dumping to (path): /opt/U2000/server/dump/ThresholdExport/Log
 - File type: CSV
- Generation Time of Data**:
 - ☒ Start time: 01/01/2010 00:00:01 [calendar icon] [DST checkbox]
 - ☒ End time: 12/31/2037 23:59:59 [calendar icon] [DST checkbox]
- Records That Meet The Dump Condition**:
 - Total records: [text box] [Query button]

Buttons at the bottom: Delete Dump Files, Default, Save, Close, Dump.

- 4 In the **Attribute** dialog box, set the dump parameters.

NOTE

- 5 Click **Dump** to dump log.

----End

7.8.4 Setting U2000 Log Export

By setting U2000 log export, you can periodically or instantly export security logs, operation logs, and system logs of the U2000. The exported logs are saved in files. Thus, they cannot be deleted from the database.

Context

Each of the types **Operation Log Export**, **Security Log Export** and **System Log Export** has a default system task that is provided by the U2000. You are not allowed to delete the system task, but you can modify its setting. In addition, you cannot create new tasks of these three types.

Procedure

- 1 Choose **Administration > Task Schedule > Task Management** from the main menu.
- 2 In the **Task Type** navigation tree, choose **File Interface > NM Operation Log Export, File Interface > NM Security Log Export** or **File Interface > NM System Log Export**.
- 3 Double-click the task in the task list.

**NOTE**

To perform the operations such as executing an export task instantly, suspending an task, and setting timing suspending and resuming, right-click the log export task in the right area and choose the corresponding menus.

- 4 In the **Attribute** dialog box, set the parameters on the **Common Parameters** and **Extended Parameters** tabs.
- 5 Click **OK**.

----End

7.9 Managing NE Syslog

Syslog management provides the occurrence time, severity, and cause of a fault on a NE, which helps you analyze and solve the problem.

This feature is related to routers, switches, and service gateways.

7.9.1 Syslog Management Overview

This describes basic concepts and functions of Syslog Management.

7.9.2 Configuration Flow of Syslog Management

This describes the process of configuring Syslog management.

7.9.3 Deploying the NE Syslog Collector

This describes the collector on the server is responsible for saving the received Syslog packets to the database and processing the packets.

7.9.4 Configuring the Information Center on the NEs

This describes how to configure the information center on the NEs. You need to configure the information center on the NEs before using the Syslog management function of the U2000.

7.9.1 Syslog Management Overview

This describes basic concepts and functions of Syslog Management.

7.9.1.1 Functions of Syslog Management

Syslog management can implement functions such as sending, receiving, and parsing Syslog packets sent by a NE. It also provides the functions of querying NE syslog running logs.

7.9.1.2 Basic Concepts

This describes basic concepts of Syslog management.

7.9.1.1 Functions of Syslog Management

Syslog management can implement functions such as sending, receiving, and parsing Syslog packets sent by a NE. It also provides the functions of querying NE syslog running logs.

NE logs record various situations occurred during the NE operation in real time. Logs can be exported to the log buffer, log file, console, terminal display, and log host for storage and browsing. When a fault occurs and you need to know the NE syslog running information, you can query the logs to locate the fault. Because the disk space of the NE is limited, the U2000 Syslog management can implement functions such as receiving, parsing, and viewing Syslog packets sent by the NEs.

7.9.1.2 Basic Concepts

This describes basic concepts of Syslog management.

Syslog Packets

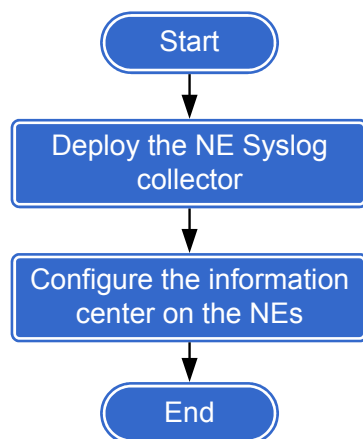
The output format of the NE log is Syslog. To enable the NMS to receive Syslog packets sent by the NEs, you need to configure related commands for sending log information to the log host on the NEs. Syslog packets are transmitted through the User Datagram Protocol (UDP) and sent to the log host (the U2000) through port 514. The U2000 parses and writes the received Syslog packets to the database. Then you can query NE logs on the U2000 client.

7.9.2 Configuration Flow of Syslog Management

This describes the process of configuring Syslog management.

Figure 7-1 shows the flowchart of configuring Syslog management.

Figure 7-1 Process of configuring Syslog management



7.9.3 Deploying the NE Syslog Collector

This describes the collector on the server is responsible for saving the received Syslog packets to the database and processing the packets.

Procedure

- 1 Install the components of the Network Element Management Subsystem.

----End

7.9.4 Configuring the Information Center on the NEs

This describes how to configure the information center on the NEs. You need to configure the information center on the NEs before using the Syslog management function of the U2000.



CAUTION

In Solaris, both the NMS syslog process and the Solaris syslogd service use the UDP port 514 to collect information. Because of the port occupation conflict, two services cannot be used at the same time. Thus, the Solaris syslogd service must be disabled. You can use one of the following methods to disable the Solaris syslogd service:

- Run the following command in the terminal window:
#syslogd -t
The command is applicable to the current configuration only. If the operating system (OS) restarts, you need to run this command again.
- Modify the file **/etc/default/syslogd**:
Modify the last line **LOG_FROM_REMOTE=YES** to **LOG_FROM_REMOTE=NO**, delete the number sign (#) in this line, and save the file. Then restart the system.

7.9.4.1 Enabling the Information Center

This describes how to enable the information center. You need to enable the information center before configuring parameters of the information center on the NEs.

7.9.4.2 Configuring the Syslog Source Interface

This describes how to configure the service status of Syslog source interface. After you configure a specified interface IP address for the Syslog service, the log host can classify logs according to the source IP address.

7.9.4.3 Adding the Syslog Host

This describes how to configure the IP Address, channel number, log tool, and log language of the log host.

7.9.4.4 Configuring the Advanced Attributes of the Syslog Service

This describes how to set the parameters about log buffer and the channel number of a log file.

7.9.4.1 Enabling the Information Center

This describes how to enable the information center. You need to enable the information center before configuring parameters of the information center on the NEs.

Context

- After the information center is enabled, the classification and output of information (especially much information for processing) may affect the system performance to some extent.
- By default, the information center is enabled. You can use the **display info-center** command to check the information center status.

If

```
Information Center:enabled
```

is displayed, the information center is enabled.

If this information is not displayed, do as follows to enable the information center.

Procedure

- 1 Run the **system-view** command to enter the system view.

- 2 Run the **info-center enable** command to enable the information center.

----End

7.9.4.2 Configuring the Syslog Source Interface

This describes how to configure the service status of Syslog source interface. After you configure a specified interface IP address for the Syslog service, the log host can classify logs according to the source IP address.

Prerequisite

- The selected NE supports the log service function on the U2000.
- The NE is configured with Telnet/STelnet parameters and its configurations are synchronized to the U2000.
- The Syslog source interface and its IP address are known.

Procedure

- 1 In the topology navigation tree or the topology view, select the NE to be operated and right-click it. Then select **NE Explorer** on the shortcut menu.
- 2 In the service tree, expand **NE Channel Management**, and then click **Syslog Service**.
- 3 Click **Enable** or **Disable** to change the service status of the Syslog source interface.



NOTE

If the Syslog source of the host is in use, you cannot select the Syslog source interface from the drop-down list box. The displayed status button is **Disable**. Click **Disable** to disable the log source. Then you can select the Syslog source interface from the drop-down list box. The displayed status button changes to **Enable**.

- 4 When the Syslog source is disabled, select the source interface for sending Syslog files, and then click **Enable**.

----End

7.9.4.3 Adding the Syslog Host

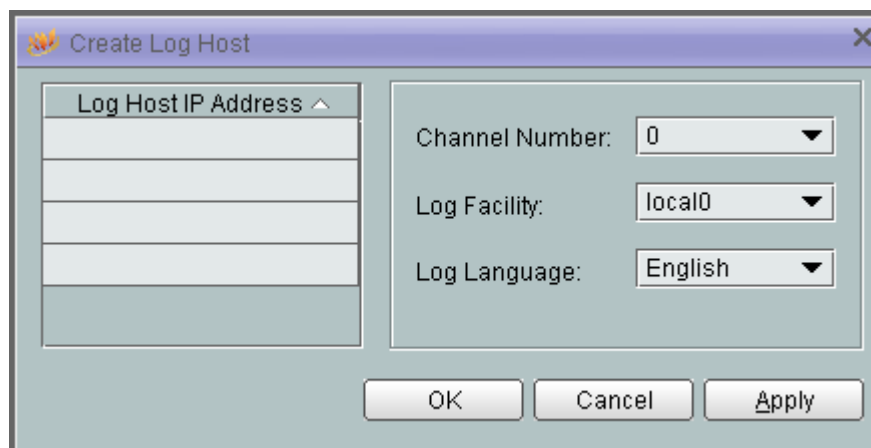
This describes how to configure the IP Address, channel number, log tool, and log language of the log host.

Prerequisite

The IP address of the log host is known.

Procedure

- 1 In the topology navigation tree or the topology view, select the NE to be operated and right-click it. Then select **NE Explorer** on the shortcut menu.
- 2 In the service tree, expand **NE Channel Management**, and then click **Syslog Service**.
- 3 Right-click on the **Syslog Service** tab and select **Create** on the shortcut menu.
- 4 In the **Create Log Host** dialog box, set the related parameters.



- 5 Click **OK** or **Apply**.



NOTE

If more than one log host is added, the **Create Log Host** progress bar is displayed.

After all the log hosts are added, click **OK**.

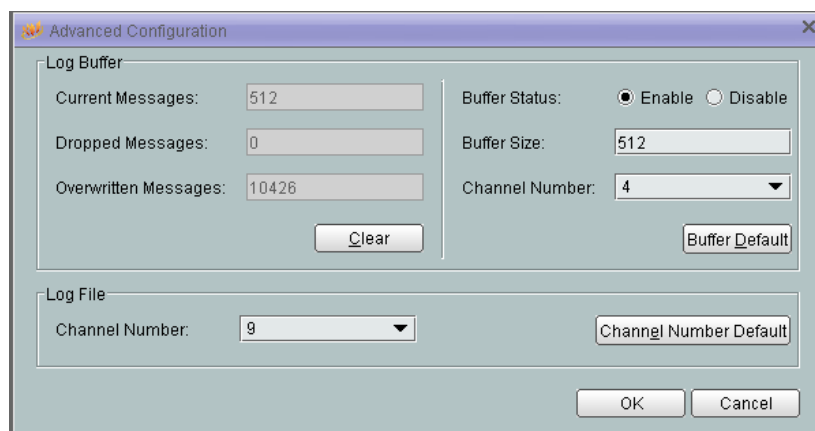
----End

7.9.4.4 Configuring the Advanced Attributes of the Syslog Service

This describes how to set the parameters about log buffer and the channel number of a log file.

Procedure

- 1 In the topology navigation tree or the topology view, select the NE to be operated and right-click it. Then select **NE Explorer** on the shortcut menu.
- 2 In the service tree, expand **NE Channel Management**, and then click **Syslog Service**.
- 3 On the **Syslog Service** tab, click **Advanced**.
- 4 In the **Advanced** dialog box, set the related parameters.



- 5 Click **OK**.

----End

7.10 Transferring NE Logs to Log Servers

The Syslog protocol allows you to transfer the logs of an NE to the log servers, in the format defined by the Syslog protocol.

Context

NOTE

Applies to the SDH and WDM series NEs.

[7.10.1 Syslog Service](#)

The syslog service is a part of the NE security management. All types of information is transmitted to the syslog server. All this information is in the format defined by the syslog protocol. The network administrator and maintainer can estimate the status of the NEs based on the severities of these information.

[7.10.2 Configuring the Syslog Server](#)

In the case of NEs that can communicate with syslog servers directly, you need to configure the syslog server on the NEs. Then, the NEs can transmit the syslog to the syslog server.

[7.10.3 Configuring the Syslog GNE](#)

In the case of For the NEs that cannot communicate with the syslog server directly, you need to configure the syslog GNE. The syslog GNE transmits all the syslog that it receives d to the syslog server.

[7.10.4 Configuring the Syslog Type and Severity](#)

Different types of syslog have different severities. The NE report the relevant information based on the severity of the syslog.

[7.10.5 Starting the Syslog Service](#)

After the syslog service is started, the NE can transmit the syslog to syslog servers.

7.10.1 Syslog Service

The syslog service is a part of the NE security management. All types of information is transmitted to the syslog server. All this information is in the format defined by the syslog protocol. The network administrator and maintainer can estimate the status of the NEs based on the severities of these information.

Definition

- Syslog Server is a workstation or a server that stores the syslog of the NEs in the network.
- Syslog GNE is an NE that receives the syslogs of other NEs and transmits all the syslogs to the Syslog Server.

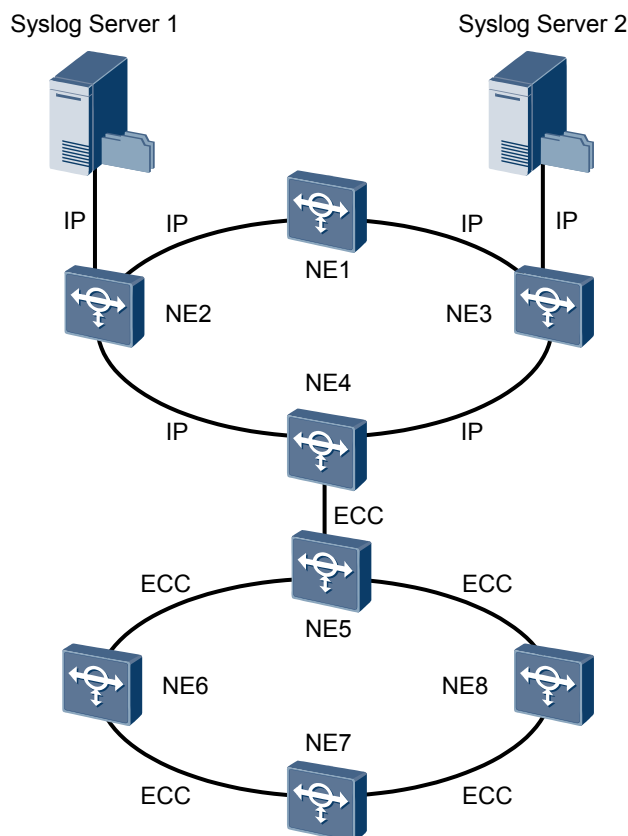
Networking Solution

For the security reasons, a transmission network must be connected to at least two syslog servers. The NEs and syslog servers usually communicate by IP protocol. Among the NEs, many protocols can be applied. For example, the NEs can communicate with each other through the ECC protocol.

Case 1:

Core NEs communicating with each other using the IP protocol, and Different syslog servers connected with different NEs. A typical type of network is shown in [Figure 7-2](#).

Figure 7-2 IP and ECC hybrid networking-1



NE1, NE2, NE3 and NE4 form an IP network. NE5, NE6, NE7 and NE8 form an ECC network. NE2 and NE3 communicate with Syslog Server 1 and Syslog Server 2 through the IP protocol separately. NE4 communicates with NE5 through the ECC channel.

In this situation, NE1, NE2, NE3 and NE4 can communicate with two different syslog servers through the IP protocol directly. So, you only need to set the IP address and port number of the syslog server for these NEs. The NE transmits the NE syslog to the syslog servers through the IP protocol. You need not set the syslog GNE.

NE5, NE6, NE7 and NE8 cannot communicate with syslog servers directly. Their syslog is transmitted to the syslog GNE through the ECC channel. Then, the syslog GNE transmits the syslog to the syslog servers. So, you only need to set the syslog GNE for these NEs. For example, NE2 may be the syslog GNE of NE5.

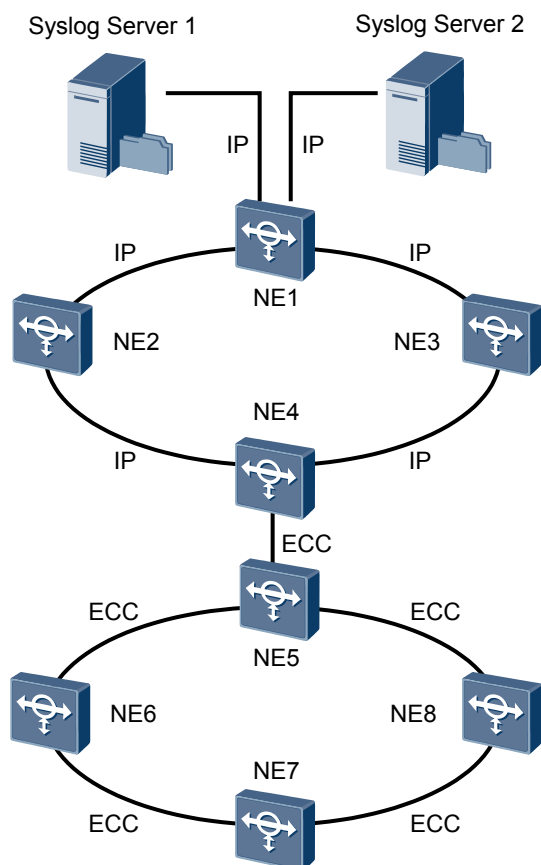
Table 7-1 Configuration List

NE	Syslog Server IP Address	Syslog GNE
NE1, NE2, NE3, NE4	129.1.0.1 129.2.0.1	None
NE5, NE6, NE7, NE8	None	NE2 NE3

Case 2:

Core NEs communicating with each other using the IP protocol, and Different syslog servers connected with the same NE. This type of network is similar to the one shown in [Figure 7-2](#). See [Figure 7-3](#).

Figure 7-3 IP and ECC hybrid networking-2

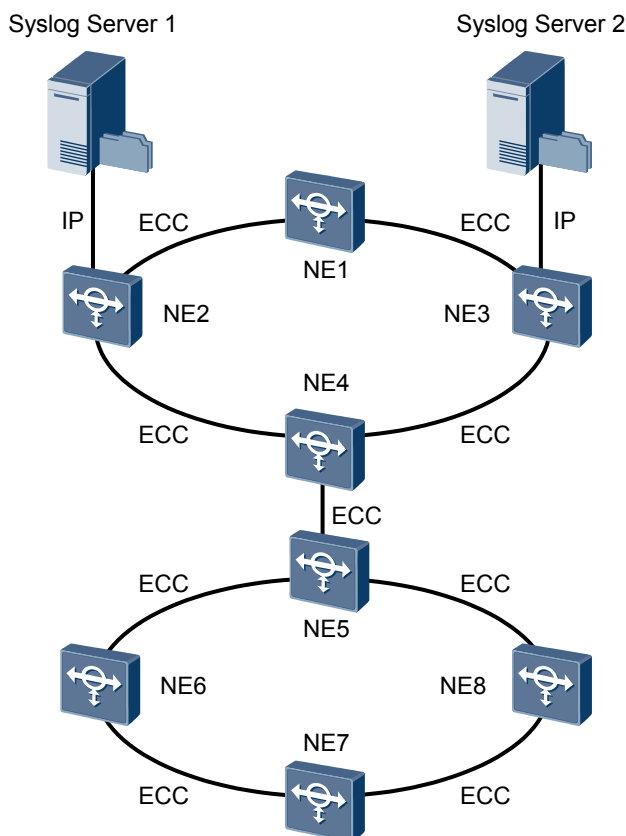


In this situation, NE1, NE2, NE3 and NE4 can also communicate with two different syslog servers through the IP protocol. So, all the NE settings are exactly the same as the settings in [Table 7-1](#).

Case 3:

Core NEs communicating with each other using the ECC protocol, and Different syslog servers connected with different NEs. A typical type of network is shown in [Figure 7-4](#).

Figure 7-4 ECC independent networking



NE1, NE2, NE3 and NE4 form an ECC network. NE5, NE6, NE7 and NE8 form another ECC network. NE2 and NE3 communicate with Syslog Server 1 and Syslog Server 2 separately through the IP protocol. NE4 communicates with NE5 through the ECC channel.

In this situation, NE2 can only communicate with Syslog Server 1 directly. NE2 cannot communicate with Syslog Server 2 directly. So, you need to set the IP address and port number of Syslog Server 1 for NE2. Then, you need set the Syslog GNE which can transmit the syslogs to Syslog Server 2. After that, NE2 can transmit the syslogs to Syslog Server 1 through the IP protocol and Syslog Server 2 through the Syslog GNE. The setting of NE3 is similar to the setting of NE2. You need to set the IP address and port number of Syslog Server 2, and then set the Syslog GNE which can transmit the syslogs to Syslog Server 1.

All other NEs cannot communicate with two syslog servers directly. Their syslog is transmitted to the syslog GNE through the ECC channel. Then, the syslog GNE transmits the syslog to the syslog servers. So, you only need to set the syslog GNE for these GNEs. For example, NE2 and NE3 may be the syslog GNEs of NE5. For details about the configurations, refer to [Table 7-2](#).

Table 7-2 Configuration List

NE	Syslog Server IP Address	Syslog GNE
NE1, NE4, NE5, NE6, NE7, NE8	None	NE2 NE3
NE2	129.1.0.1	NE3
NE3	129.2.0.1	NE2

7.10.2 Configuring the Syslog Server

In the case of NEs that can communicate with syslog servers directly, you need to configure the syslog server on the NEs. Then, the NEs can transmit the syslog to the syslog server.

Prerequisite

- You must be an NM user with "NE operator" authority or higher.
- The NE must be able to communicate with the syslog server directly.

Procedure

- 1 In the topology navigation tree or the topology view, select the NE to be operated and right-click it. Then select **NE Explorer** on the shortcut menu.
- 2 In the NE Explorer, select an NE and choose **Security > NE Log Forwarding** from the Function Tree.
- 3 Click the **Syslog Server** tab. The list of syslog servers is displayed.
- 4 Click **Query** to load the configuration data of the syslog server from the NE.
- 5 Click **New** and the **Add Syslog Server** dialog box is displayed.
- 6 Set the **IP Address**, **Send Mode** and **Port** based on the network settings.
- 7 Click **OK**. A prompt appears telling you that the operation was successful.

----End

7.10.3 Configuring the Syslog GNE

In the case of For the NEs that cannot communicate with the syslog server directly, you need to configure the syslog GNE. The syslog GNE transmits all the syslog that it receives d to the syslog server.

Prerequisite

You must be an NM user with "NE operator" authority or higher.

Procedure

- 1 In the topology navigation tree or the topology view, select the NE to be operated and right-click it. Then select **NE Explorer** on the shortcut menu.
- 2 In the NE Explorer, select an NE and choose **Security > NE Log Forwarding** from the Function Tree.
- 3 Click the **Syslog GNE** tab. The list of syslog GNEs is displayed.
- 4 Click **Query** to load the syslog GNE configuration from the NE.
- 5 Click **New** and the **Object Select** dialog box is displayed.
- 6 Choose proper NEs as the syslog GNEs.
- 7 Click **OK**. A prompt appears indicating the operation was successful.

----End

7.10.4 Configuring the Syslog Type and Severity

Different types of syslog have different severities. The NE report the relevant information based on the severity of the syslog.

Prerequisite

You must be an NM user with "NE operator" authority or higher.

Procedure

- 1 In the topology navigation tree or the topology view, select the NE to be operated and right-click it. Then select **NE Explorer** on the shortcut menu.
- 2 In the NE Explorer, select an NE and choose **Security > NE Log Forwarding**.
- 3 On the **Basic Info** tab, click **Query** to load the configuration data from the NE.
- 4 Click **New**. The **Add Basic Info** dialog box is displayed.
- 5 Choose proper **Log Type** and **Log Severity** based on the network requirements.
- 6 Click **OK**. A prompt appears indicating the operation was successful.

----End

7.10.5 Starting the Syslog Service

After the syslog service is started, the NE can transmit the syslog to syslog servers.

Prerequisite

You must be an NM user with "NE operator" authority or higher.

Procedure

- 1 In the topology navigation tree or the topology view, select the NE to be operated and right-click it. Then select **NE Explorer** on the shortcut menu.

- 2 In the NE Explorer, select an NE and choose **Security > NE Log Forwarding** from the Function Tree.
- 3 On the **Basic Info** tab, click **Query** to load the configuration data from the NE.
- 4 Check the **Start the log forwarding service** check box.
- 5 Click **Apply** to deploy the latest configuration data. A prompt appears indicating the operation was successful.

----End

8 Monitoring the U2000 Processes

About This Chapter

This topic describes how to manage the processes on the U2000 server through the system monitor client.

[8.1 Process Overview](#)

This topic describes the processes of the U2000.

[8.2 Logging In to the System Monitor Client](#)

The U2000 System Monitor Client uses the client/server model. To perform an operation, you need to log in to the server through the U2000 client.

[8.3 Setting the Monitoring Parameters](#)

You can set thresholds for the server monitoring, hard disk monitoring, database monitoring, and process monitoring. When the threshold is reached, the U2000 raises an alarm.

[8.4 Monitoring the Running Status of the U2000](#)

This topic describes how to monitor the status of the U2000 server. This facilitates you to view the statuses of the processes, databases, performance, and hard disks of the U2000 server in the centralized mode.

[8.5 Starting and Stopping a Process](#)

This topic describes how to start and stop a U2000 service process.

[8.6 Setting the Process Start Mode](#)

This topic describes the functions and setting methods of the three start modes of U2000 process: Automatic, Manual, and Disable.

8.1 Process Overview

This topic describes the processes of the U2000.

8.1.1 Start Mode

This topic describes the start mode of the U2000 processes.

8.1.2 U2000 Process List

This topic describes the information about U2000 processes, such as the functions and dependent processes of each process and the port occupied by each process.

8.1.1 Start Mode

This topic describes the start mode of the U2000 processes.

The U2000 processes can be started in the following modes:

- Automatic start:
In this mode, a process is automatically started when the system starts. If a process is abnormally stopped, the system automatically restarts the process.
- Manual start:
In this mode, a process needs to be manually started rather than being automatically started when the system starts. If a process is abnormally stopped, the system does not automatically restart the process.
- Disabled start:
In this mode, a process cannot be automatically started by the system or be manually started. A process in disabled start mode can be started only after the start mode is changed to the automatic start mode or manual start mode.

8.1.2 U2000 Process List

This topic describes the information about U2000 processes, such as the functions and dependent processes of each process and the port occupied by each process.

Table 8-1 shows the description of U2000 services and processes.

Table 8-1 U2000 process list

Process Name	Path	Port	Required Processes	Protocol Type	Function Description
EmfGnlDevDm	server/bin	None	None	None	General Device Process. General device service provides the function of managing the third-party NEs.
StdCltsiDm	server/nemgr/nemgr_access/bin	9002, 9003	BmsTest	TCP, TCP	112 Test. This process provides the 112 test.

Process Name	Path	Port	Required Process	Protocol Type	Function Description
LDAPAgent	server/common/ip/dmf/bin	None	sm_agent	None	LDAP Agent. This process provides the IP LDAP agent service.
snmpserver	server/common/ip/dmf/bin	None	None	None	SNMP Service(H3C). This process provides the SNMP forwarding function of H3C switches.
DmsBaseDm	server/common/ip/base/bin	None	sm_agent	None	IP Base Service. This process provides the basic IP services, such as link search, system log, interface inventory, and change audit.
DmsIPDm	server/common/ip/ipview/bin	None	sm_agent,eam_agent	None	IP View Manager. This process provides the IP view management service.
DmsBatchConfigDm	server/common/ip/batchconfig/bin	None	None	None	Batch Config. This process provides the function of configuring NEs in batches.
DmsNetAclDm	server/common/ip/netacl/bin	None	None	None	NetACL. This process provides the function of configuring the multi-NE ACL in batches.
QosPolicyDm	server/common/ip/qos/bin	None	None	None	Qos Manager. This process provides the QoS management function.
VasDiagDm	server/common/ip/vas/bin	None	sm_agent	None	Test and Diagnosis Manager. This process provides the test diagnosis function.
DeployDm	server/common/ip/deployment/bin	None	None	None	Deployment Manager. This process provides the deployment center function.

Process Name	Path	Port	Required Process	Protocol Type	Function Description
GctlDm	server/common/ip/gctl/bin	None	eam_agent	None	General Configuration Template. This process provides the general configuration template function.
gcli	server/common/ip/guicli/bin	13003, 13004	None	TCP, TCP	IP Graphic CLI. This process provides the switch and router GCL function.
nemgr_ptn	server/nemgr/nemgr_ptn/bin	11000~11100, 35600~35654	Eml_PubSvr	TCP, UDP	PTN NE Manager. This process provides the function of managing Metro Ethernet PTN frame-shaped and caseshaped NEs.
BoxSWMgrDm	server/nemgr/nemgr_switchmgr/switchmgr_box/bin	None	eam_agent	None	Switch NE Manager (Box). This process provides the function of managing Quidway case-shaped switches.
FrameSWMgrDm	server/nemgr/nemgr_switchmgr/switchmgr_frame/bin	None	eam_agent	None	Switch NE Manager (Frame). This process provides the function of managing Quidway frame-shaped switches.
itnotify	server/server/nbi/corba/bin	12002, 22002	None	TCP, TCP	CORBA Notify Service (Orbix). This process provides the CORBA NBI management service (Orbix).
Agent_CORBA	server/server/nbi/corba/bin	12003, 22003	None	TCP, TCP	CORBA Service. This process provides the CORBA NBI management service.
xmlagent	server/server/nbi/xml/bin	443, 9997	None	TCP, TCP	XML Service. This process provides the XML NBI management service.
RouterMgrDm	server/nemgr/nemgr_router/routermgr/bin	None	eam_agent	None	Router NE Manager. This process provides the function of managing Quidway routers.

Process Name	Path	Port	Required Process	Protocol Type	Function Description
SGMgrDm	server/nemgr/nemgr_router/sgmgr/bin	None	eam_agent	None	Service Gateway Manager. This process provides the function of managing Quidway service gateways.
SecurityMgrDm	server/nemgr/nemgr_securitymgr/bin	4999	eam_agent	UDP	Security NE Manager. This process provides the function of managing FW/USG, SIG, and SVN series security equipment.
secpolicymgr	server/vsm/secpolicymgr/bin	None	None	None	Policy Manager. This process provides the functions such as centralized policy configuration and attack defense configuration.
secvpnmgr	server/vsm/secvpnmgr/bin	None	None	None	VPN Manager. This process provides the IPSec/L2TP VPN management function.
Eml_WebLCTSVr	server/server/common/trans_core/bin	11000~11100	Eml_monitomeat	TCP	WEB LCT Service. This process provides the function of managing Web LCT NEs.
Nml_ason_otn	server/nml/ason_otn/bin	None	Eml_PubSvr	None	OTN ASON Network Manager. This process provides the OTN ASON network management function.
Nml_ason_sdh	server/nml/ason_sdh/bin	None	Eml_PubSvr	None	SDH ASON Network Manager. This process provides the SDH ASON network management function.
Eml_mm1	server/mml/bin	15000, 15001	None	TCP, TCP	MML Service. This process provides the MML NBI service.

Process Name	Path	Port	Required Process	Protocol Type	Function Description
nemgr_ext	server/nemgr/nemgr_ext/bin	11000~11100, 35600~35654	Eml_PubSvr	TCP, UDP	EXT NE Manager. This process provides the function of managing the OSN900A and OTU40000.
nemgr_marine	server/nemgr/nemgr_marine/bin	11000~11100, 35600~35654	Eml_PubSvr	TCP, UDP	MARINE NE Manager. This process provides the function of managing submarine cable series equipment.
nemgr_naotn	server/nemgr/nemgr_naotn/bin	11000~11100, 35600~35654	Eml_PubSvr	TCP, UDP	OTN(TL1). This process provides the function of managing North America OTN series equipment.
nemgr_nawdm	server/nemgr/nemgr_nawdm/bin	11000~11100, 35600~35654	Eml_PubSvr	TCP, UDP	WDM(TL1). This process provides the function of managing North America WDM series equipment.
nemgr_otn	server/nemgr/nemgr_otn/bin	35600~35654	Eml_PubSvr	UDP	OTN NE Manager. This process provides the function of managing OTN series equipment.
nemgr_rtn	server/nemgr/nemgr_rtn/bin	11000~11100, 35600~35654	Eml_PubSvr	TCP, UDP	RTN NE Manager. This process provides the function of managing RTN series equipment.
nemgr_sdh	server/nemgr/nemgr_sdh/bin	11000~11100, 35600~35654	Eml_PubSvr	TCP, UDP	SDH NE Manager. This process provides the function of managing SDH/MSTP/OSN series equipment.

Process Name	Path	Port	Required Process	Protocol Type	Function Description
nemgr_wdm	server/nemgr/nemgr_wdm/bin	11000~11100, 35600~35654	Eml_PubSvr	TCP, UDP	WDM NE Manager. This process provides the function of managing LHWDM/Metro WDM series equipment.
Eml_PubSvr	server/common/trans_core/bin	1500	lic_agent,mc	UDP	Transmit Common Service. This process provides the function of inter-NE management on transferdomain NEs and reports.
Eml_PerfSvr	server/common/trans_core/bin	None	Eml_PubSvr	None	Transmit Performance Service. This process provides the transfer-domain performance management function.
profile	server/common/frame/profile/bin	None	None	None	Global Profile Manager. This process provides the profile management function.
itm_agent	server/bin	31015, 31065	None	TCP, TCP	Integrated Task Management. Provides the functions of integrated task management.
lic_agent	server/bin	31001, 31051	None	TCP, TCP	License Process. A service interface is provided to check the validity of the license file of the current version
imap_sysmonitor	server/bin	None	None	None	System Monitor. Provides service to monitor the process of the system

Process Name	Path	Port	Required Process	Protocol Type	Function Description
log_agent	server/bin	31005 , 31055 , 31006	None	TCP, TCP, TCP	Log/Syslog/Access Device Log Process. This process provide the functions as follow: 1. Records the system logs. It receives, manages, and stores the system logs of other processes through a port 2. Syslog forwarding service is used to forward the iMAP logs to the third-party Syslog Server based through the BSD Syslog protocol 3. Provides the management of access NES device log
sm_agent	server/bin	31008 , 31058	lic_agent	TCP, TCP	Security Process. Provides the functions of managing network management system (NMS) users, NMS user rights, and NE user rights.
tm_agent	server/bin	31010 , 31060	None	TCP, TCP	Topo Process. Provides the functions of integrated task management.
ifms_agent	server/bin	31011 , 31061	None	TCP, TCP	Fault Process. Collects and saves the alarm information from the managed devices through the NE engine. It also provides the function of querying and analyzing the alarm information.
snmp_agent	server/bin	982, 9812	None	TCP, UDP	SNMP Service. Provides the northbound interface which adopts the SNMP protocol.

Process Name	Path	Port	Required Process	Protocol Type	Function Description
manager_agent	server/bin	31013 , 31063	None	TCP, TCP	System Service. Provides the management interface for network management system (NMS) version information, including querying the version information of the operating system, checking the software version of the client, querying the software version of the server and client, and querying the upgrade information of the client.
porttrunk_agent	server/bin	31035	None	TCP	Port Trunk Service . The port trunking service is used to have the ports of independent services converge at one port.
CAU	server/bin	8250	None	TCP	Client Auto Upgrade Service. Provides Client Auto Upgrade Service
ds_agent	server/bin	31037 , 31038 , 31039 , 31040 , 31041 ~31050	None	TCP, TCP, TCP, TCP, TCP	Desktop Service Process. The DS provides data presentation and operation services on various types of client interfaces, such as Java GUI and Web. If multiple DSs are deployed, they reduce the pressure of the server for connecting to a large number of clients.
eam_agent	server/bin	31036 , 31099	None	TCP, TCP	EAM Process. EAM Maintains a global NE list in network management.

Process Name	Path	Port	Required Process	Protocol Type	Function Description
JMSServer	server/bin	8161, 61616, 61617	None	TCP, TCP, TCP	JMS Service (ActiveMQ). The Thrift Software, JMS(Java Message Service)
bmsmoni apache	server/nemgr/ nemgr_access/bin	None	None	None	Access Apache Service. This process provides the function of monitoring the Apache service status.
BmsHG MPDm	server/nemgr/ nemgr_access/bin	None	None	None	HGMP Manager Process. HGMP manager service provides the function of managing HGMP
EmfTrap Receiver	server/bin	162, 11101 ~11104	None	UDP, TCP	Trap Receiver Process. This Trap Receiver receives the Trap messages sent to the server through SNMP.
EmfProj DocDm	server/bin	None	None	None	Project Document Process. Provide the function of exporting the project data of the network management system.
Notify_S ervice	server/bin	12002 , 22002	None	TCP, TCP	CORBA Notification Service(TAO). CORBA notification service
Naming_ Service	server/bin	12001 , 22001	None	TCP, TCP	CORBA Naming Service(TAO). CORBA naming service
HedExSe rvice	server/bin	None	None	None	Help Process. Provides help document.
BmsAtur	server/nemgr/ nemgr_access/bin	None	ifms_a gent,m c	None	Access Device ATUR Manager. This process provides the xDSL terminal management service.

Process Name	Path	Port	Required Process	Protocol Type	Function Description
BmsCommon	server/nemgr/nemgr_access/bin	None	ifms_agent,mc	None	Access Device Common Service. This process provides license, task scheduling, etc. management of the access domain.
BmsGdm	server/nemgr/nemgr_access/bin	None	ifms_agent,mc	None	Access Device Manager. This process provides the equipment management of the access domain.
BmsProfile	server/nemgr/nemgr_access/bin	None	mc	None	Access Device Profile Manager. This process provides the profile service management of the access domain.
BmsPvc	server/nemgr/nemgr_access/bin	None	ifms_agent,mc	None	Access Device PVC Service Manager. This process provides the PVC, ServicePort service management of the access domain.
BmsRack	server/nemgr/nemgr_access/bin	None	mc	None	Access Device Rack Manager. This process provides rack management of the access domain.
BmsService	server/nemgr/nemgr_access/bin	None	ifms_agent,mc	None	Access Device Generated Service Manager. This process provides IGMP, VLAN, Voice, Ethernet port, Protocol, etc. management of the access domain.
BmsTest	server/nemgr/nemgr_access/bin	None	ifms_agent,mc	None	Access Device Line Test. This process provides line test of the access domain.
BmsTimingTask	server/nemgr/nemgr_access/bin	None	mc	None	TL1 Timing Task Manager. This process provides TL1 timing task management.

Process Name	Path	Port	Required Process	Protocol Type	Function Description
bmsXdsl	server/nemgr/nemgr_access/bin	None	ifms_agent,mc	None	Access Device xDSL Service Manager. This process provides the xDSL service management service.
BmsXpon	server/nemgr/nemgr_access/bin	None	ifms_agent,mc	None	Access Device xPON Service Manager. This process provides the xPON service management service.
cltsi	server/nemgr/nemgr_access/bin	9000	BmsTest	TCP	112 Test(CLTSi). This process provides the CLTSi 112 test.
inTL1NBiDm	server/nemgr/nemgr_access/bin	9820	mc	TCP	TL1 Proxy Inner Interface. This process provides the XML NBI Proxy,Service Provisioning Profile management.
TL1NBiDm	server/nemgr/nemgr_access/bin	9819	lic_agent,mc	TCP	TL1NBiDm Process. This process provides TL1 NBI Management service.
CFMSiDm	server/nemgr/nemgr_access/bin	8001, 9001	None	TCP, TCP	Customer Feature Management NBI. This process provides Customer Feature Management NBI service.
DSLMgrDm	server/nemgr/nemgr_access/bin	None	mc	None	Port Conformity Statistics. This process provides port conformity statistics of the access domain.
lte_agent	server/bin	31033, 31083	lic_agent	TCP, TCP	Common License Process. A service interface is provided to manager the ne license.
BmsPonEmsTL1	server/nemgr/nemgr_access/bin	13027	mc	TCP	Access PON TL1 Process. This process provides PON TL1 Management service.

Process Name	Path	Port	Required Process	Protocol Type	Function Description
U2560WLANDm	server/nemgr/nemgr_cnm/bin	None	None	None	WLAN Equipment Management Service. This process provides WLAN device management of customer network devices.
U2560TR069Dm	server/nemgr/nemgr_cnm/bin	13029 , 13030 , 13033	None	TCP, TCP, TCP	TR069 Terminals Management Service. This process provides TR069 terminals management of customer network devices.
U2560CommonDm	server/nemgr/nemgr_cnm/bin	None	None	None	Customer Network Device Common Service. This process provides license, poll manage, etc. management of customer network.
trapdispatcher	server/common/trapdispatcher/bin	162, 162	ifms_agent	UDP, UDP	Trap Dispatcher. Provide trap receiving and dispatching function
EmfTrapReceiver1	server/bin	None	None	None	Extended Trap Receiver. Receive the trap reported from network elements, as the extension of default Trap Receiver, SNMP interface device used.
datacollectorsvr	server/tools/datacollector/bin	None	None	None	Data Collector Process. The Datacollector is mainly used for collecting the complete and correct fault data in case of NE failure and helps to locate faults quickly
neproxy	server/tools/datacollector/bin	None	None	None	DataCollector Neproxy Process. DataCollector Neproxy Process

Process Name	Path	Port	Required Process	Protocol Type	Function Description
PnpMgr DM	server/common/pnpmgr/dhcp/bin	67, 68	None	UDP, UDP	Automatic NE Configuration. This process provides router automatic NE configuration function
Diagnose Controller	server/common/ipda/controller/bin	None	None	None	Fault Diagnose Controller Process. Provide fault diagnose function of Access network and PTN network
DCServer	server/common/dc/bin	22, 22, 69, 21	None	TCP, TCP, TCP, TCP	DC. This process provides the function of NE software management and disaster recovery management. The detailed functions are NE software upgrade, patch installation, data backup and recovery for disaster recovery, and plug-andplay automatic upgrade of case-shaped equipment.
toolkit	server/common/dc/toolkit/server	8999, 13006	None	TCP, TCP	Toolkit. This process provides the service of upgrading boardlevel transmission equipment.
Enpower Dm	server/common/env/bin	None	itm_agent	None	Access environment and power monitor. This process provides the function of centralized monitoring on the access NE environment status and the power supply status.
PMDDataSynchronizer	server/common/pms/bin	None	None	None	Remote Data Synchronizer. This process provides the function of importing data in text files.

Process Name	Path	Port	Required Process	Protocol Type	Function Description
PMSDm	server/common/pms/bin	None	None	None	Performance Service. This process provides the collector management function.
PQMDm	server/common/pms/bin	None	Eml_monitomeat	None	Group Monitor. This process provides the function of grouping performance monitoring and display.
TXTNBIDm	server/common/pms/bin	None	None	None	Text Export. This process provides the NBI function. It is used to transmit performance data in the text format through FTP.
BulkCollectorDm	server/common/pmscollector/bin	21	None	TCP	Bulk Collector. This process provides the function of collecting performance data in batches.
SNMPCollectorDm	server/common/pmscollector/bin	None	None	None	SNMP Collector. This process provides the function of collecting performance data through SNMP.
XftpDm	server/common/xftp/bin	None	None	None	XFTP. This process provides the function of setting XFTP connection parameters.
SyslogCollectorDM	server/common/devicelog/bin	514	None	UDP	System Log Collector. This process provides the function of collecting NE operation and running log data, and managing files.
inventorydm	server/common/inventory/bin	None	None	None	Inventory Manager. This process provides the inventory data management function, such as physical resource management, cable management, and customer management.

Process Name	Path	Port	Required Process	Protocol Type	Function Description
NmslogzipDm	server/common/unitedmgr/bin	None	None	None	Zip Server. This process provides the function of compressing NMS files.
UniteUtilDM	server/common/unitedmgr/bin	13005	None	UDP	United Manager. This process provides the basic functions, such as importing and exporting scripts, managing NE time, synchronizing NEs, and managing NE objects, of the inter-domain universal NMS.
Nml_common	server/nml/nmlcommon/bin	None	None	None	Network Common Service. This process provides the E2E common management service. The other E2E processes all depend on this process.
Nml_cps	server/nml/nmlcps/bin	None	None	None	Composite Service Manager. This process provides the composite service management function.
Nml_eth	server/nml/nmlcth/bin	None	Nml_common	None	MSTP ETH and ATM. This process provides the MSTP ETH/ATM E2E management service.
Nml_ip	server/nml/nmlip/bin	None	None	None	IP Service Manager. This process provides the IP E2E management service.
Nml_otn	server/nml/nmlotn/bin	None	Nml_common	None	OTN Network Manager. This process provides the OTN E2E management service.
Nml_sdh	server/nml/nmlsdh/bin	None	Nml_common	None	SDH Network Manager. This process refers to the Web service process. It provides Web services.

Process Name	Path	Port	Required Process	Protocol Type	Function Description
Nemgr_vmf	server/nemgr/nemgr_vmf/bin	13001, 9801, 8099	None	TCP, TCP, TCP	Router NE Manager (VRP V8). This process provides the function of managing V8 routers equipment.
Eml_monitorcat	common/Tomcat/bin	None	None	None	Tomcat Service. This process provides the function of monitoring the Tomcat service status.
mc	server/common/frame/mc/bin	None	None	None	Distribution Manager. This process provides the basic NE distribution service.
dam	server/common/frame/dam/bin	None	None	None	Device Access Manager. This process provides the function of creating SNMP equipment.

8.2 Logging In to the System Monitor Client

The U2000 System Monitor Client uses the client/server model. To perform an operation, you need to log in to the server through the U2000 client.

Prerequisite

Before login, ensure that the U2000 client and server are connected normally, and the server works correctly.

Context

- The default port number of the server is **31030**. Do not change it in normal conditions. Otherwise, you cannot log in to the U2000 server.
- The login mode is classified into the SSL mode and the common mode. In SSL mode, the data is encrypted when being transmitted between the client and the server. In common mode, the data is not encrypted during transmission.
- The port used for login in common mode is different from that in SSL mode. The port is 31030 in common mode, and 31080 in security (SSL) mode.
- If you do not log in during the preset period after the previous login, the U2000 disables or delete the user account.
- If you never use a new user account for login, the account is not restricted to these rules, that is, the U2000 does not set it to be invalid or delete it.

Procedure

1 Double-click the related shortcut icon on the desktop to start the system monitor client.

2 In the **Login** dialog box, select a server from the **Server** drop box.

 NOTE

If there is no server to select, do as the followings:

1. Click  on the right of **Server** drop box.
2. In the **Server List** dialog box, click **Add**.
3. In the **Add Server Information** dialog box, specify **Name** and **Server Name(or IP Address)**, and then select a login mode. Click **OK**.
4. In the **Server List** dialog box, click **OK**.

3 In the **Login** dialog box, enter the user name and password.

The user name and password are the same as those for the U2000 client.

4 Click **Login**.

 NOTE

- If the user name and the password are correct, the **Loading** dialog box is displayed, indicating the loading progress.
- If the user name or password is wrong, the **Information** dialog box prompts cannot login.
- If the password is to expire in the specified days, the system prompts you to change the password before the expiration date.
- If the license is to expire in the specified days, the system notifies you of the expiration date.
- If you use a temporary license, you are prompted to apply for an official license.

----End

8.3 Setting the Monitoring Parameters

You can set thresholds for the server monitoring, hard disk monitoring, database monitoring, and process monitoring. When the threshold is reached, the U2000 raises an alarm.

[8.3.1 Setting the Parameters for the U2000 Server Monitoring](#)

You can set the server monitoring parameters to monitor the performance (CPU usage and memory usage) of the U2000 server. When the CPU usage or memory usage reaches the specified threshold, alarms are generated. You can also set whether to display pop-up messages on the client. From pop-up messages, you can understand server performance exceptions in time.

[8.3.2 Setting the Parameters for the U2000 Server Hard Disk Monitoring](#)

You can set the hard disk monitoring parameters to monitor the usage of the hard disk on the U2000 server. When the hard usage of the hard disk on the U2000 server reaches the threshold, a high hard disk usage alarm occurs. You can also set whether to display pop-up messages on the client. From pop-up messages, you can understand hard disk exceptions in time.

[8.3.3 Setting the Parameters for the U2000 Server Database Monitoring](#)

You can set the database monitoring parameters to monitor the U2000 database usage. When the U2000 server database usage reaches the threshold for alarm generation, an alarm is generated.

[8.3.4 Setting the Parameters for the U2000 Server Process Monitoring](#)

You can set the parameters for the process monitoring to refresh period of the system resources monitoring.

8.3.1 Setting the Parameters for the U2000 Server Monitoring

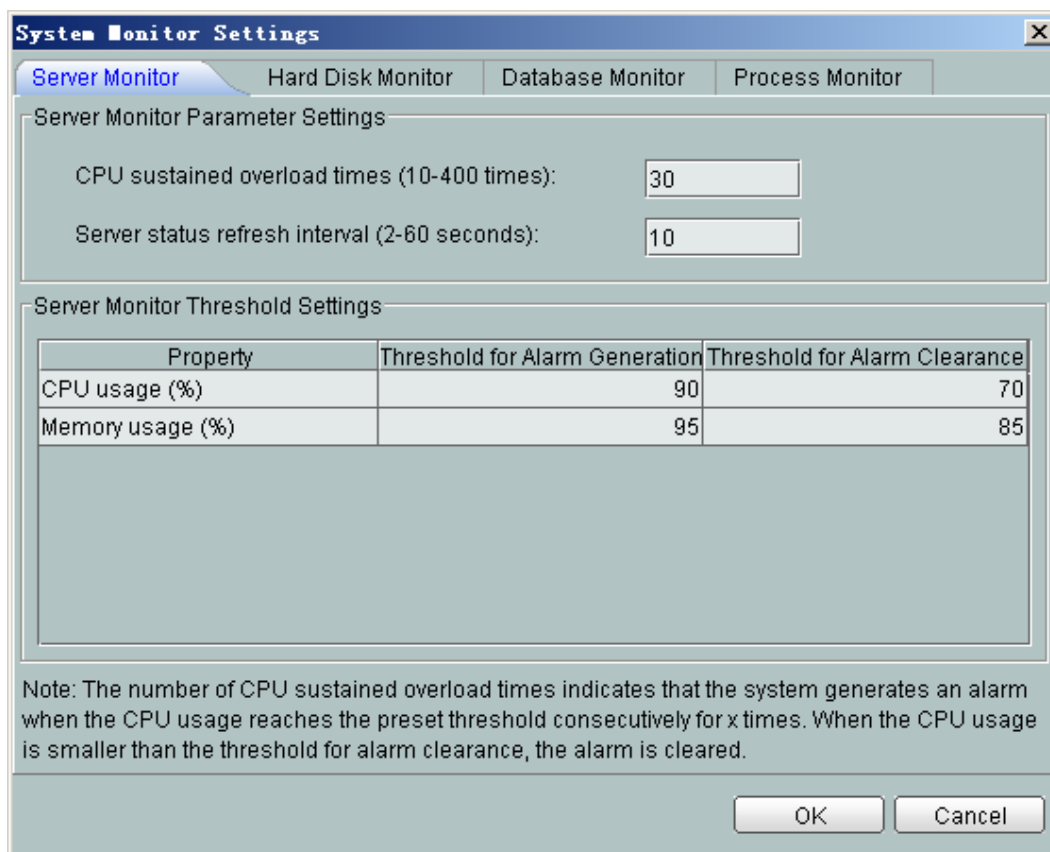
You can set the server monitoring parameters to monitor the performance (CPU usage and memory usage) of the U2000 server. When the CPU usage or memory usage reaches the specified threshold, alarms are generated. You can also set whether to display pop-up messages on the client. From pop-up messages, you can understand server performance exceptions in time.

Context

- The number of consecutive sampling times is equal to **CPU sustained overload times**. The sampling interval is equal to **Server status refresh interval**. If the CPU usage sampled each time is larger than the generation threshold, it means that the CPU is consecutively overloaded. When the number of overload times reaches the specified value, a high CPU usage alarm is generated. If the CPU usage sampled at a time is smaller than the clearance threshold, the high CPU usage alarm is cleared.
- When the memory usage is larger than the threshold for alarm generation, a high memory usage alarm is generated. When the memory usage is smaller than the threshold for alarm clearance, the high memory usage alarm is cleared.
- When the condition for generating a performance alarm is met, the corresponding icon on the **Server Monitor** tab turns red. If you enable the function of displaying pop-up messages, you can receive notifications of performance exceptions on the status bar on the client.

Procedure

- 1 [Log in to the system monitor client](#).
- 2 Choose **Administration > Settings** from the main menu.
- 3 In the **System Monitor Settings** dialog box, click the **Server Monitor** tab.



4 Set the property values in the **Server Monitor** tab.

5 Click **OK**.

----End

8.3.2 Setting the Parameters for the U2000 Server Hard Disk Monitoring

You can set the hard disk monitoring parameters to monitor the usage of the hard disk on the U2000 server. When the hard usage of the hard disk on the U2000 server reaches the threshold, a high hard disk usage alarm occurs. You can also set whether to display pop-up messages on the client. From pop-up messages, you can understand hard disk exceptions in time.

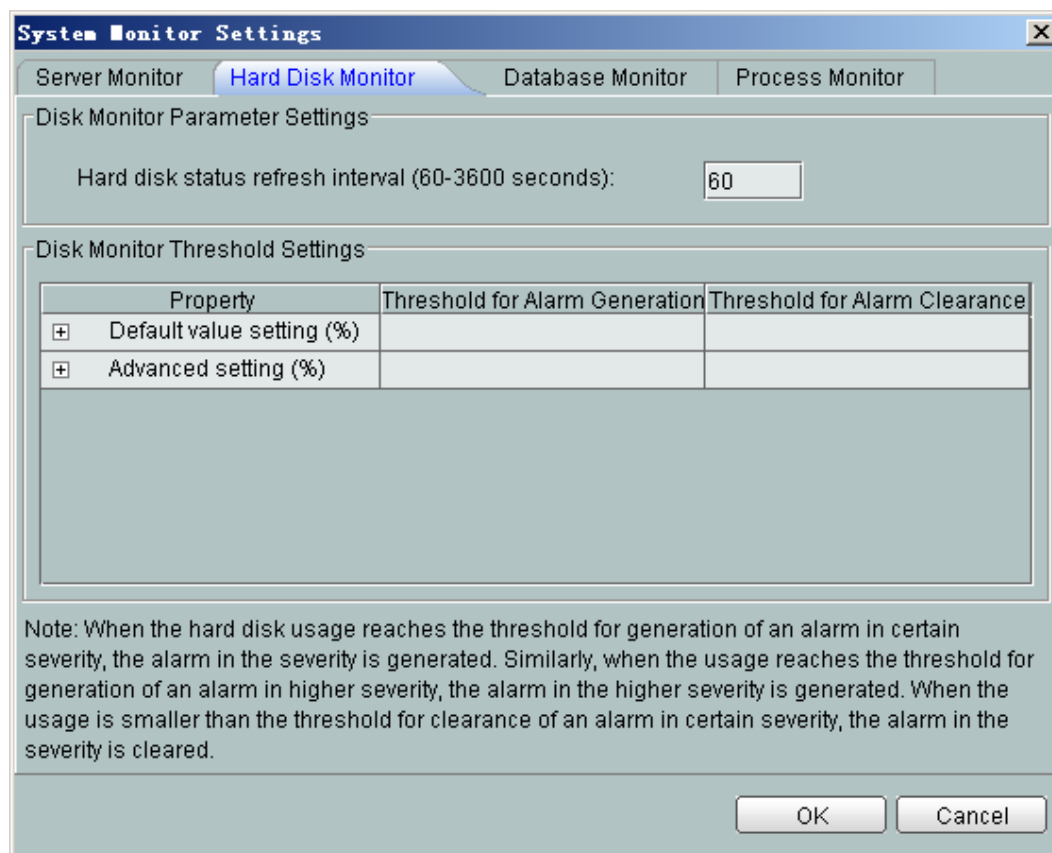
Context

- When the usage of the hard disk on the U2000 server reaches the threshold for alarm generation, a high hard disk usage alarm occurs. When the hard disk usage is smaller than the threshold for alarm clearance, the high hard disk usage alarm is cleared.
- When the condition for generating a high hard disk usage alarm is met, the corresponding icon on the **Hard Disk Monitor** tab turns red. If you enable the function of displaying pop-up messages, you can receive notifications of hard disk exceptions on the status bar on the client.

Procedure

- 1 **Logging In to the System Monitor Client.**

- 2 Choose **Administration > Settings** from the main menu.
- 3 In the **System Monitor Settings** dialog box, click the **Hard Disk Monitor** tab.



NOTE

The threshold for generating an alarm of lower severity is smaller than that for clearing an alarm of higher severity.

- 4 Set the property values in the **Hard Disk Monitor** tab.
- 5 Click **OK**.

----End

8.3.3 Setting the Parameters for the U2000 Server Database Monitoring

You can set the database monitoring parameters to monitor the U2000 database usage. When the U2000 server database usage reaches the threshold for alarm generation, an alarm is generated.

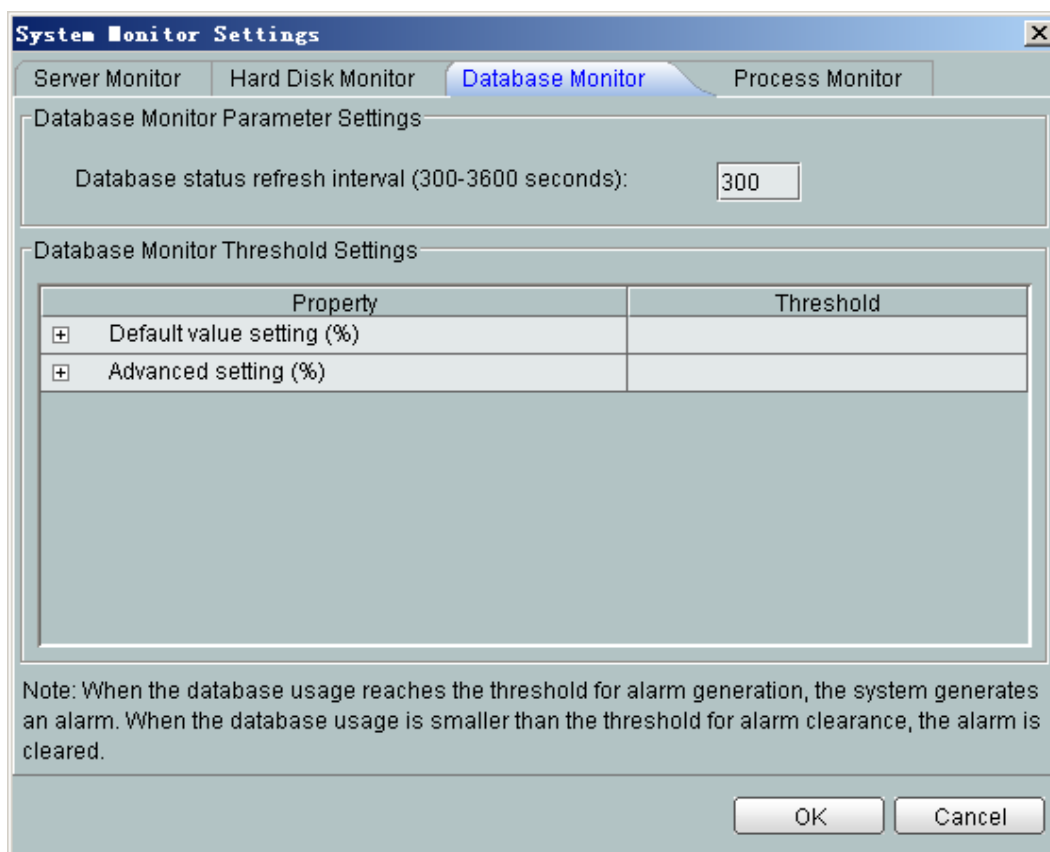
Context

- When the U2000 server database usage reaches the threshold, the U2000 raises an alarm. When the usage is smaller than the threshold, the corresponding clearance alarm is generated.

- When the condition for generating a high database usage alarm is met, the state icon on the **Database Monitor** tab turns red.

Procedure

- 1 [Log in to the system monitor client.](#)
- 2 Choose **Administration > Settings** from the main menu.
- 3 In the **System Monitor Settings** dialog box, click the **Database Monitor** tab to set the property values.



- 4 Set the property values in the **Database Monitor** tab.
- 5 Click **OK**.

----End

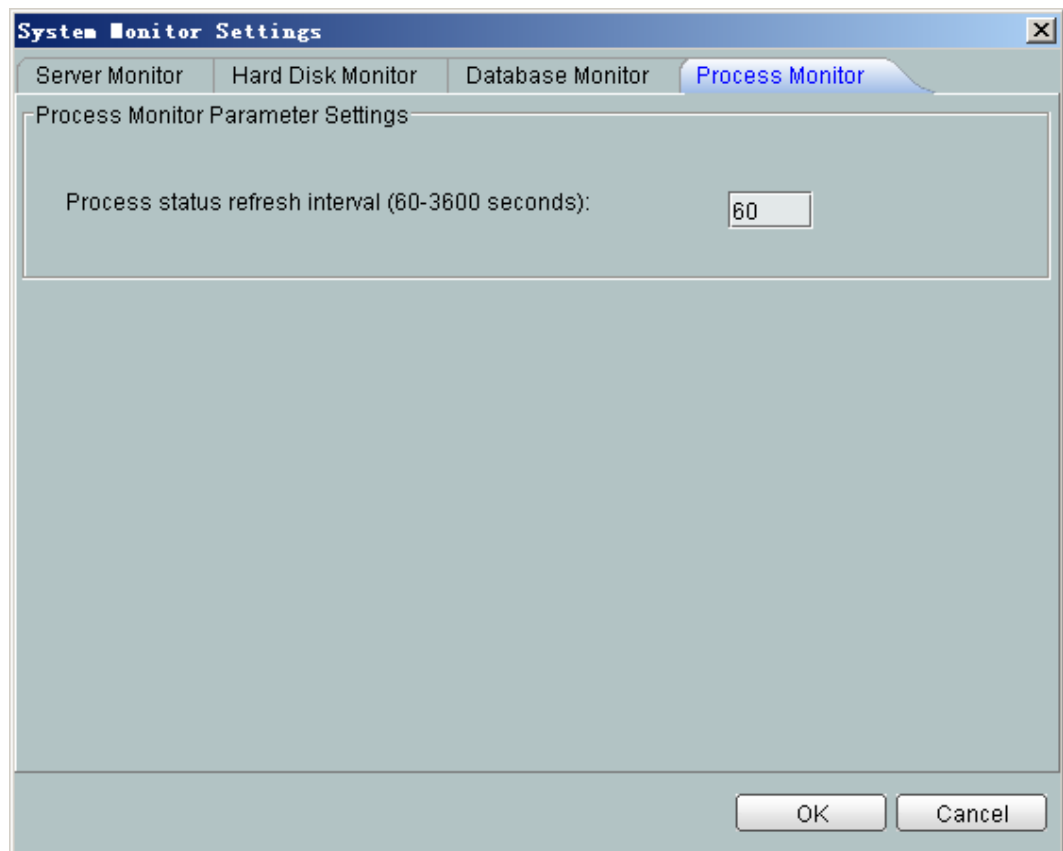
8.3.4 Setting the Parameters for the U2000 Server Process Monitoring

You can set the parameters for the process monitoring to refresh period of the system resources monitoring.

Procedure

- 1 [Log in to the system monitor client.](#)

- 2 Choose **Administration > Settings** from the main menu.
- 3 In the **System Monitor Settings** dialog box, click the **Process Monitor** tab.



- 4 On the **Process Monitor** tab, set **Process status refresh interval**.
- 5 Click **OK**.

----End

8.4 Monitoring the Running Status of the U2000

This topic describes how to monitor the status of the U2000 server. This facilitates you to view the statuses of the processes, databases, performance, and hard disks of the U2000 server in the centralized mode.

Monitoring the Process Status

You can monitor the process status of the U2000 server to easily view information about the processes in the centralized mode. You can start or stop a process and set the startup mode of a process.

To monitor the process status, proceed as follows:

- 1 Log in to the System Monitor.
- 2 Click the **Process Monitor** tab to list the details of all the processes that can be monitored.
- 3 Select one or more processes, right-click, and choose the relevant menus for relevant operations. The specific menus and their functions are described as follows:

 NOTE

Note that you can view the details of only one process each time.

- **Refresh:** It is used to refresh the information about the selected processes.
- **Start the Process:** It is used to start the selected processes that are not started.
- **Stop the Process:** It is used to stop the selected processes.
- **Startup Mode:** It is used to set the required startup modes for the selected processes, including **Automatic**, **Manual**, and **Disabled**.
- **Details:** It is used to view the details of the processes.

Monitoring the Disk Status

You can monitor the disk status to easily obtain the usage rate and remaining space of the disk.

When the hard disk usage of the server exceeds the preset alarm threshold, the system monitor server sends the relevant alarm to the server. In addition, the record on the System Monitor turns red.

To monitor the disk status, proceed as follows:

1. Click the **Hard Disk Monitor** tab to list the hard disk information about the server.
2. Select one or more records, right-click, and choose **Refresh** to refresh the selected hard disk information.

Monitoring the Database Status

You can monitor the database status to obtain the data space, log space, and backup of the server in the centralized mode.

When the database usage exceeds the preset alarm threshold, the U2000 generates an alarm. In addition, the record on the System Monitor turns red.

To monitor the database status, proceed as follows:

1. Click the **Database Monitor** tab to list the details of all the databases that can be managed.
2. Select one databases, right-click, and choose the relevant menus for relevant operations, as shown in the following:

Refresh: It is used to refresh the information about the selected databases.

Monitoring the Resource Status

You can monitor the resource status to easily obtain the CPU occupancy, physical memory, used memory, and free memory of the server.

To monitor the resource status, proceed as follows:

1. Click the **Server Monitor** tab to list the information about the OS that runs on the server.
2. Select one or more records, right-click, and choose **Refresh** to refresh the information about the selected system resources.

Monitoring the U2000 Component Status

You can monitor the component status to easily obtain the name and version of the components.

To monitor the components status, proceed as follows:

1. Click the **Component Information** tab to list the U2000 components information.
2. Select one or more records, right-click, and choose **Refresh** to refresh the selected components information.

Monitoring the Log Status

You can monitor the log status to easily obtain the operation time, client, and result.

To monitor the log status, proceed as follows:

1. Click the **Operation Logs** tab to list the details of all the logs.
2. Select one or more logs, right-click, and choose the relevant menus for relevant operations, as shown in the following:
 - **Refresh**: It is used to refresh the information about the selected logs.
 - **Details**: It is used to view the details of the logs.

8.5 Starting and Stopping a Process

This topic describes how to start and stop a U2000 service process.

Prerequisite

Other processes that depend on the process to be stopped must be stopped.

Context

- When **Start Mode** is set to **Disabled**, the processes cannot automatically start.
- When the system starts, the processes in automatic start mode start automatically.
- Stopping a process affects the functions of the U2000. Therefore, perform this operation with caution.
- The system does not automatically start the manually stopped process.

Procedure

- 1 On the System Monitor, click the **Process Monitor** tab.
- 2 Select a process, right-click, and choose **Start Process** or **Stop Process**.

----End

8.6 Setting the Process Start Mode

This topic describes the functions and setting methods of the three start modes of U2000 process: Automatic, Manual, and Disable.

Context

- **Automatic**: When a process stops in the case of a fault, the U2000 automatically attempts to start the process.

- Manual: On the client, if the start mode of the process selected in the service monitoring list is Manual, it indicates that you can manually change the start mode of the process.
- Disable: You can manually set the start mode of a stopped process to Disable.

Procedure

- 1 [Log in to the system monitor client.](#)
- 2 In the main window, click the **Process Monitor** tab.
- 3 On the **Process Monitor** tab, right-click a process record to choose a submenu of **Start Mode**.



NOTE

You can select the **Disable** mode for only the stopped service.

----End

9 Common Veritas Operations

About This Chapter

This topic describes how to use the Veritas Cluster Server (VCS) tool, Veritas Enterprise Administrator (VEA) tool, and Veritas commands to view the server status, perform the switchover, and manage and maintain objects such as resource groups, resources, and replication volumes.

[9.1 Switchover Principle of the Two-Site Cluster](#)

This topic describes the switchover principle of the U2000 HA system (Veritas hot standby).

[9.2 Managing the Login of VCS Users](#)

VCS users manage the local clusters by logging in to the VCS client through which the centralized management for all the local hardware and software resources is realized. The software of the VCS also provides basic data ports to global cluster option (GCO) and monitors the system and the application services in real time. When the hardware or software is faulty, the VCS restarts or shuts down the application service.

[9.3 Managing Resource Groups](#)

This topic describes how to manage resource groups using the Cluster Explorer and commands.

[9.4 Managing Resources](#)

This topic describes how to manage resources in resource groups using the Cluster Explorer and commands.

[9.5 Managing Replication Volumes](#)

This topic describes how to manage replication volumes using the Cluster Explorer and commands.

[9.6 Switching Over the Active Site and the Standby Site](#)

This topic describes how to switch over the active site and the standby site.

[9.7 Monitoring Active and Standby Sites](#)

This topic describes how to monitor the status of active and standby sites by using the VCS or the commands.

9.1 Switchover Principle of the Two-Site Cluster

This topic describes the switchover principle of the U2000 HA system (Veritas hot standby).

During running, the HA system (Veritas hot standby) may have four different status. Refer to [Table 9-1](#).

Table 9-1 HA system status

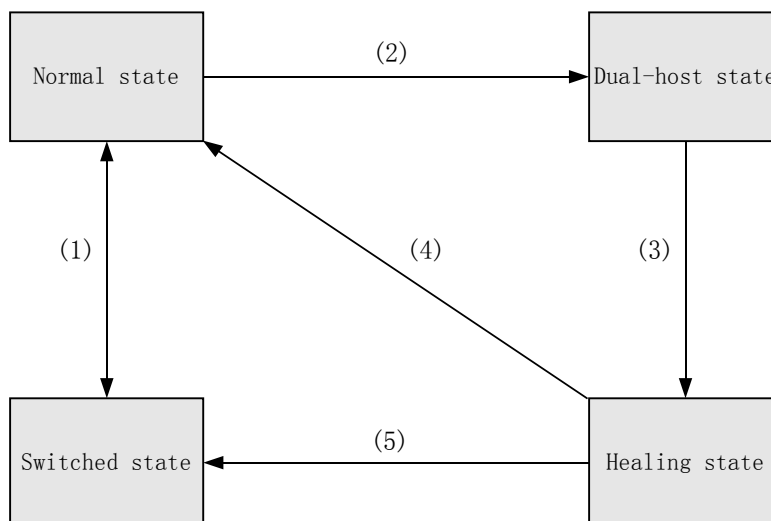
System Status	U2000 Running Condition	Data Replication Direction	Remarks
Normal state	Run on the primary site only	From the primary site to the secondary site	This is a normal HA system status.
Switched state	Run on the secondary site only	From the secondary site to the primary site	This is also a normal HA system status. The difference from the Normal state is that the active/standby switchover occurs and the data replication direction is reversed.
Dual-host state	Run on the primary and secondary sites	No data replication	This status usually occurs when the communication between the primary and secondary sites is interrupted. The two sites may force each other to log out of an NE. In this case, you need to handle the problem.
Healing state	Run on the secondary site only. The disk of the primary site is not writable	No data replication	No data is replicated. This is a status of managing the network on a single system. It is converted from the Dual-host state after the communication between the primary and secondary sites is recovered. In this case, you need to handle the problem.

 NOTE

Normally, when the system is in the **Normal state**, the primary site is the active site and the secondary site is the standby site. That is, the U2000 runs on the primary site.

[Figure 9-1](#) shows the conversion relations between the four statuses.

Figure 9-1 shows the conversion relations between the four status.



- Conversion (1): To convert between the **Normal state** and **Switched state**, use the Veritas software to automatically complete the operation or perform manual switching.
 - When the U2000 server program on the active site becomes faulty, the Veritas software automatically starts the U2000 server program on the standby site and the system changes to the **Switched state**.
 - When you need to maintain a certain site or temporarily restart the site, you can manually switch the active site to another site.

After switching, the active/standby switchover occurs and the data replication direction is reversed.

- Conversion (2): When the time of disconnection between the active and standby sites exceeds the preset threshold (the default value is 600 seconds), the Veritas software automatically performs forced handover and starts the U2000 server program on the standby server. The system changes to the **Dual-host state**.
- Conversion (3): After the communication between the primary and secondary sites becomes normal, the system automatically changes from the **Dual-host state** to the **Healing state**.
- Conversion (4): After the communication between the primary and secondary sites is recovered, if the data on the primary site is the latest, you need to perform data synchronization on the primary site and set the primary site to the active site. The system is restored to the **Normal state**. Performing this operation overwrites the data on the secondary site.
- Conversion (5): After the communication between the primary and secondary sites is recovered, if the data on the secondary site is the latest, you need to perform data synchronization on the secondary site and set the secondary site to the active site. The system is restored to the **Switched state**. Performing this operation overwrites the data on the primary site.

9.2 Managing the Login of VCS Users

VCS users manage the local clusters by logging in to the VCS client through which the centralized management for all the local hardware and software resources is realized. The software of the VCS also provides basic data ports to global cluster option (GCO) and monitors

the system and the application services in real time. When the hardware or software is faulty, the VCS restarts or shuts down the application service.

9.2.1 Adding a Cluster

This topic describes how to add a cluster on the VCS.

9.2.2 Logging In to the VCS Client

This topic describes how to log in to the VCS client.

9.2.3 Deleting a Cluster

This topic describes how to delete a cluster from the VSC.

9.2.4 Logging Out of the VCS Client

This topic describes how to log out of the VCS client.

9.2.5 Exiting the VCS Client

This topic describes how to exit the VCS client.

9.2.1 Adding a Cluster

This topic describes how to add a cluster on the VCS.

Procedure

- 1 Log in to the active site as the **root** user.

**NOTE**

In a distributed system, log in to the master server of the active site as the **root** user.

- 2 Run the following command to start the VCS client.

```
# hagu&
```

**NOTE**

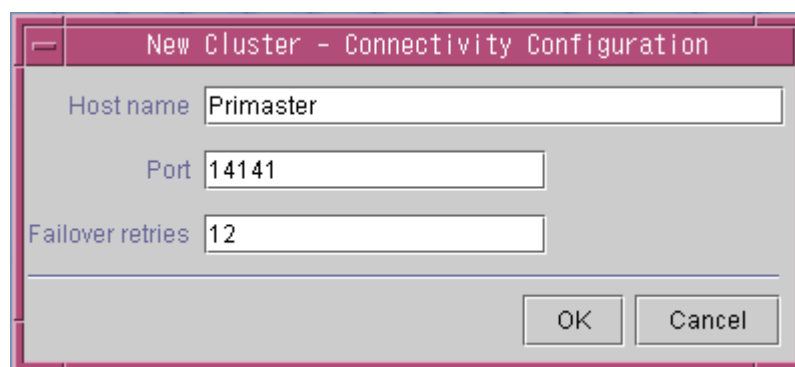
In the Windows OS, choose **Start > Programs > Symantec > Veritas Cluster Server > Veritas Cluster Manager - Java Console** to start the VCS client.

- 3 In the **Cluster Monitor** window, choose **File > New Cluster**.
- 4 In the dialog box that is displayed, enter the equipment name of the server such as **Primaster**, and click **OK**, as shown in [Figure 9-2](#).

**NOTE**

In **Host name**, you can also enter the system IP address of the site for login.

Figure 9-2 Adding a cluster



----End

9.2.2 Logging In to the VCS Client

This topic describes how to log in to the VCS client.

Prerequisite

The VCS service process must be started.

Procedure

- 1 Start the VCS client.

- In the Solaris or SUSE Linux OS:



In a distributed system, log in to the master server of the active site as the **root** user.

Run the following command to start the VCS client.

hagu&

- In the Windows OS:

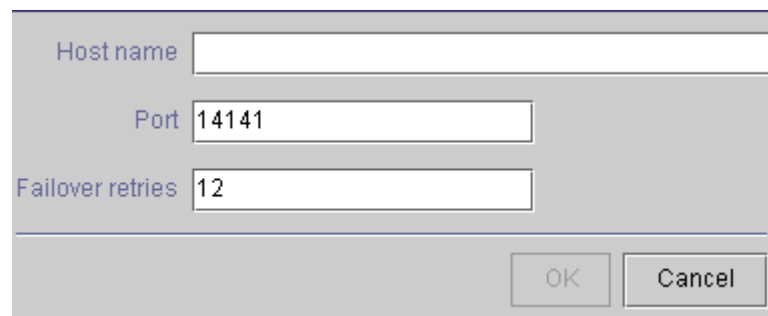
Choose **Start > Programs > Symantec > Veritas Cluster Server > Veritas Cluster Manager - Java Console** to start the VCS client.

- 2 In the **Cluster Monitor** window, select an active server from the list, such as Primaster.

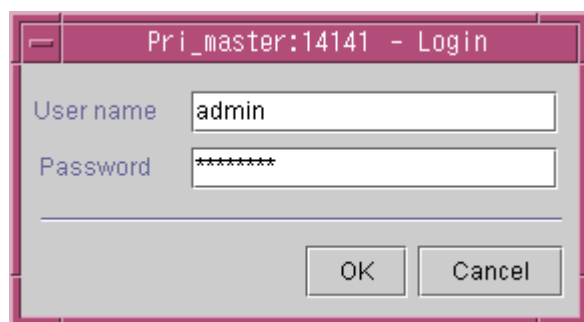


If you log in to the VCS client for the first time, the login is not recorded in the information list area. In this case, you need to create a cluster. For details, see [9.2.1 Adding a Cluster](#).

Figure 9-3 Cluster monitor

A dialog box titled "Cluster monitor" 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, there are two buttons: "OK" and "Cancel".

- 3 In the dialog box as shown in [Figure 9-4](#), input the legal user name and password, and click **OK**.

Figure 9-4 Logging in to the VCS**NOTE**

By default, the superuser of the VCS is **admin** and the password is **password**.

----End

9.2.3 Deleting a Cluster

This topic describes how to delete a cluster from the VSC.

Procedure

- 1 Log in to the active site as the **root** user.

NOTE

In a distributed system, log in to the master server of the active site as the **root** user.

- 2 Run the following command to start the VCS client.

```
# hagui&
```

NOTE

In the Windows OS, choose **Start > Programs > Symantec > Veritas Cluster Server > Veritas Cluster Manager - Java Console** to start the VCS client.

- 3 In the **Cluster Monitor** window, select a cluster, right-click, and choose **Delete**.
- 4 In the confirmation dialog box, click **Yes**.

----End

9.2.4 Logging Out of the VCS Client

This topic describes how to log out of the VCS client.

Prerequisite

You have logged in to the VCS client.

Procedure

- 1 On the VCS client that is logged in to , choose **File > Logout**.

----End

9.2.5 Exiting the VCS Client

This topic describes how to exit the VCS client.

Prerequisite

The VCS client is started.

Procedure

- 1 On the VCS client that is logged in to, choose **File > Exit**.

----End

9.3 Managing Resource Groups

This topic describes how to manage resource groups using the Cluster Explorer and commands.

[9.3.1 Bringing a Resource Group Online](#)

This topic describes how to bring a resource group online. You can bring all resources in a resource group online.

[9.3.2 Taking a Resource Group Offline](#)

This operation enables you to take all resources in a resource group offline offline.

[9.3.3 Locking a Resource Group](#)

This operation enables you to lock a resource group of the VCS. That is, lock all resources in the resource group.

[9.3.4 Unlocking a Resource Group](#)

This operation enables you to unlock a locked resource group of the VCS.

[9.3.5 Enabling a Resource Group](#)

This operation enables you to enable a resource group of the VCS.

[9.3.6 Disabling a Resource Group](#)

This operation enables you to disable a resource group of the VCS.

[9.3.7 Clearing a Resource Group Fault Flag](#)

This operation enables you to clear a resource group fault flag of the VCS.

9.3.1 Bringing a Resource Group Online

This topic describes how to bring a resource group online. You can bring all resources in a resource group online.

Prerequisite

The resource group must be enabled and not be frozen.

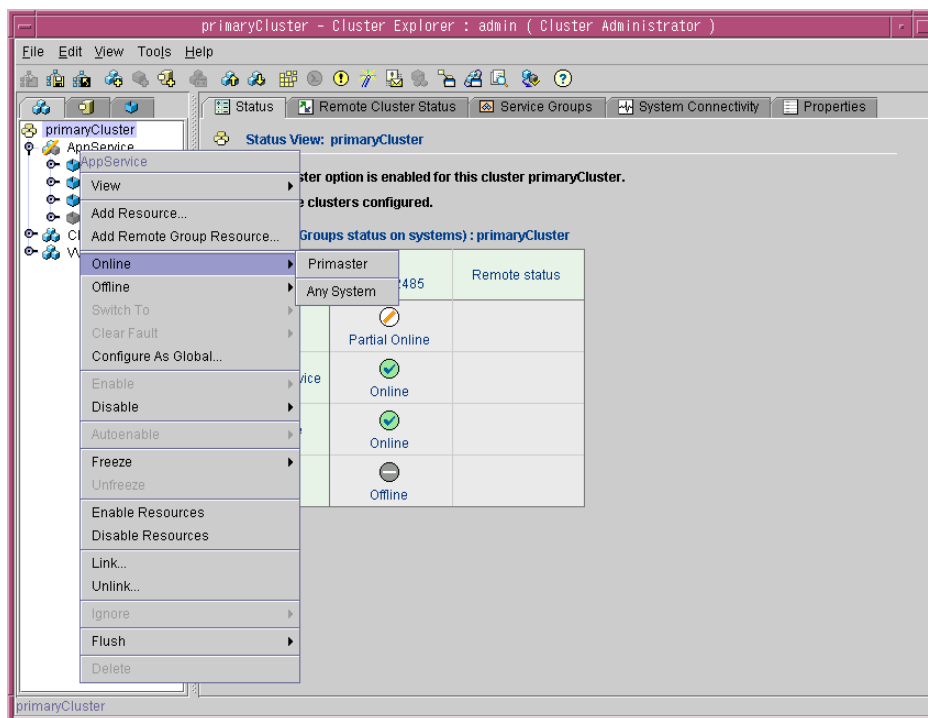
NOTE

- If the resource group is disabled, you must enable the resource group. For details, see [9.3.5 Enabling a Resource Group](#).
- If the resource group is frozen, you must unfreeze the resource group. For details, see [9.3.4 Unlocking a Resource Group](#).

Procedure

- Using the Cluster Explorer
 1. Choose a resource group, such as **AppService**, from the navigation tree of the VCS client.
 2. Right-click the resource group and choose **Online > Primaster** from the shortcut menu, as shown in [Figure 9-5](#).

Figure 9-5 Bringing a resource group online



3. Click **Yes**, bring a resource group online.
- Using the Command Lines
 - In the Solaris or SUSE Linux OS:
hagrp -online <service_group_name> -sys <hostname>
 Command example:
hagrp -online AppService -sys Primaster
 - In the Windows OS:
hagrp -online AppService -any

----End

9.3.2 Taking a Resource Group Offline

This operation enables you to take all resources in a resource group offline offline.

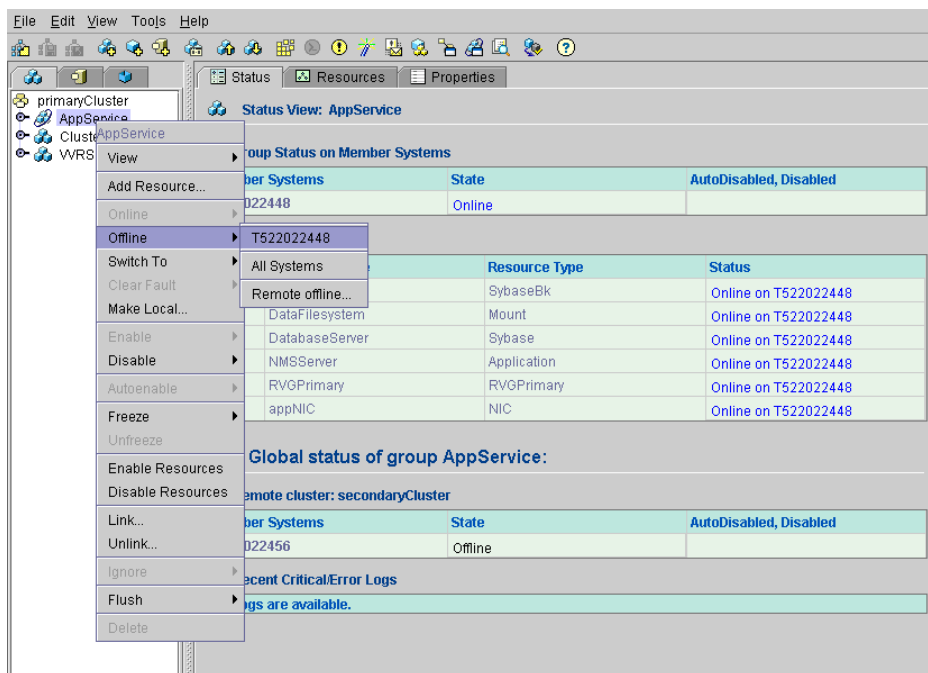
Prerequisite

The resource group is not frozen.

Procedure

- Using the Cluster Explorer
 1. On the navigation tree of the VCS client, select a resource group (such as **AppService**
 2. Right-click, and choose **Offline > Primaster**, as shown in [Figure 9-6](#).

Figure 9-6 Bringing a resource group offline



3. Click **Yes**.
- Using the Command Line
 - In the Solaris or SUSE Linux OS:
hagrp -offline <service_group_name> -sys <hostname>
Command example:
hagrp -offline AppService -sys Primaster
 - In the Windows OS:
hagrp -offline AppService -any

----End

9.3.3 Locking a Resource Group

This operation enables you to lock a resource group of the VCS. That is, lock all resources in the resource group.

Context

You need to lock resource groups for system maintenance. If a resource group is locked, you cannot bring it online, take it offline, or carry out the switchover.

Procedure

- Using the Cluster Explorer
 1. On the navigation tree of the VCS client, select a resource group (such as **AppService**).
 2. Right-click, and choose **Freeze > Temporary** or **Freeze > Persistent**.
 - Run **Freeze > Temporary** to lock the current resource group temporarily. After the VCS process is restarted, the resource group is unlocked.
 - Run **Freeze > Persistent** to lock the current resource group permanently. You need to recover the resource group manually. Otherwise, the resource group cannot be unlocked.
- Using the Command Line
 1. **hagrp -freeze <service_group_name> [-persistent]**

Command example:

hagrp -freeze AppService

----End

9.3.4 Unlocking a Resource Group

This operation enables you to unlock a locked resource group of the VCS.

Procedure

- Using the Cluster Explorer
 1. On the navigation tree of the VCS client, select a resource group (such as **AppService**).
 2. Right-click, and choose **Unfreeze**.
- Using the Command Line
 1. **hagrp -unfreeze <service_group_name> [-persistent]**

Command example:

hagrp -unfreeze AppService

----End

9.3.5 Enabling a Resource Group

This operation enables you to enable a resource group of the VCS.

Procedure

- Using the Cluster Explorer
 1. On the navigation tree of the VCS client, select a resource group (such as **AppService**).
 2. Right-click, and choose **Enable > Primaster**.
- Using the Command Line
 1. **haconf -makerw**

2. **hagrp -enable** <service_group_name> [-sys hostname]

Command example:

hagrp -enable AppService

----End

9.3.6 Disabling a Resource Group

This operation enables you to disable a resource group of the VCS.

Procedure

- Using the Cluster Explorer
 1. On the navigation tree of the VCS client, select a resource group (such as **AppService**).
 2. Right-click, and choose **Disable > Primaster**.
- Using the Command Line
 1. **haconf -makerw**
 2. **hagrp -disable** <service_group_name> [-sys hostname]

Command example:

hagrp -disable AppService

----End

9.3.7 Clearing a Resource Group Fault Flag

This operation enables you to clear a resource group fault flag of the VCS.

Procedure

- Using the Cluster Explorer
 1. On the navigation tree of the VCS client, select a resource group (such as **AppService**).
 2. Right-click, and choose **Clear Fault > Pri_master**.
- Using the Command Line
 1. **hagrp -clear** <service_group_name> [-sys hostname]

Command example:

hagrp -clear AppService

----End

9.4 Managing Resources

This topic describes how to manage resources in resource groups using the Cluster Explorer and commands.

9.4.1 Bringing a Resource Online

This operation enables you to bring a resource of the VCS online.

9.4.2 Taking a Resource Offline

This operation enables you to take a resource of the VCS offline.

9.4.3 Enabling a Resource

This operation enables you to enable a resource of the VCS.

9.4.4 Disabling a Resource

This operation enables you to disable a resource of the VCS.

9.4.5 Detecting Resources

This operation enables you to detect the resource status of the VCS.

9.4.6 Clearing a Resource Fault Flag

This operation enables you to clear a resource fault flag of the VCS.

9.4.7 Clearing the Current Operation

When you perform the online or offline operation on a resource group, all the resources in the resource group are taken online or offline. This topic describes how to clear the current operation if the operation needs to be stopped on a resource.

9.4.1 Bringing a Resource Online

This operation enables you to bring a resource of the VCS online.

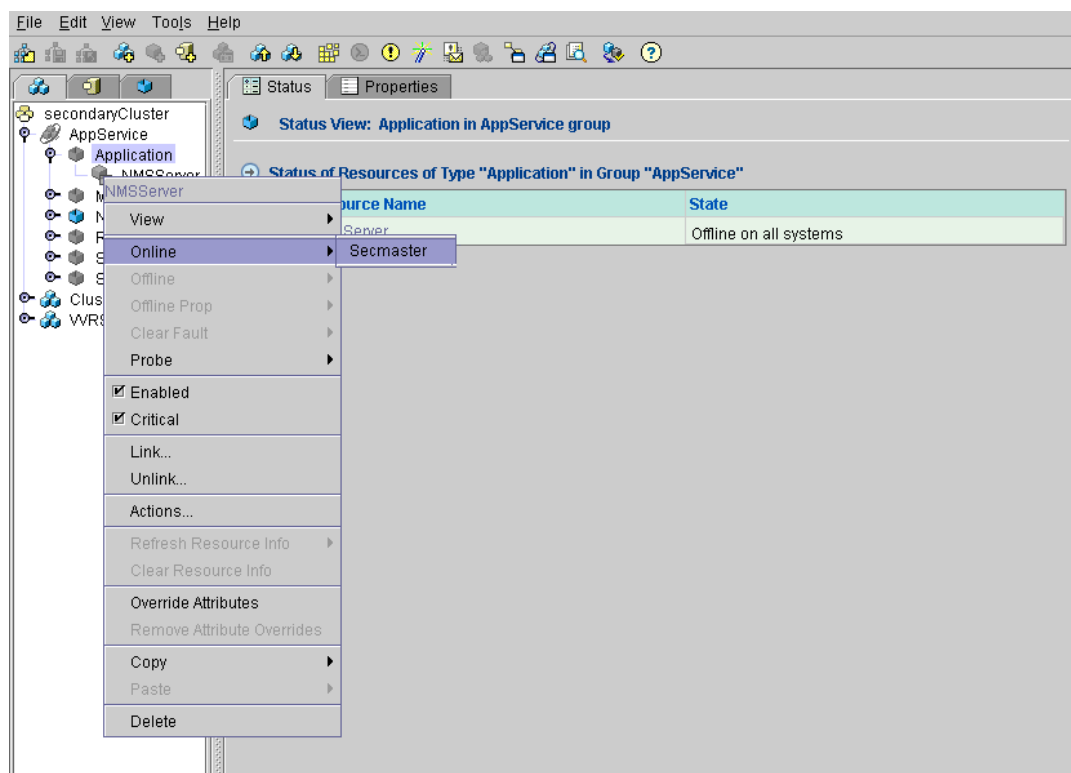
Prerequisite

The resource status is **enabled**, and all the dependent resources are online.

Procedure

- Using the Cluster Explorer
 1. On the navigation tree of the VCS client, select a resource (such as **NMSServer**).
 2. Right-click, and choose **Online > Secmaster**, as shown in **Figure 9-7**.

Figure 9-7 Bringing a resource online



3. Click **Yes** to enable the resource to be online.
- Using the Command Line
 1. **hares -online <resource_name> -sys <hostname>**

Command example:

hares -online NMSServer -sys Secmaster

----End

9.4.2 Taking a Resource Offline

This operation enables you to take a resource of the VCS offline.

Prerequisite

The dependent resources are offline.

Procedure

- Using the Cluster Explorer
 1. On the navigation tree of the VCS client, select a resource.
 2. Right-click, and choose **Offline > Primaster**.
 3. Click **Yes**.
- Using the Command Line

1. **hares -offline** <resource_name> [-ignoreparent] **-sys** <hostname> or **hares -offprop** <resource_name> [-ignoreparent] **-sys** <hostname>

Command example:

hares -offline NMSServer -sys Primaster

----End

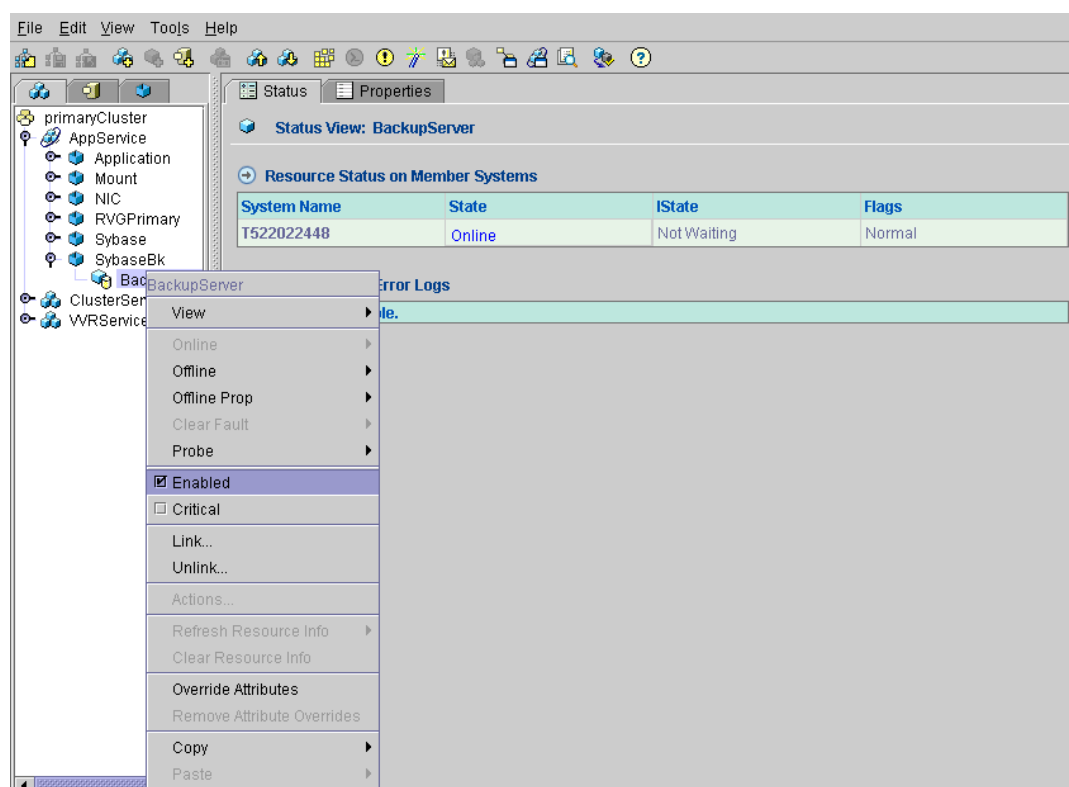
9.4.3 Enabling a Resource

This operation enables you to enable a resource of the VCS.

Procedure

- Using the Cluster Explorer
 1. On the navigation tree of the VCS client, select a resource (such as **BackupServer**).
 2. Right-click, and choose the **Enabled** check box, as shown in [Figure 9-8](#).

Figure 9-8 Enabling a resource



- Using the Command Line
 1. **hares -modify** <resource_name> **Enabled 1**

Command example:

- (1) Assign the read/write right to the resource:
haconf -makerw

- (2) Enable the resource:
`# hares -modify BackupServer Enabled 1`
- (3) Assign the read-only right to the resource:
`# haconf -dump -makero`

----End

9.4.4 Disabling a Resource

This operation enables you to disable a resource of the VCS.

Context

If a resource is disabled, you cannot bring it online.

Procedure

- Using the Cluster Explorer
 1. On the navigation tree of the VCS client, select a resource.
 2. Right-click, and deselect the **Enabled** check box.
- Using the Command Line
 1. **hares -modify <resource_name> Enabled 0**

Command example:

```
# haconf -makerwassign the read/write right to the resource
# hares -modify BackupServer Enabled 0disable the resource
# haconf -dump -makeroassign the read-only right to the resource
```

----End

9.4.5 Detecting Resources

This operation enables you to detect the resource status of the VCS.

Context

You can detect resources to check whether the resources are configured and started in the VCS.

Procedure

- Using the Cluster Explorer
 1. On the resource view of the Cluster Explorer, select a resource (such as **NMSServer**).
 2. Right-click, and choose **Probe > Primaster**.
- Using the Command Line
 1. **hares -probe <resource_name> -sys <hostname>**

Command example:

```
hares -probe NMSServer -sys Primaster
```

----End

9.4.6 Clearing a Resource Fault Flag

This operation enables you to clear a resource fault flag of the VCS.

Procedure

- Using the Cluster Explorer
 1. On the Cluster Explorer, select a resource (such as **NMSServer**).
 2. Right-click, and choose **Clear Fault > Primaster**.
- Using the Command Line
 1. **hares -clear <resource_name> [-sys hostname]**

Command example:

hares -clear NMSServer

----End

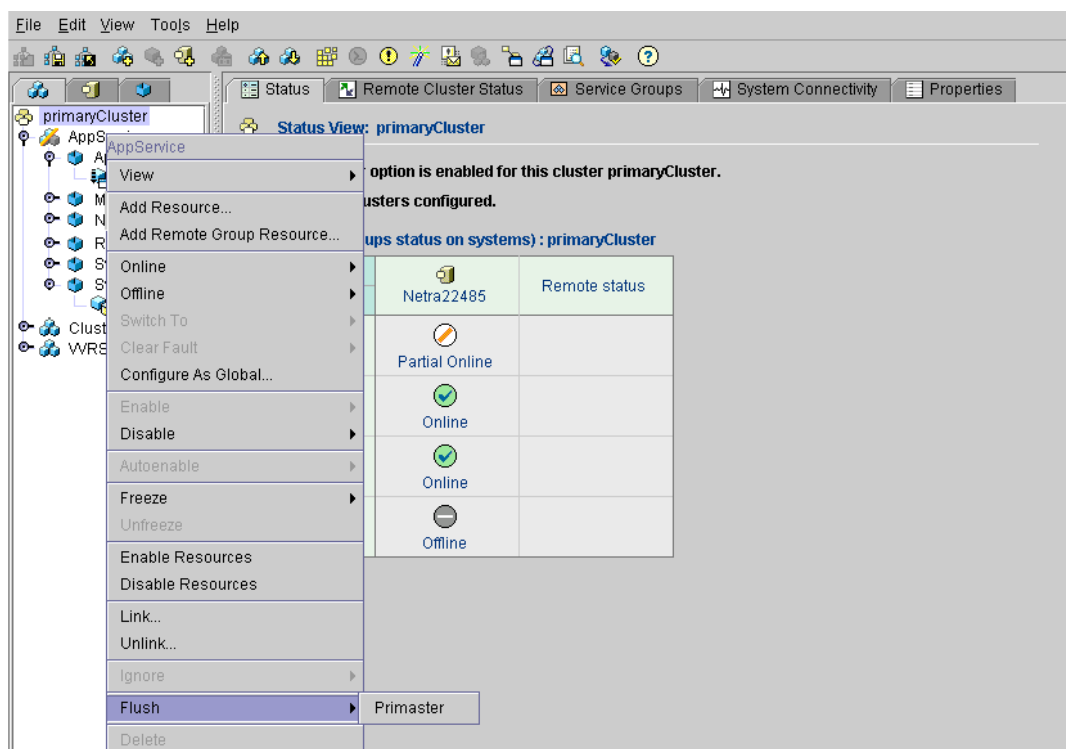
9.4.7 Clearing the Current Operation

When you perform the online or offline operation on a resource group, all the resources in the resource group are taken online or offline. This topic describes how to clear the current operation if the operation needs to be stopped on a resource.

Procedure

- 1 On the tree of the VCS client, select a resource group node, such as **AppService**. Suppose that the online or offline operation stops on **AppService**.
- 2 Right-click, and choose **Flush > Primaster**, as shown in [Figure 9-9](#).

Figure 9-9 Clearing the current operation



----End

9.5 Managing Replication Volumes

This topic describes how to manage replication volumes using the Cluster Explorer and commands.

9.5.1 Importing a Disk Group

This topic describes how to import a disk group. You can import a disk group by using the commands.

9.5.2 Recovering a Disk Volume

This operation enables you to recover a disk volume using the commands.

9.5.3 Recovering the RVG

This operation enables you to recover the RVG using commands.

9.5.4 Recovering the RLink

This operation enables you to recover the RLink using commands.

9.5.5 Re-synchronizing the Data on Primary and Secondary Sites

This topic describes how to recover and reestablish the replication relationship and how to synchronize the latest data on a site to the other by using commands, if the replication relationship between the primary and secondary sites is abnormal.

9.5.1 Importing a Disk Group

This topic describes how to import a disk group. You can import a disk group by using the commands.

Prerequisite

The VxVM process must be started.

Context

Normally, the disk group is imported when the VxVM starts. In this case, you do not need to perform this operation.

Procedure

- In the Solaris or SUSE Linux OS:
`vxdg import <diskgroupname>`
`vxrecover -g <diskgroupname> -sb`
Command example:
`vxdg import datadg`
`vxrecover -g datadg -sb`
- In the Windows OS:
`vxdg -g <diskgroupname> import`

Command example:

```
vxdbg -g datadg import
```

 **NOTE**

You can run the **vxdbg list** command to query *<diskgroupname>*.

----End

9.5.2 Recovering a Disk Volume

This operation enables you to recover a disk volume using the commands.

Context

Run the **vxprint -v** command to check the status of a disk volume.

Check if **STATE** is **ACTIVE** and **KSTATE** is **ENABLED**. If not, it indicates that the disk volume is abnormal.

Procedure

- 1 Run the following commands to recover and start the disk volume.

```
vxrecover -g <diskgroupname> -sb
```

```
vxvol -g <diskgroupname> start <volumename>
```

----End

Example

```
vxrecover -g datadg -sb
```

```
vxvol -g datadg start lv_nms_data
```

 **NOTE**

You can run the **vxdbg list** command to query the *<diskgroupname>*, and run the **vxprint -v** command to query the *<volumename>*.

9.5.3 Recovering the RVG

This operation enables you to recover the RVG using commands.

Context

Run the **vxprint -VI** command to check the RVG status.

Check if **state** is **ACTIVE** and **kernel** is **ENABLED**. If not, it indicates that the RVG is abnormal.

Procedure

- 1 Run the following commands to recover and start the RVG.

```
vxrvrg -g <diskgroupname> recover <rvgname>
```

```
vxrvrg -g <diskgroupname> start <rvgname>
```


Command example:

```
vxrvrg -g datadg recover datarvg
```

```
vxrvrg -g datadg start datarvg
```

 **NOTE**

You can run the **vx dg list** command to query the *<diskgroupname>*, and run the **vradmin printrvg** command to query the *<rvname>*.

----End

9.5.4 Recovering the RLink

This operation enables you to recover the RLink using commands.

Context

Run the **vxprint -PI** command to check the RLink Status.

Check if **state** is **ACTIVE**. If not, it indicates that the RLink is abnormal.

Procedure

- 1 Run the following commands to recover the RLink.

```
vxrlink -g <diskgroupname>
```

```
recover <rlinkname>
```

Command example:

```
vxrlink -g datadg recover datarlk
```

----End

9.5.5 Re-synchronizing the Data on Primary and Secondary Sites

This topic describes how to recover and reestablish the replication relationship and how to synchronize the latest data on a site to the other by using commands, if the replication relationship between the primary and secondary sites is abnormal.

Procedure

- 1 Check that the replication relationship between the primary and secondary sites is normal.

Run the following command to check the replication relationship between the primary and secondary sites:

```
vradmin -g <diskgroupname> -l repstatus <rvname>
```

Command example:

```
vradmin -g datadg -l repstatus datarvg
```

Check the following items:

- Whether **Data status** is **consistent, up-to-date**
- Whether **Replication status** is **replicating (connected)**

If not, it indicates that the replication relationship is abnormal. run the following command to recover the replication relationship between the primary and secondary sites:

- In the Solaris or SUSE Linux OS:

```
vxrlink -g <diskgroupname> att <rlinkname>
```

Command example:

```
vxrlink -g datadg att datarlk
```

- In the Windows OS:

```
vxrlink -g <diskgroupname> -a -r rvg att <rlinkname>
```

Command example:

```
vxrlink -g datadg -a -r rvg att datarlk
```

 NOTE

This command needs to be run on both the active site and the standby site.

- 2 Run the following command to synchronize the latest data on a site to the other:

```
vxrvrg -g <diskgroupname> resync <rvgname>
```

Command example:

```
vxrvrg -g datadg resync datarvg
```

 NOTE

This command needs to be run only on the active site or the standby site.

----End

9.6 Switching Over the Active Site and the Standby Site

This topic describes how to switch over the active site and the standby site.

9.6.1 Manual Switchover Between Active and Standby Sites

This topic describes how to manually switch over the U2000 applications from the active site to the standby site and then from the standby site to the active site. In this way, you can check the system reliability and maintain the system.

9.6.2 Automatic Switchover Between Primary and Secondary Sites

This topic describes how to enable the automatic switchover function so that the automatic switchover operation can be performed.

9.6.1 Manual Switchover Between Active and Standby Sites

This topic describes how to manually switch over the U2000 applications from the active site to the standby site and then from the standby site to the active site. In this way, you can check the system reliability and maintain the system.

Prerequisite

Ensure that the following prerequisites are met before performing the operation.

- The heartbeat connection between the active site and the standby site is normal.
- The data replication between the active site and the standby site is normal.
- The active site and the standby site are normal and no fault occurs.

Context

After the active site is switched over to the standby site, the original standby site in the cluster changes to the active site. In addition, the replication relation between the active site and the standby site is repaired and the replication direction is specified again.

Procedure

- 1 Run the following command to check the replication status.

In the Solaris or SUSE Linux OS:

```
# vradmin -g <diskgroupname> repstatus <rvgname>
```

Command example:

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

The following information appears.

```
Replicated Data Set: datarvg
Primary:
  Host name:          10.71.210.78
  RVG name:           datarvg
  DG name:            datadg
  RVG state:          enabled for I/O
  Data volumes:       4
  VSets:              0
  SRL name:           lv_srl
  SRL size:           3.00 G
  Total secondaries:  1

Secondary:
  Host name:          10.71.210.76
  RVG name:           datarvg
  DG name:            datadg
  Data status:        consistent, up-to-date
  Replication status: replicating (connected)
  Current mode:       asynchronous
  Logging to:         SRL
  Timestamp Information: behind by 0h 0m 0s
```

NOTE

You can perform the active/standby replication switchover only when **Data status** is **consistent, up-to-date**.

In the Windows OS:

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

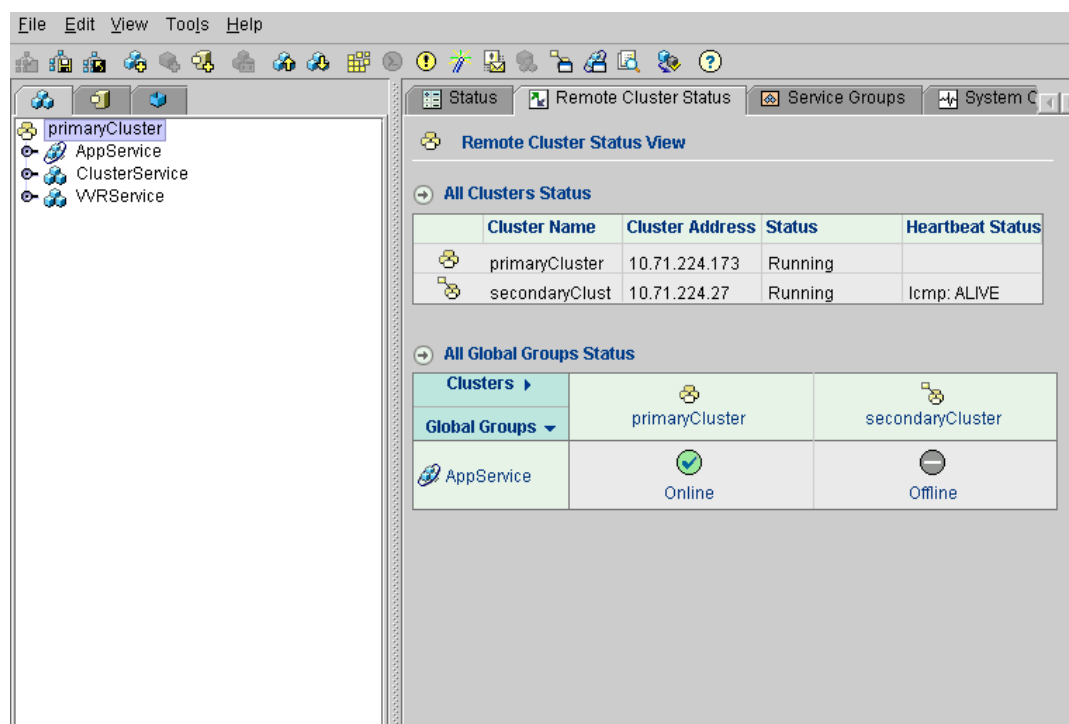
The following information appears.

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

NOTE

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

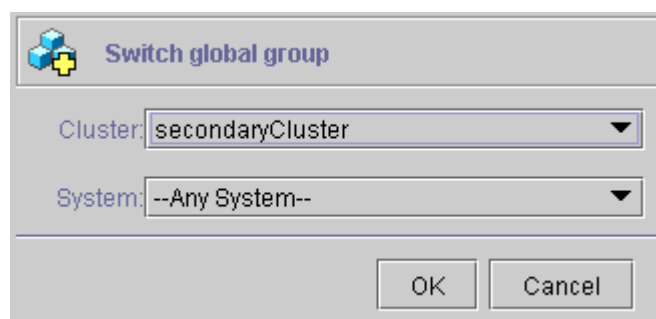
- 2 [Log in to the VCS client.](#)
- 3 On the navigation tree on the VCS client, click the **primaryCluster** root node, and click the **Remote Cluster Status** tab to view the status of the active and standby sites, heartbeat, **AppService**, **ClusterService** and **RepService** resource groups, as shown in [Figure 9-10](#).

Figure 9-10 Viewing the status of the remote cluster**NOTE**

You can perform the active/standby replication switchover only when the following requirements are met:

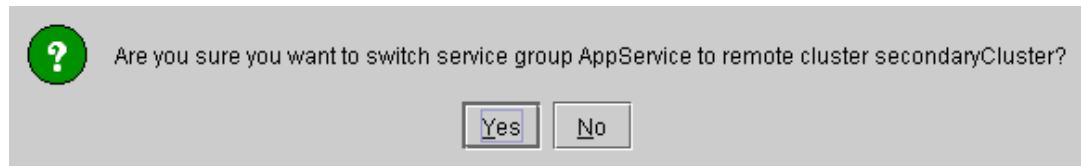
- The status of the active and standby sites is **Running**.
- The status of the heartbeat between the active site and the standby site is **ALIVE**.
- The status of the application resource group of the active site (such as AppService) is **Online**.
- The status of the application resource group of the standby site (such as AppService) is **Offline**.

- 4 On the navigation tree on the left side, choose the **AppService** node, right-click, and choose **Switch To > Remote switch**.
- 5 Set **Cluster** to **U2KClusterSecserver** and **System** to **Secmaster**, as shown in [Figure 9-11](#).

Figure 9-11 Switching over the global group

- 6 Click **OK**, as shown in [Figure 9-12](#).

Figure 9-12 Confirming the switchover



- 7 Click **Yes**, as shown in [Figure 9-12](#). The service of the U2000 is switched over to the standby site.

 NOTE

- The switchover duration depends on the installed components and network conditions. It usually takes 10 to 15 minutes.
- Choose the AppService resource group on the navigation tree, and then click the **Status** tab. If **State of Group Status on Member Systems** is **Online**, it indicates that the switchover between the active and standby sites is successful.

----End

9.6.2 Automatic Switchover Between Primary and Secondary Sites

This topic describes how to enable the automatic switchover function so that the automatic switchover operation can be performed.

Prerequisite

When the following faults occur on the active site, the VCS automatically switches the database and the U2000 server to the standby site.

- The core process of the U2000 service is abnormal.
- The database is abnormal.

 NOTE

When the standby site is switched to the active site, if the preceding faults occur, the VCS automatically switches the database and the U2000 server to the original active site.

Procedure

- 1 The automatic switchover function is enabled when the core process of the U2000 is abnormal or the database is abnormal.

Only one active site exists. The switchover operation can be performed between the active and standby sites. After a fault is rectified, you can switch the applications to the original active site manually. For details of the manual switchover, see [9.6.1 Manual Switchover Between Active and Standby Sites](#).

- 2 The automatic switchover function is enabled when the heartbeat is stopped between the active and standby sites or the replication is abnormal.

Two primary servers exist. When the fault is troubleshot, the recovery operation needs to be performed again. The recovery duration depends on the data amount.

----End

9.7 Monitoring Active and Standby Sites

This topic describes how to monitor the status of active and standby sites by using the VCS or the commands.

9.7.1 Checking the Data Replication Status

This topic describes how to check the data replication status of the active and standby sites.

9.7.2 Checking the Status of the Active and Standby Sites

This topic describes how to check the status of the all the resource groups on the active and standby sites and the heartbeat status.

9.7.1 Checking the Data Replication Status

This topic describes how to check the data replication status of the active and standby sites.

Procedure

- In the Solaris or SUSE Linux OS:

1. Log in to the active site as the **root** user.

NOTE

In a distributed system, log in to the master server of the active site as the **root** user.

2. Run the following command to check the data replication status of the active and standby sites.

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

The following information appears.

```
Replicated Data Set: datarvg
Primary:
  Host name:          10.71.210.78
  RVG name:           datarvg
  DG name:            datadg
  RVG state:          enabled for I/O
  Data volumes:       4
  VSets:              0
  SRL name:           lv_srl
  SRL size:           3.00 G
  Total secondaries:  1

Secondary:
  Host name:          10.71.210.76
  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
```

Check whether the displayed information about the **Data status** is **consistent, up-to-date** and that of **Replication status** is **replicating (connected)**. If yes, it indicates that the replication relation between the active site and the standby site is normal. Otherwise, you need to create the replication relation again.

- In the Windows OS:

1. Log in to the active site.
2. Run the following command to check the data replication status of the active and standby sites.

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

The following information appears.

```
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.

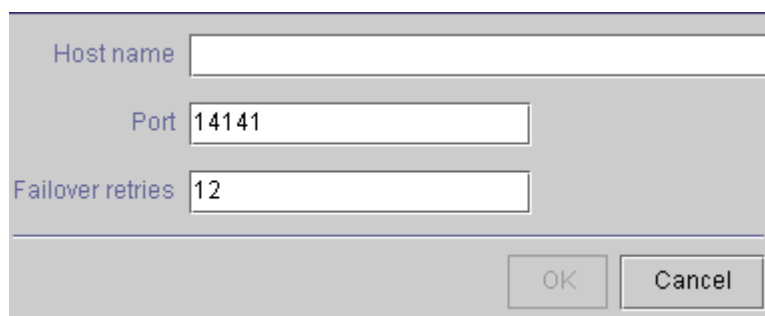
----End

9.7.2 Checking the Status of the Active and Standby Sites

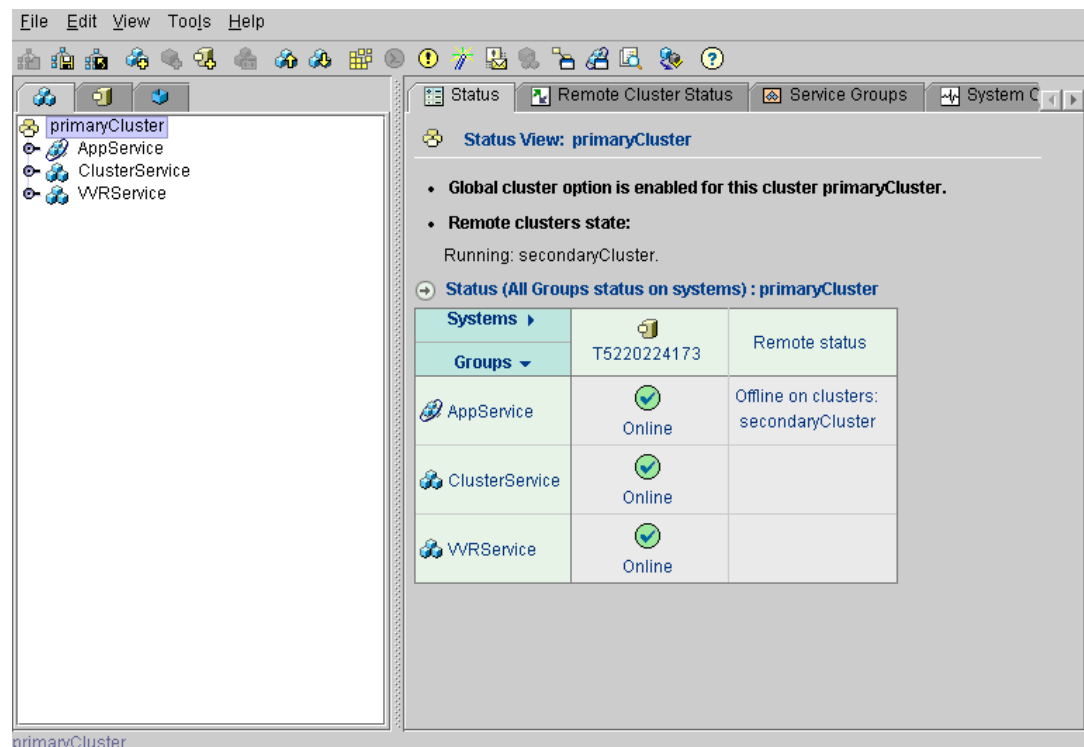
This topic describes how to check the status of the all the resource groups on the active and standby sites and the heartbeat status.

Procedure

- 1 Start the VCS client.
 - In the Solaris or SUSE Linux OS:
 **NOTE**
In a distributed system, log in to the master server of the active site as the **root** user.
Run the following command to start the VCS client.
hagu&
 - In the Windows OS:
Choose **Start > Programs > Symantec > Veritas Cluster Server > Veritas Cluster Manager - Java Console** to start the VCS client.
- 2 In the **Cluster Monitor** window, click **File > New Cluster**, the following dialog box is displayed.

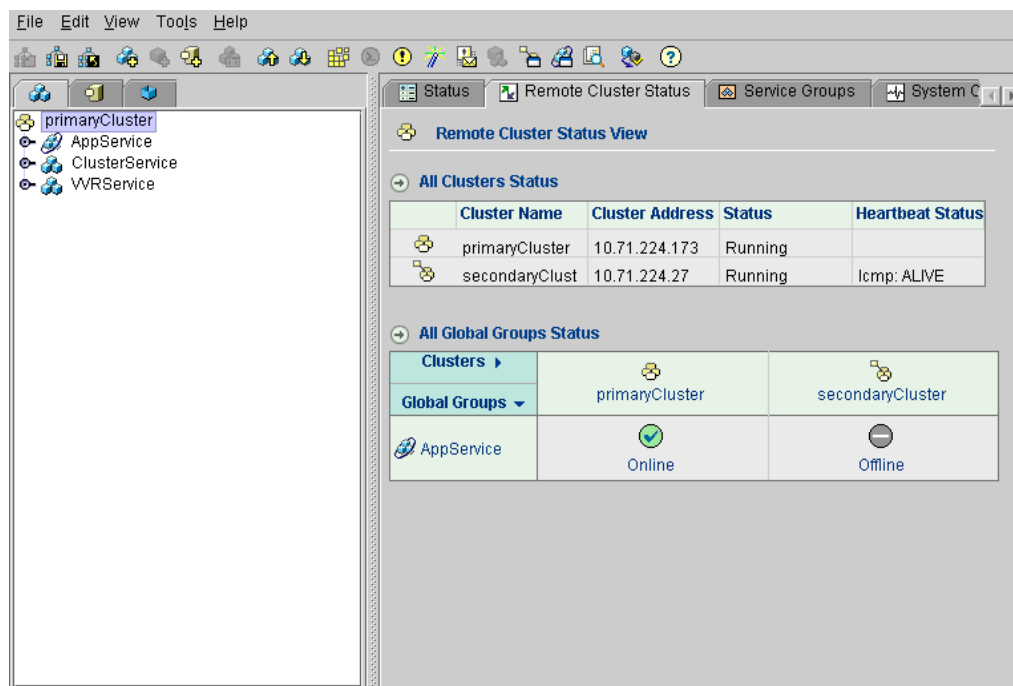
A dialog box titled "New Cluster" with a light gray background. It contains three input fields: "Host name" (empty), "Port" (containing "14141"), and "Failover retries" (containing "12"). At the bottom right, there are two buttons: "OK" and "Cancel".

- 3 In **Host name**, enter the system IP address of the active site for login.
- 4 In the login dialog box that is displayed, input the user name and password of the VCS, and click **OK**.
 **NOTE**
The default user and password of the VCS are **admin** and **password**.
- 5 After logging in to the Cluster Explorer, select the **primaryCluster** node on the tree in the left pane, and click the **Status** tab in the right pane. The interface is as shown in [Figure 9-13](#).

Figure 9-13 Status of the resource groups on the active site

The status of **AppService**, **ClusterService**, and **ClusterService** of **VVRService** in the information list is **Online**.

- Click the **Remote Cluster Status** tab to check the heartbeat status of the center standby site at the remote end. The interface is as shown in [Figure 9-14](#).

Figure 9-14 Heartbeat status of the center standby site

In the **All Clusters Status** area, the **Status** of the clusters **primaryCluster** and **secondaryCluster** for the active and standby sites is **Running**.

The **Heartbeat Status** of the cluster **secondaryCluster** corresponding to the standby site in the **All Clusters Status** area is **Icmp:ALIVE**.

The application resource group status of the clusters **primaryCluster** and **secondaryCluster** corresponding to the active site and the standby site in the **All Global Groups Status** area is **Online** and **Offline** respectively.

- 7 In the **Cluster Monitor** window, click **File > New Cluster**, the following dialog box is displayed.

The 'New Cluster' dialog box is shown with the following fields and values:

- Host name:
- Port:
- Failover retries:

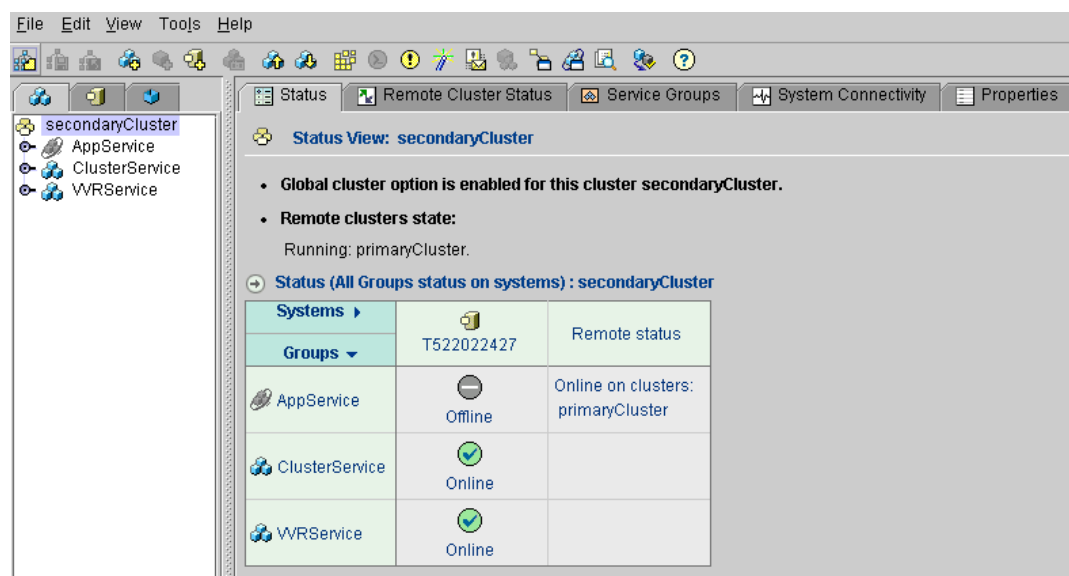
Buttons: OK, Cancel

- 8 In **Host name**, enter the system IP address of the standby site for login.
- 9 In the login dialog box that is displayed, input the user name and password of the VCS, and click **OK**.

NOTE

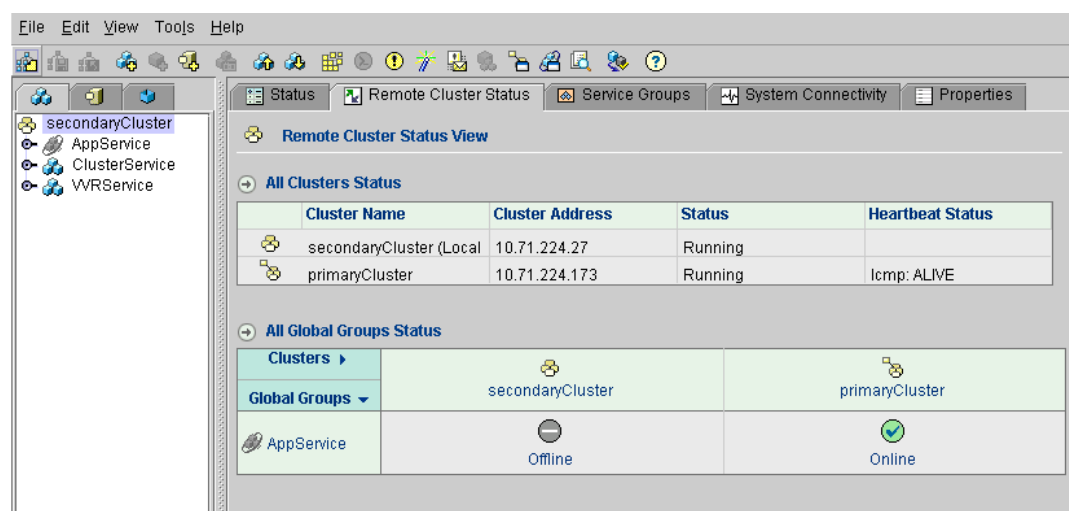
The default user and password of the VCS are **admin** and **password**.

- 10 After logging in to the Cluster Explorer, select the **secondaryCluster** node on the tree in the left pane, and click the **Status** tab in the right pane. The interface is as shown in **Figure 9-15**.

Figure 9-15 Resource group status of the center standby site

The status of **ClusterService** and **VVRService** of **Secserver** is **Online**. The status of **AppService** is **Offline**.

- Click the **Remote Cluster Status** tab to check the heartbeat status of the active server at the remote end. The interface is as shown in [Figure 9-16](#).

Figure 9-16 Heartbeat status of the active server

In the **All Clusters Status** area, the **Status** of the clusters **primaryCluster** and **secondaryCluster** for the active and standby sites is **Running**.

The **Heartbeat Status** of the cluster **primaryCluster** corresponding to the standby site in the **All Clusters Status** area is **Icmp:ALIVE**.

The application resource group status of the clusters **primaryClusterr** and **secondaryCluster** corresponding to the active site and the standby site in the **All Global Groups Status** area is **Online** and **Offline** respectively.

----End

10 U2000 Port List

About This Chapter

This topic describes the service ports used by the U2000.

[10.1 U2000 Service Port Overview](#)

This topic describes the U2000, service ports to be filtered and the method to query service ports.

[10.2 Ports Between the U2000 Server and the NEs](#)

This topic describes the ports used between the U2000 server and the NEs.

[10.3 Ports Between the U2000 Server and the Clients](#)

This topic describes the ports used between the U2000 server and the clients.

[10.4 Ports Between the U2000 Server and the OSS](#)

This topic describes the ports used between the U2000 server and the operation support system (OSS).

[10.5 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.

[10.6 Ports for Internal Processes of the U2000 Server](#)

This topic describes the ports for internal processes of the U2000 server.

[10.7 Ports for Remote Maintenance](#)

This topic describes the ports for remote maintenance.

[10.8 Ports for Other Connections](#)

This topic describes the ports for communication between the U2000 server and other applications.

10.1 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.

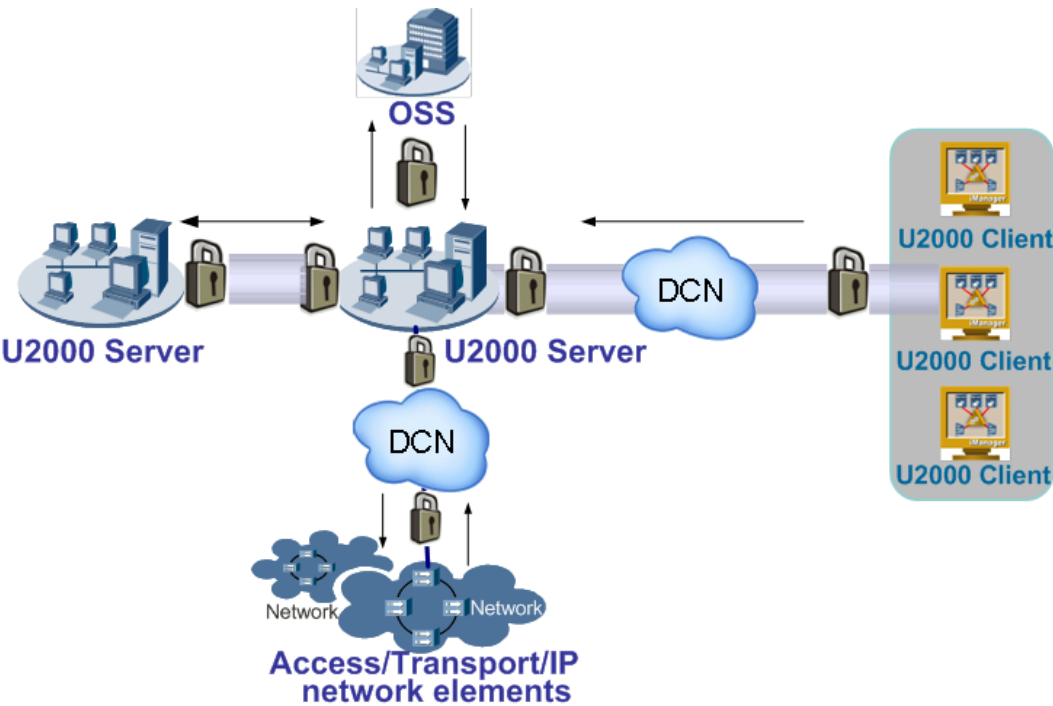
U2000 service ports are classified into the following types:

- 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 10-1 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
  -----
  *.*
  *.4145             *.*                 0      0 49152      0 IDLE
  *.8989             *.*                 0      0 49152      0 LISTEN
  *.8199             *.*                 0      0 131760     0 LISTEN
  *.14150            *.*                 0      0 49152      0 LISTEN
  *.111              *.*                 0      0 49152      0 LISTEN
  ...

```

10.2 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 10-1](#).
- Any port on the NEs can connect to the ports listed in [Table 10-2](#).

Table 10-1 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 10-2 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.

10.3 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 10-3](#).

Table 10-3 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.

10.4 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 10-4](#).

Table 10-4 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 10-5 lists the ports on the OSS for connecting the U2000 server.

Table 10-5 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.

10.5 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 10-6**.

 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 10-6 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.

10.6 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 10-7](#).

Table 10-7 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.

10.7 Ports for Remote Maintenance

This topic describes the ports for remote maintenance.

Table 10-8 lists the ports for remote maintenance.

Table 10-8 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.

10.8 Ports for Other Connections

This topic describes the ports for communication between the U2000 server and other applications.

Table 10-9 lists the ports for communication between the U2000 server and other applications.

Table 10-9 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.

11 Changing the System IP Address and Host Name

About This Chapter

This topic describes how to change the system IP address and host name for different installation schemes. Related operation steps vary according to installation schemes.

[11.1 How to Change the IP Address of the Single-Server System on Windows](#)

[11.2 How to Change the Host Name of the Single-Server System on Windows](#)

[11.3 How to Change the IP Address and Host Name for the Single-Server System \(Solaris\)](#)

[11.4 How to Change the IP Address and Host Name of the Single-Server System \(SUSE Linux-Distributed\)](#)

[11.5 How to Modify the Server IP Address of High Availability System \(Windows\)](#)

[11.6 How to Change the Host Name of the High Availability System \(Windows\)](#)

[11.7 How to Change the IP Address and Host name for the High Availability System \(Solaris\)](#)

[11.8 How to Change the IP Address and Host Name of the High Availability System \(SUSE Linux-Distributed\)](#)

11.1 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

11.2 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

11.3 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

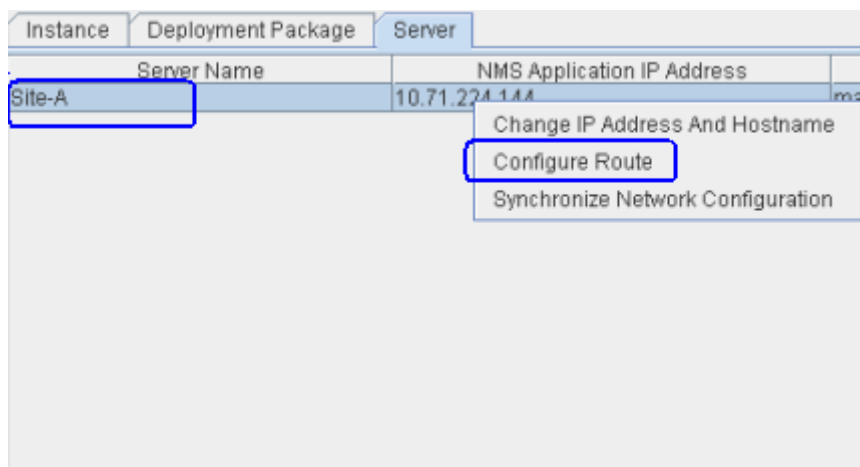
NOTE

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.



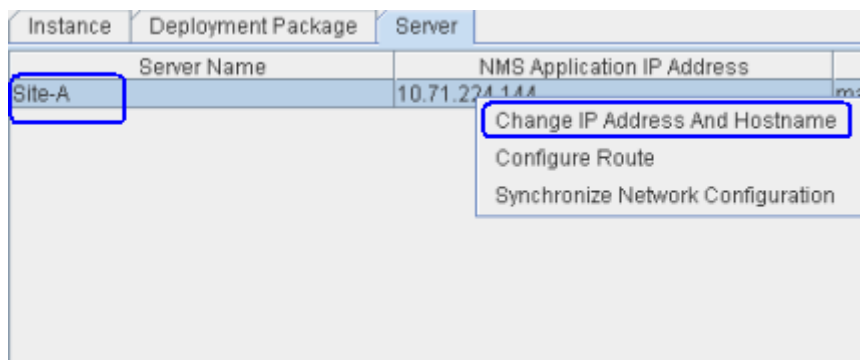
2. In the dialog box that is displayed, click **Add** or **Delete** according to actual route conditions to re-configure the route.

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

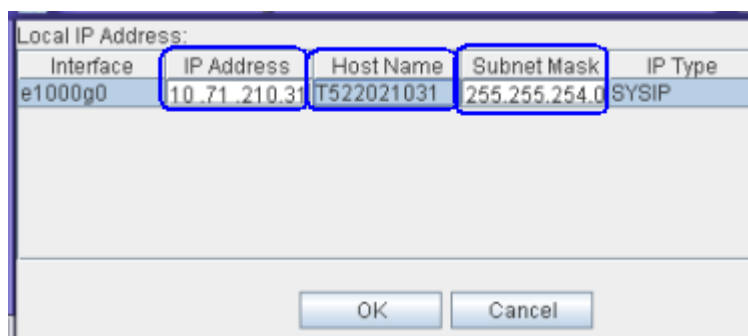
3. Click **OK**.

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.



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

11.4 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

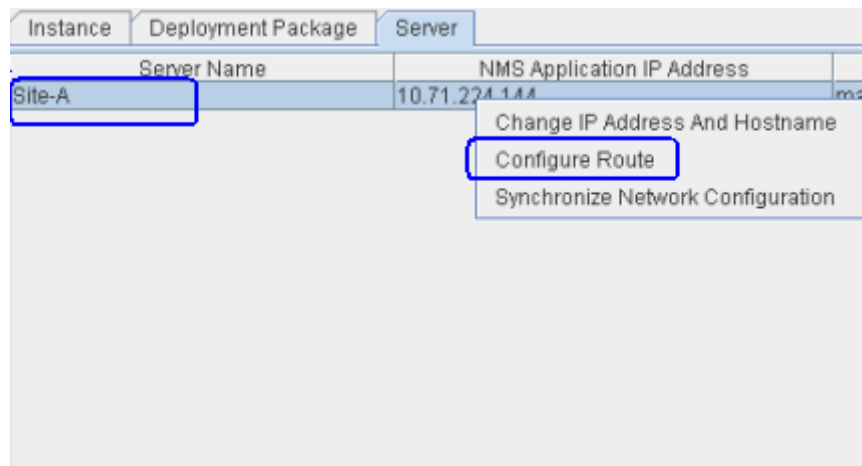
If multiple slave servers are installed, perform this step on every slave server.

- 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.



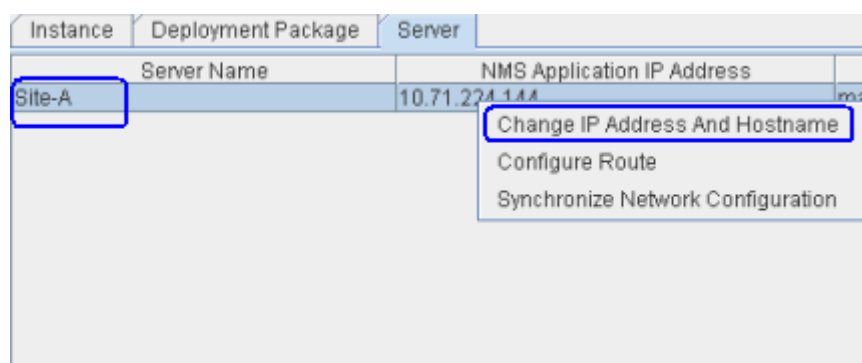
2. In the dialog box that is displayed, click **Add** or **Delete** according to actual route conditions to re-configure the route.

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

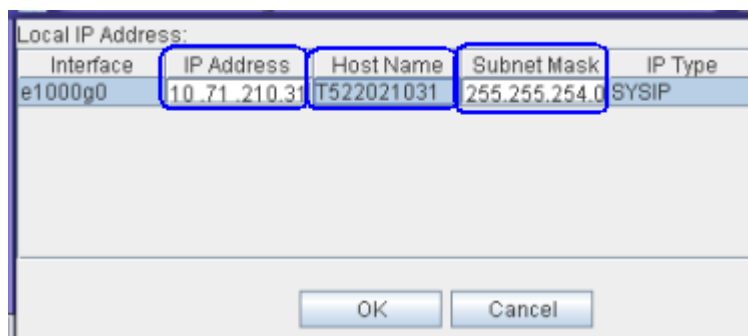
3. Click **OK**.

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.9.28 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

11.5 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.

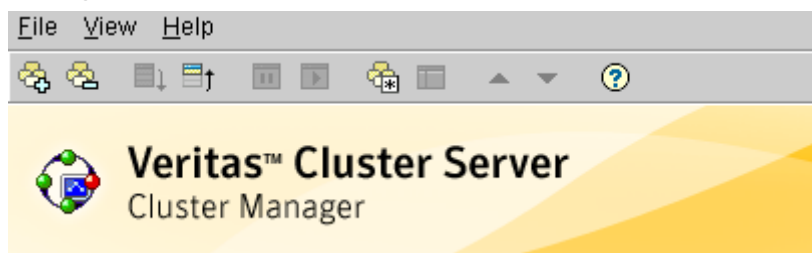
Changing an IP address includes the following major steps:

1. Separate the primary and secondary sites.
2. Shut down the U2000 server and client, and ensure that the database is running.

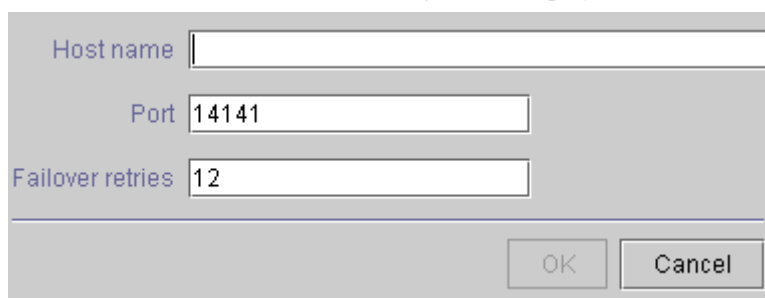
3. Shut down the U2000 MSuite server.
4. Change the IP address of the U2000 server.
5. Change the system IP address that is set in the VCS.
6. Start the U2000 MSuite server.
7. Log in to the U2000 MSuite client and synchronize IP address changes in configuration files. If the IP address changes are not 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

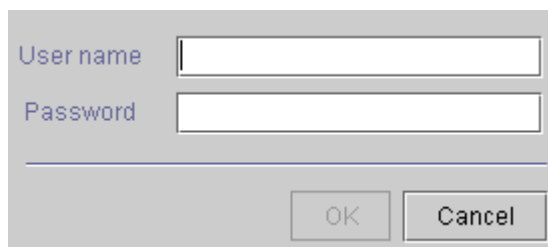
- 1 Log in to the NMS maintenance tool client. Choose **Deploy > Separate the primary and secondary sites**. The **Separate the primary and secondary sites** dialog box is displayed.
- 2 Click **OK**. The progress bar is displayed indicating the status of separating the primary and secondary sites. Wait 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.

11.6 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.

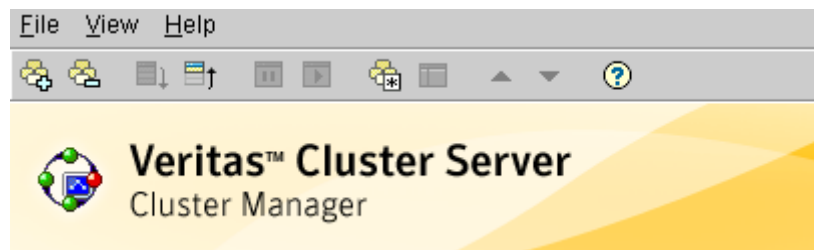
Do not change an IP address and a host name at the same time. Otherwise, the U2000 fails to be started.

Changing the host name includes the following major steps:

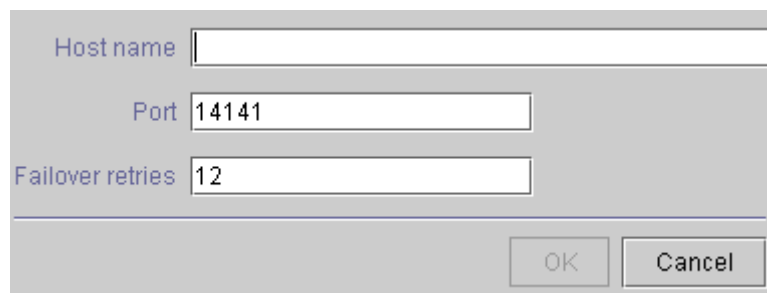
1. Shut down the U2000 server and client.
2. Stop the VCS service and communication.
3. Change the host name changes in configuration files.
4. Change the host name of the U2000 server.
5. Restart the OS.
6. Log in to the U2000 MSuite client and synchronize host name changes in configuration files. If the host name changes are not synchronized, the U2000 fails to start properly.

Answer

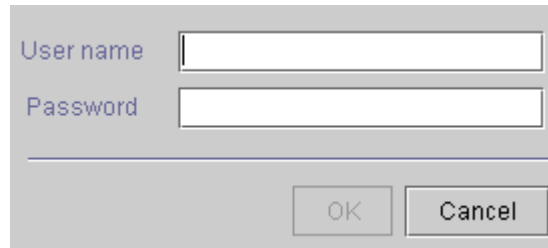
- 1 Log in to the OS as a user with administrator rights.
- 2 At the primary site, perform the following operations to end the U2000 processes:
 1. Choose **Start > Programs > Symantec > Veritas Cluster Server > Veritas Cluster Manager - Java Console** to start the VCS client.



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 : \> 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

11.7 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

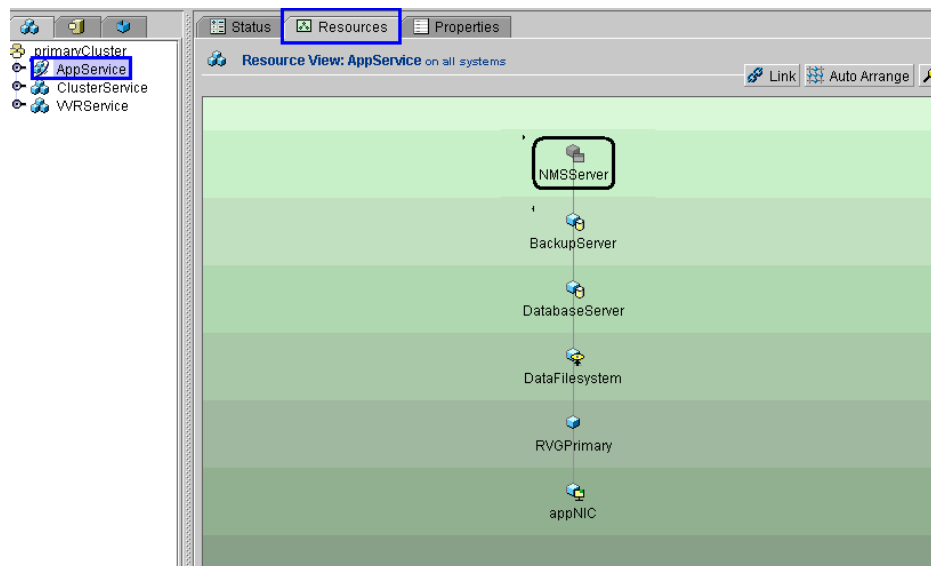
To change the IP address and host name for the single-server system (Solaris), do as follows:

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 [C.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.

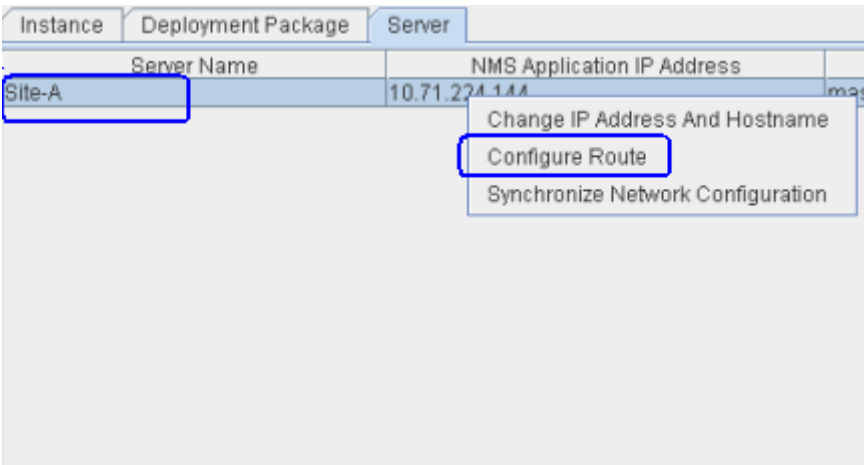
Figure 11-1 High Availability System (Solaris) resources



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.
 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

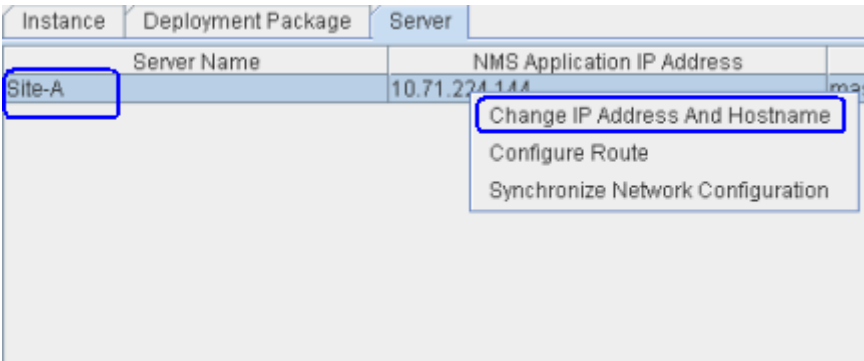
Add

Delete

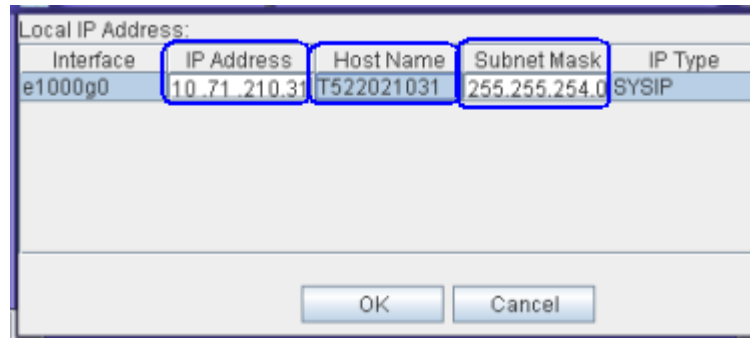
3. Click **OK**.

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.



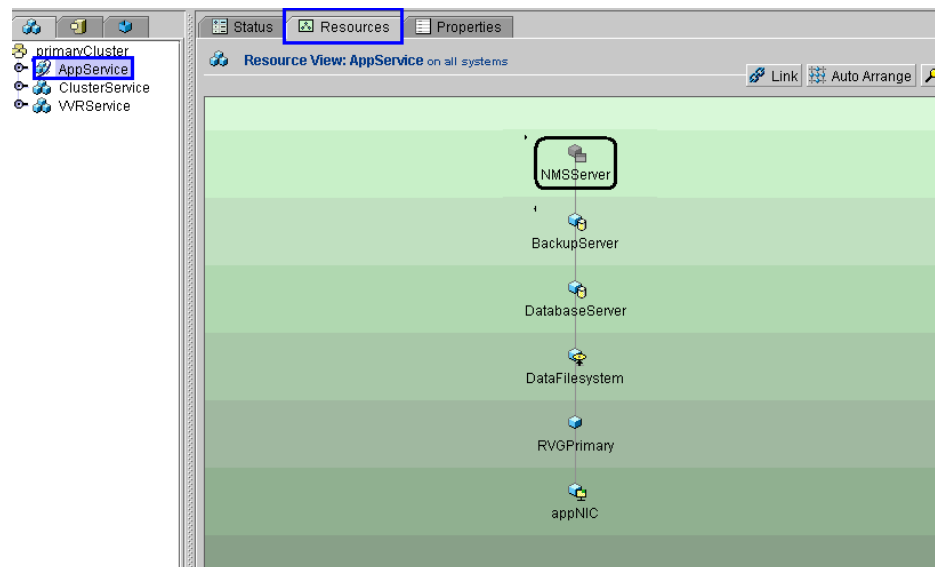
2. In the **Change IP Address And Hostname** dialog box, enter the new host name, IP address, and subnet mask.



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.


```
# 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 11-2 High Availability System (Solaris) resources



 NOTE

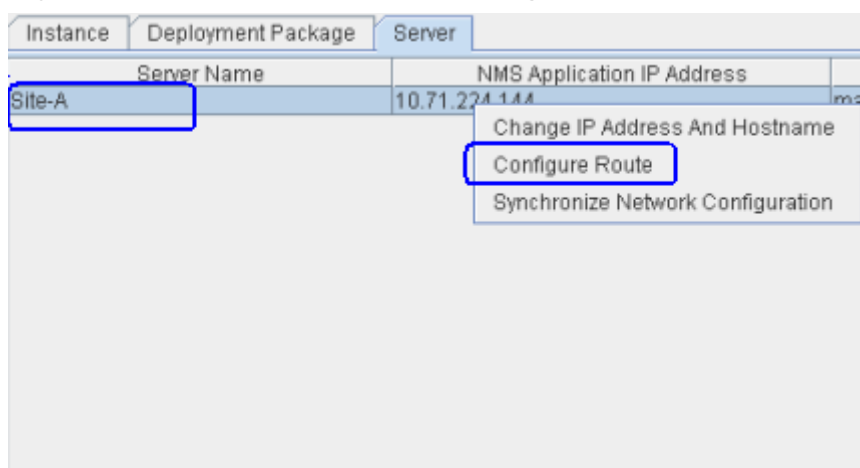
- Resources whose icons are grayed out are in the **offline** state. For example, the **NMSServer** resource in the preceding figure. Resources whose resource icons are not grayed out are in the **online** state. For example, the **BackupServer** resource in the preceding figure.
- Check the status of 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.



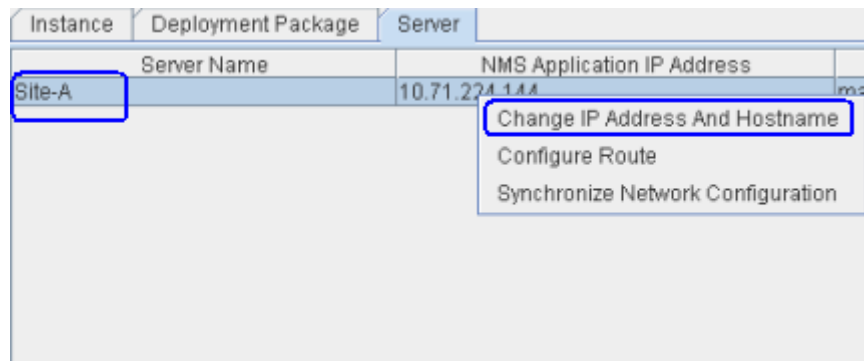
- In the dialog box that is displayed, click **Add** or **Delete** according to actual route conditions to re-configure the route.

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

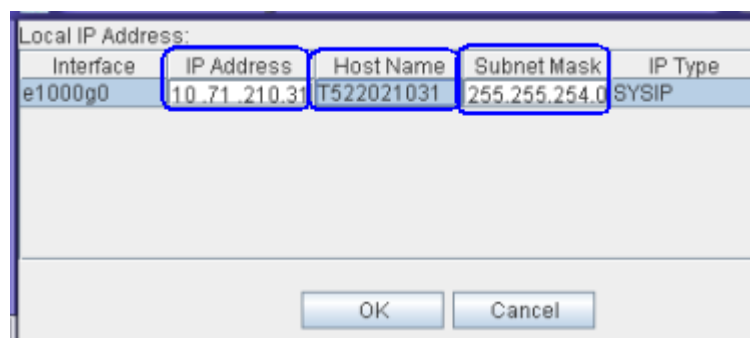
- Click **OK**.

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.



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**.
- 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 [C.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

## 11.8 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:

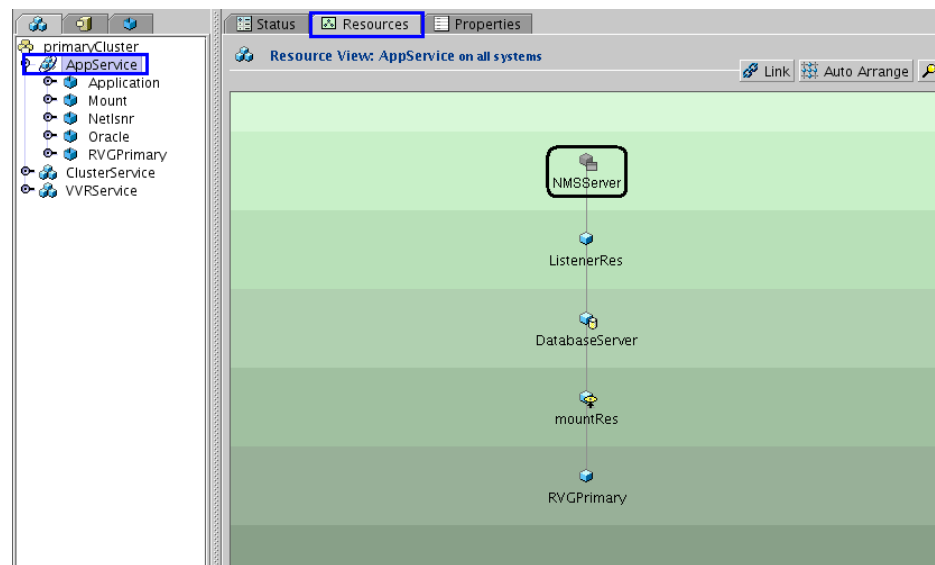
1. Use the MSuite to separate the primary site from the secondary site.
2. Log in to a VCS client and ensure that the **NMSServer** resource is in **offline** state and other resources are in **online** state on the primary site.
3. Use the MSuite to change the IP address and host name for the primary 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 [C.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.

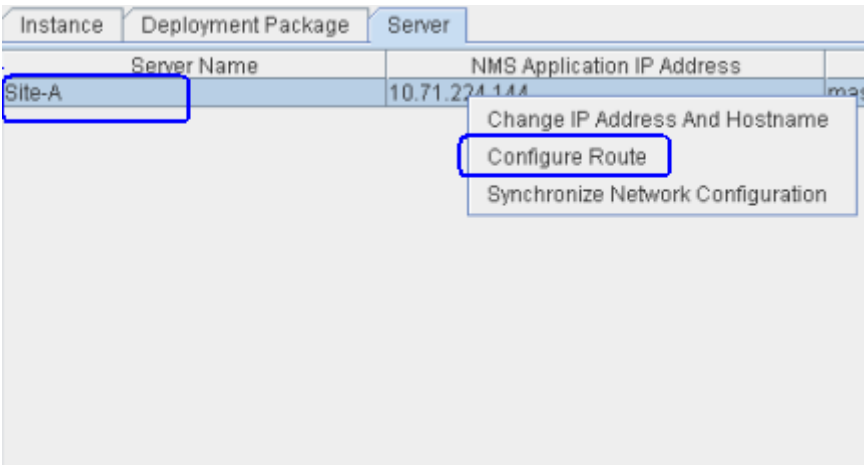
**Figure 11-3** High Availability System (SUSE Linux-Distributed) resources**NOTE**

- 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.
- 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

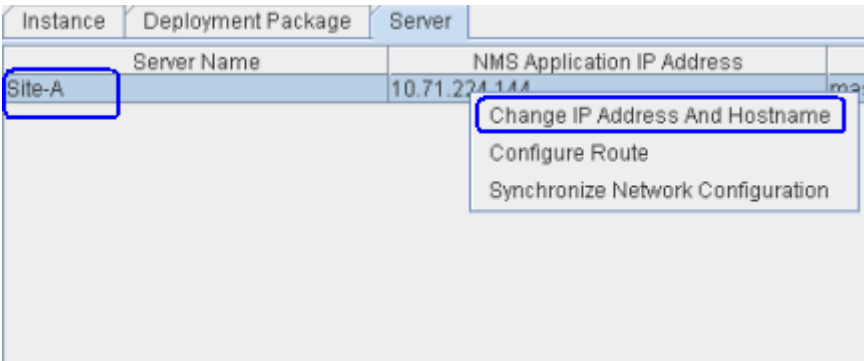
Add

Delete

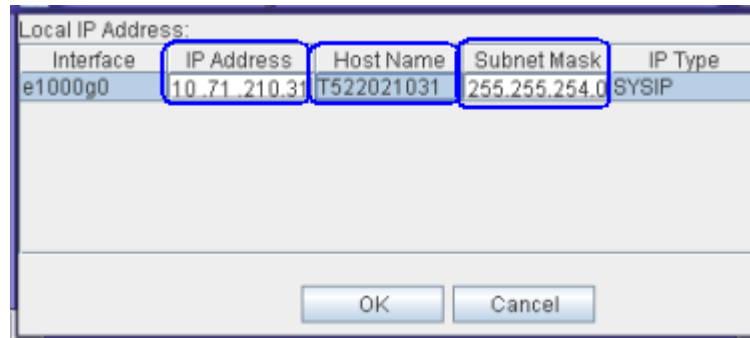
3. Click **OK**.

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.

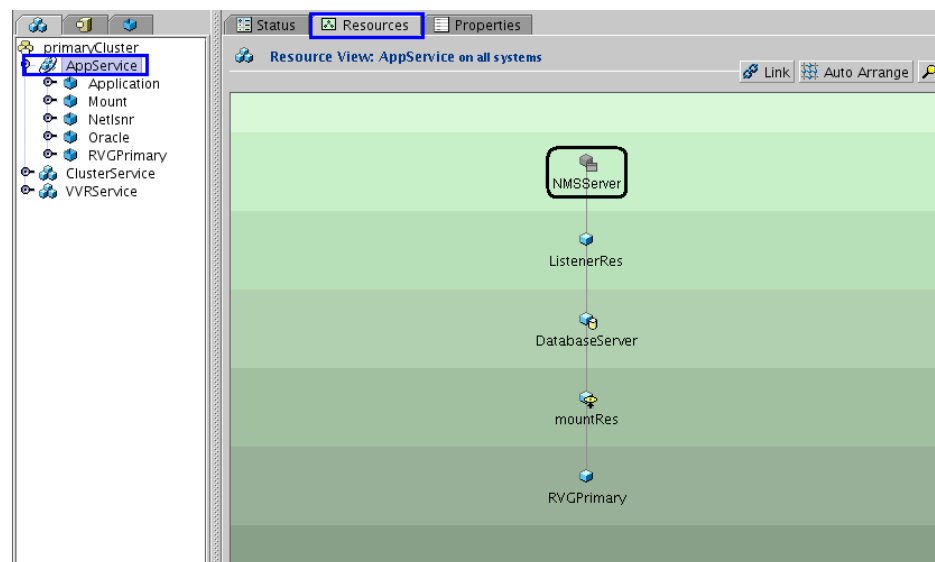


2. In the **Change IP Address And Hostname** dialog box, enter the new host name, IP address, and subnet mask.



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
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 11-4** 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**

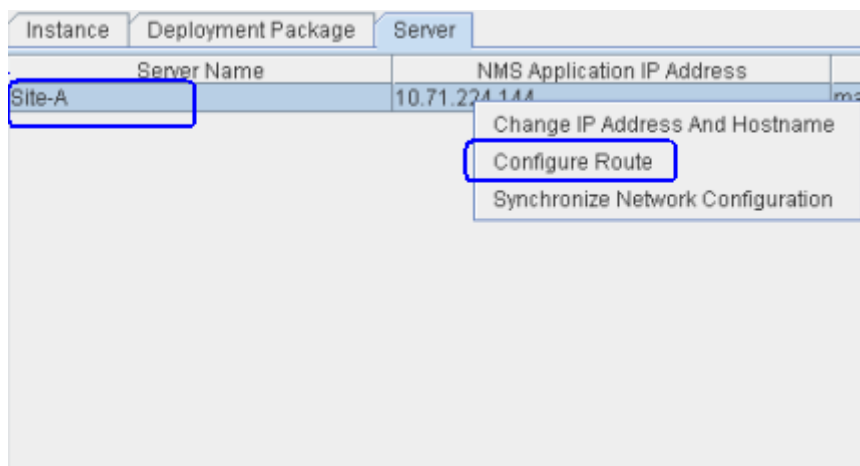
There must be a space between the dot (.) and **svc\_profile.sh**.

- 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.



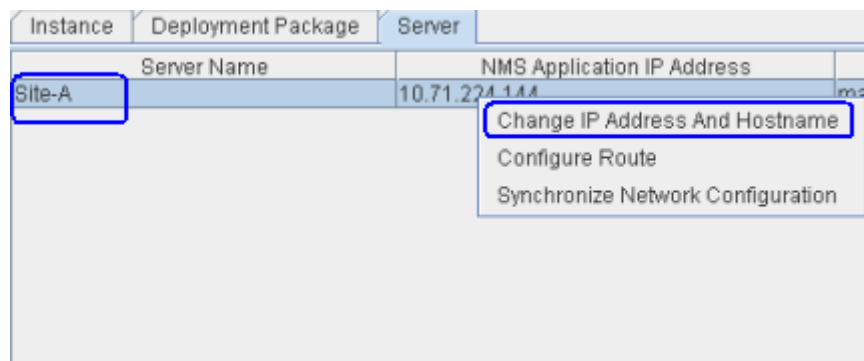
- In the dialog box that is displayed, click **Add** or **Delete** according to actual route conditions to re-configure the route.

| 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 [C.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.9.28 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 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?

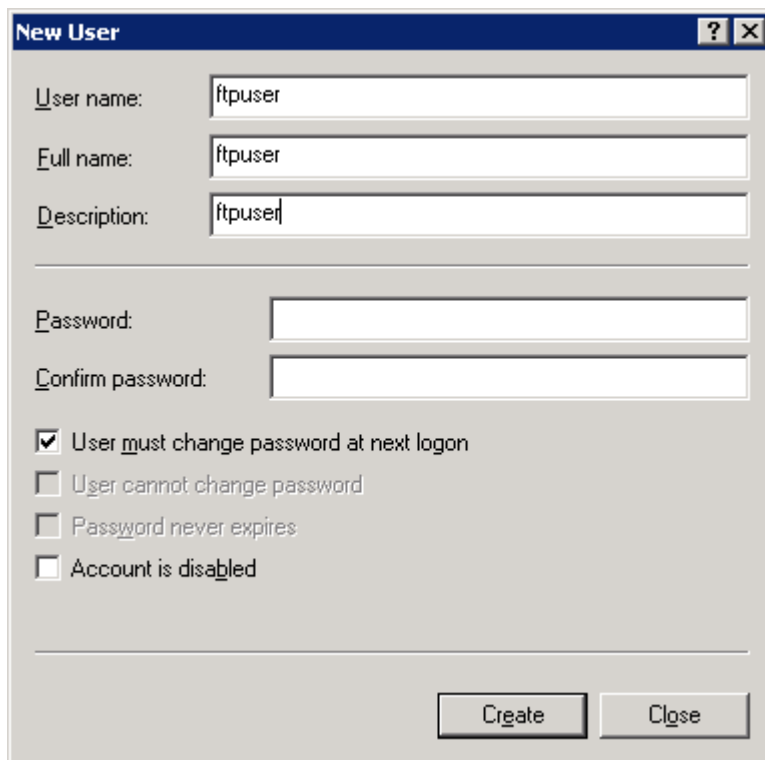


#### NOTE

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

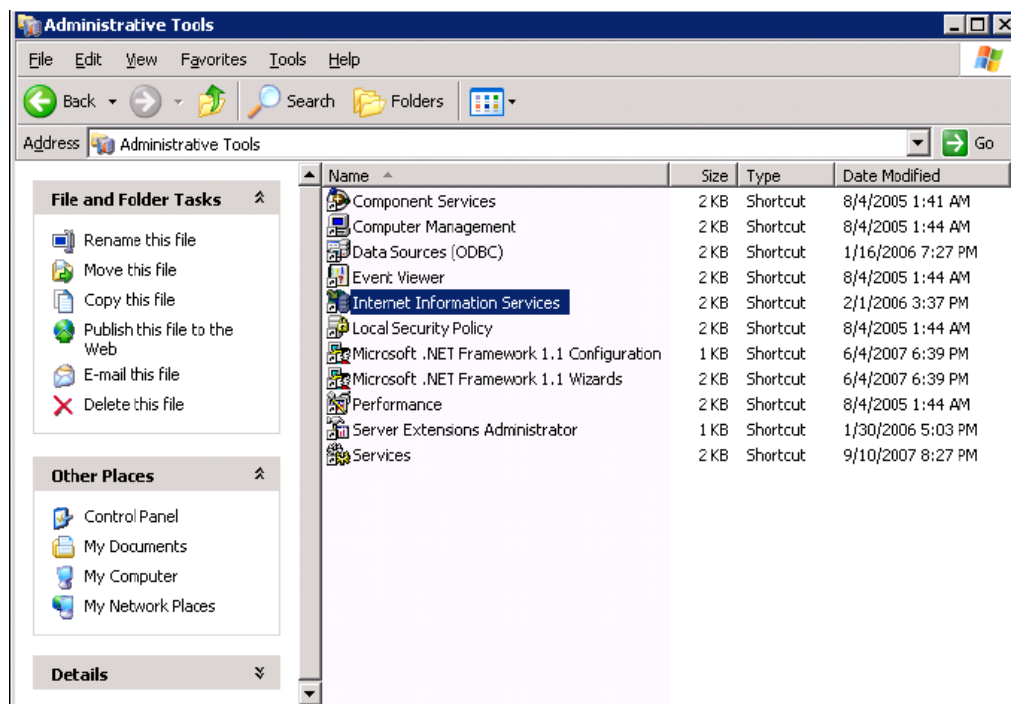
☐ User cannot change password

☐ Password never expires

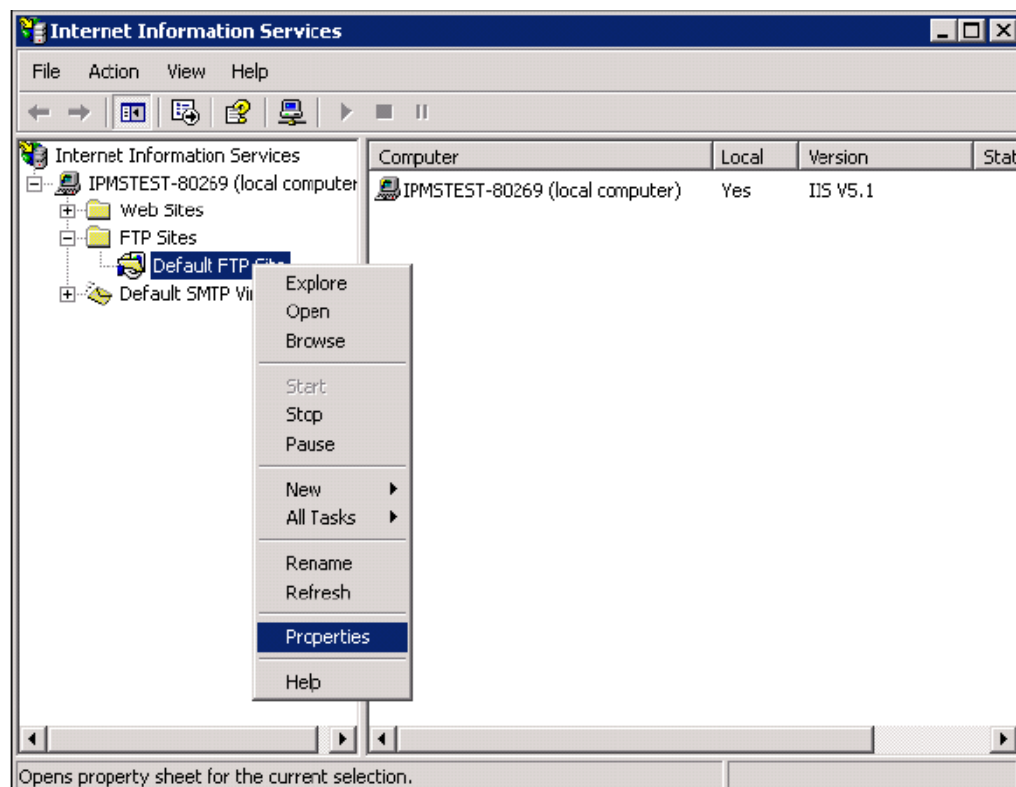
☐ Account is disabled

Create Close

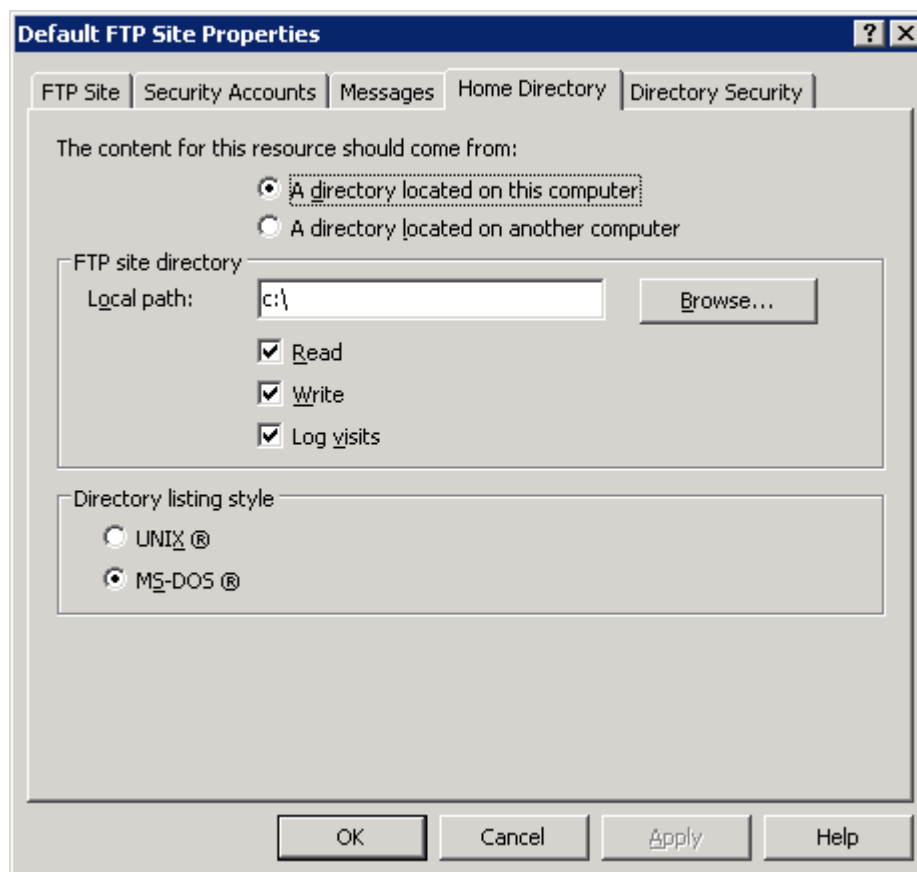
- 5 Enter the **User name** and the **Password**, click **Create** to create the **FTP** user account.
- 6 Click **Start > Settings > Control Panel**.
- 7 On the **Control Panel** window, double click **Add or Remove Programs** to display the **Add or Remove Programs** dialog box.
- 8 Click **Add/Remove 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

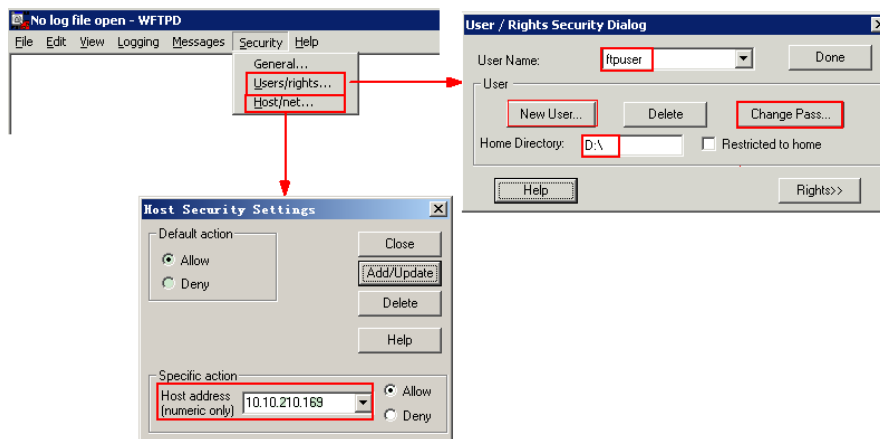
How do I configure the FTP, SFTP, or TFTP service on Windows OS?

#### NOTE

The third-party tool must be started after the FTP, SFTP, or TFTP server is configured.

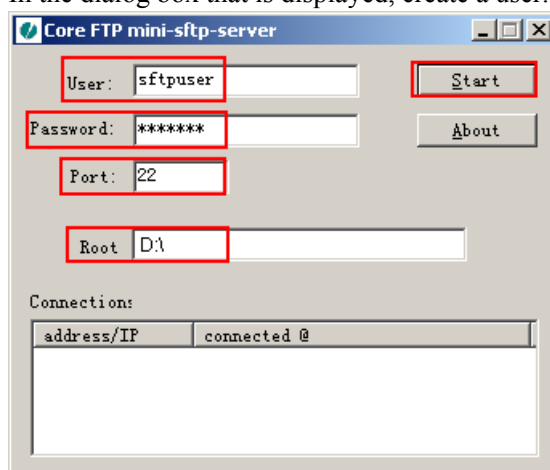
### Answer

- **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.



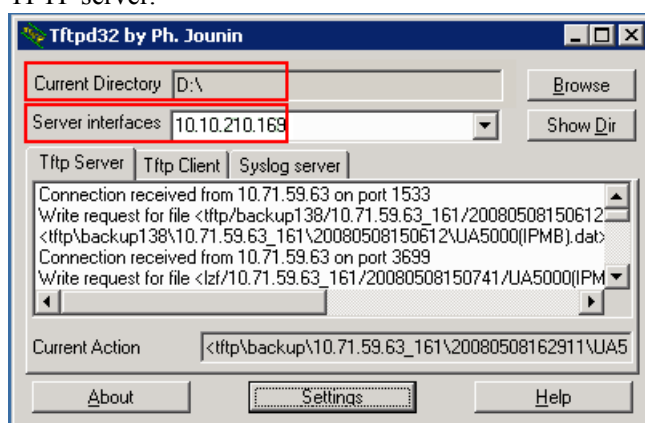
- **Configuring the SFTP server using the third-party tool msftpsrvr.exe**

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

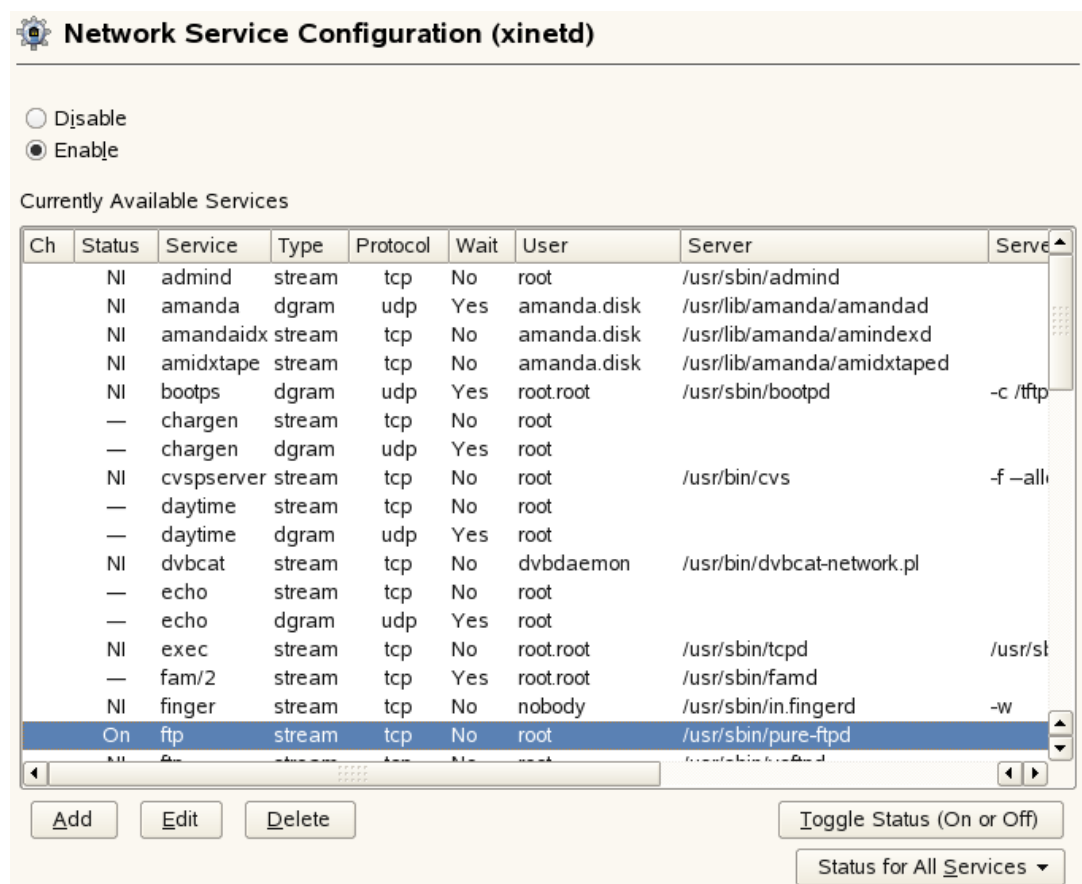
How to start/stop the FTP, TFTP, SFTP, and Telnet services in the SUSE Linux OS?

## 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 **ftputers** file in the **/etc** directory. Add the comment tag (#) to the beginning of the following line in the **ftputers** file to comment out this line:

```
root
```
  3. Run the command **wq!** to save and close the **ftputers** 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 **ftputers** file in the **/etc** directory. delete the comment tag (#) to the beginning of the following line in the **ftputers** file:

```
root
```
  3. Run the command **wq!** to save and close the **ftputers** 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                                                                 |
|------------|--------------------------------------------------------------------------|
| <b>ESC</b> | Press <b>ESC</b> 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                                                                                     |
|----------|----------------------------------------------------------------------------------------------|
| <b>a</b> | Appends text at the cursor (append).                                                         |
| <b>A</b> | Appends text at the end of the line where the cursor locates.                                |
| <b>i</b> | Adds text in front of the cursor (insert).                                                   |
| <b>I</b> | Adds text to the front of the first non-null character in the line where the cursor locates. |
| <b>o</b> | Adds text at the beginning of the next line where the cursor locates (open).                 |
| <b>O</b> | 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                                                                                         |
|----------------------|--------------------------------------------------------------------------------------------------|
| <b>h</b>             | Moves the cursor to the left.                                                                    |
| <b>j</b>             | Moves the cursor downwards.                                                                      |
| <b>k</b>             | Moves the cursor upwards.                                                                        |
| <b>l</b>             | Moves the cursor to the right.                                                                   |
| <b>Line number G</b> | Moves the cursor to a specified line. For example, <b>1G</b> moves the cursor to the first line. |
| <b>G</b>             | 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                                           |
|----------|----------------------------------------------------|
| <b>x</b> | Deletes the character where the cursor is located. |



| Command   | Function                                      |
|-----------|-----------------------------------------------|
| <b>dd</b> | 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                                             |
|------------|------------------------------------------------------|
| <b>:wq</b> | Saves changes and quits the vi editor.               |
| <b>:q</b>  | Quits the vi editor without saving changes.          |
| <b>:q!</b> | Forcibly quits the vi editor without saving changes. |
| <b>:w</b>  | Saves changes without quitting the vi editor.        |

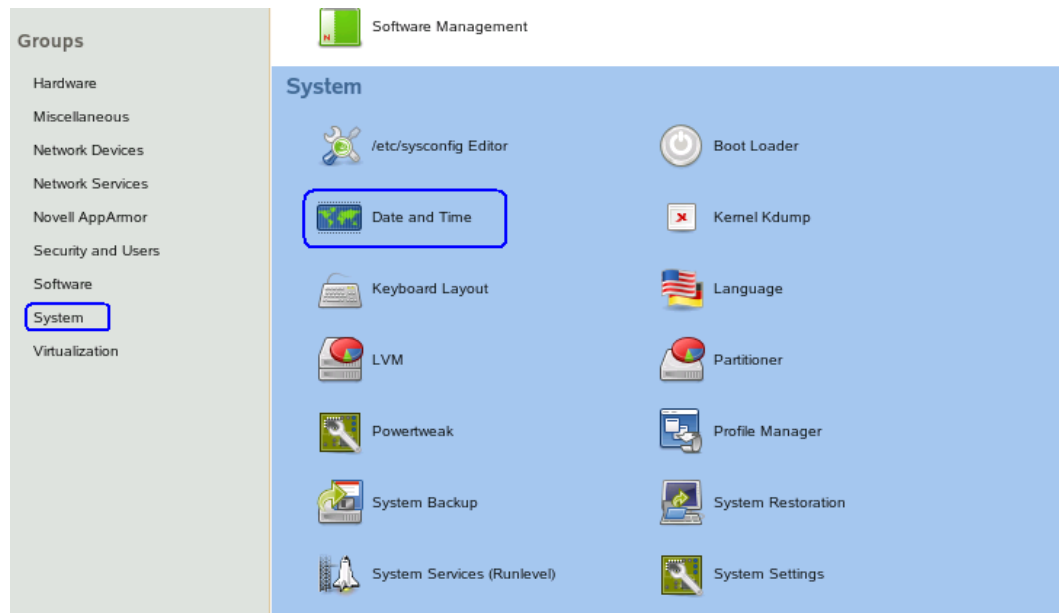
## A.2.9 How to Change the Time and Time Zone of the SUSE Linux OS?

### Question

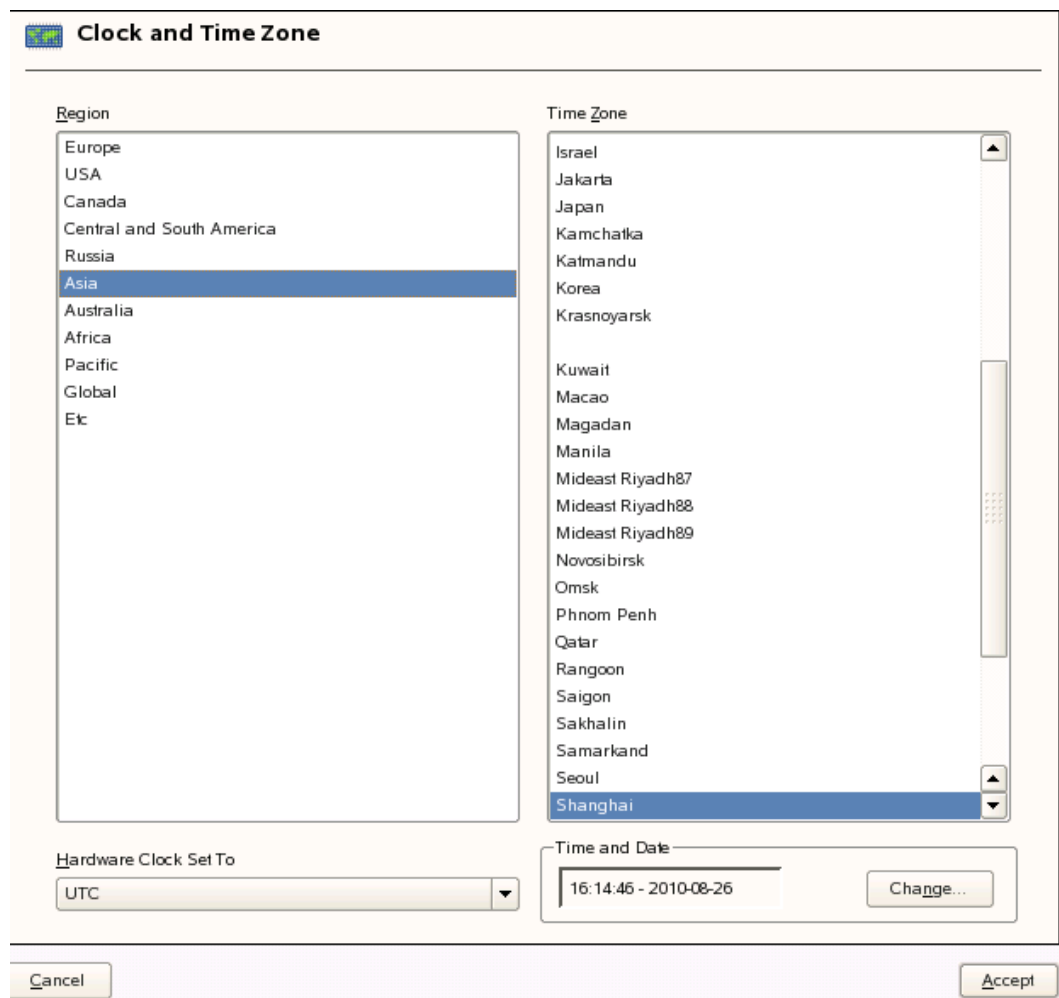
How to change the time and time zone of a SUSE Linux OS where the U2000 is not installed yet?

### 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:

```
svcadm enable ftp
```

- Starting the TFTP service

1. Log in to Solaris OS as user **root**.
2. Run the following command to verify that the TFTP service is running:

```
svcs -a|grep tftp
```

The TFTP service is not started if there is no response.

3. Run the following command to modify the **inetd** configuration file:

```
vi /etc/inetd.conf
```

Delete # to the left of TFTP.D.

4. Run the following command to start the TFTP service:

```
/usr/sbin/inetconv -i /etc/inetd.conf
```

```
svcadm enable svc:/network/tftp/udp6:default
```

5. Run the following command to verify that the TFTP service is running:

```
svcs -a|grep tftp
```

The TFTP service is running if a message is displayed:

```
online 22:07:11 svc:/network/tftp/udp6:default
```

- Starting the SFTP service

1. Log in to Solaris OS as user **root**.
2. Run the following command to start the SFTP service:

```
vi /etc/ssh/sshd config
```

Modify the "PAMAuthenticationViaKBDInt yes" to "PAMAuthenticationViaKBDInt no", and run the **:wq!** command to save the settings and exit.

```
svcadm restart network/ssh
```

```
svcadm enable network/ssh
```

- Starting the Telnet service

1. Log in to Solaris OS as user **root**.
2. Run the following command to start the Telnet service:

```
svcadm enable telnet
```

- Stop the FTP, TFTP, SFTP, and Telnet services as follows:

- Stopping the FTP service

1. Log in to Solaris OS as user **root**.
2. Run the following command to stop the FTP service:

```
svcadm disable ftp
```

- Stopping the TFTP service

1. Log in to Solaris OS as user **root**.
2. Run the following command to verify that the TFTP service is stopped:

```
svcs -a|grep tftp
```

The TFTP service is running if a message similar to the following is displayed:

```
online 22:07:11 svc:/network/tftp/udp6:default
```

3. Run the following command to modify the **inetd** configuration file:  
`# vi /etc/inetd.conf`  
 Add # to the left of TFTPd.
4. Run the following command to verify that the TFTP service is stopped:  
`# svcs -a|grep tftp`  
 If there is no response, the TFTP service is stopped.
- Stopping the SFTP service
  1. Log in to Solaris OS as user **root**.
  2. Run the following command to stop the SFTP service:  
`# svcadm disable network/ssh`
- Stopping the Telnet service
  1. Log in to Solaris OS as user **root**.
  2. Run the following command to stop the Telnet service:  
`# svcadm disable telnet`

### 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<br>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\$<br>Size | CPU<br>Implementation | CPU<br>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@0,0/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:

```
gzcata 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                                                                 |
|------------|--------------------------------------------------------------------------|
| <b>ESC</b> | Press <b>ESC</b> 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                                                                                     |
|----------|----------------------------------------------------------------------------------------------|
| <b>a</b> | Appends text at the cursor (append).                                                         |
| <b>A</b> | Appends text at the end of the line where the cursor locates.                                |
| <b>i</b> | Adds text in front of the cursor (insert).                                                   |
| <b>I</b> | Adds text to the front of the first non-null character in the line where the cursor locates. |
| <b>o</b> | Adds text at the beginning of the next line where the cursor locates (open).                 |
| <b>O</b> | 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                                                                                         |
|----------------------|--------------------------------------------------------------------------------------------------|
| <b>h</b>             | Moves the cursor to the left.                                                                    |
| <b>j</b>             | Moves the cursor downwards.                                                                      |
| <b>k</b>             | Moves the cursor upwards.                                                                        |
| <b>l</b>             | Moves the cursor to the right.                                                                   |
| <b>Line number G</b> | Moves the cursor to a specified line. For example, <b>1G</b> moves the cursor to the first line. |
| <b>G</b>             | 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                                           |
|-----------|----------------------------------------------------|
| <b>x</b>  | Deletes the character where the cursor is located. |
| <b>dd</b> | 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                                             |
|------------|------------------------------------------------------|
| <b>:wq</b> | Saves changes and quits the vi editor.               |
| <b>:q</b>  | Quits the vi editor without saving changes.          |
| <b>:q!</b> | Forcibly quits the vi editor without saving changes. |
| <b>:w</b>  | 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: <ul style="list-style-type: none"><li>● <b>state</b> is <b>ACTIVE</b>.</li><li>● <b>kernel</b> is <b>ENABLED</b>.</li></ul>                     |
| assoc    | Indicates the association relationship of the disk volume. <ul style="list-style-type: none"><li>● <b>rvg</b> indicates the RVG of the disk volume.</li><li>● <b>plexes</b> indicates the plexes contained by the disk volume.</li></ul> |
| 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, <b>type</b> 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

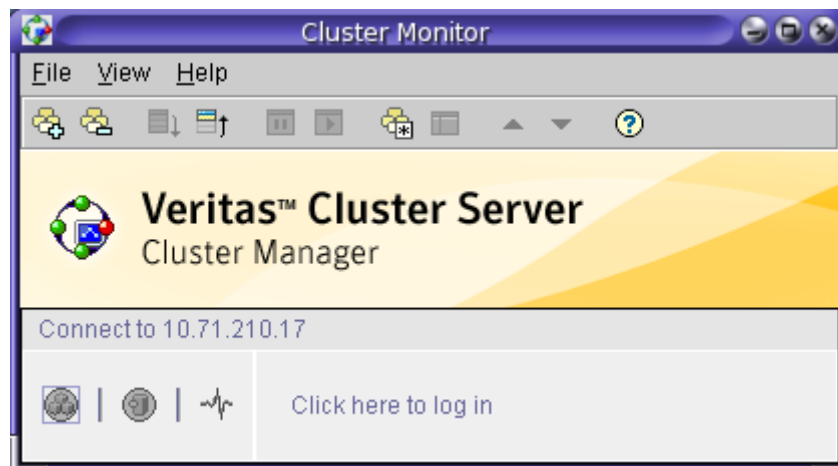
### 1 Log in to the VCS.

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.

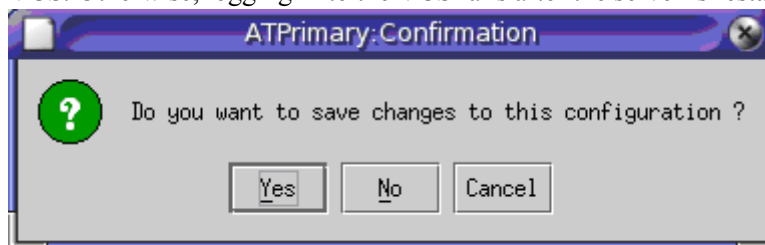
4. Click **OK**.

### 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: <ul style="list-style-type: none"><li>● <b>state</b> is set to <b>ACTIVE</b>.</li><li>● <b>kernel</b> is set to <b>ENABLED</b>.</li></ul>                                                                                                  |
| assoc  | Indicates the association information about the RVG. <ul style="list-style-type: none"><li>● <b>datavols</b> indicates the data disk volume that the RVG contains.</li><li>● <b>srl</b> indicates the SRLog disk volume that the RVG contains.</li><li>● <b>rlinks</b> indicates the RLink that the RVG contains.</li></ul> |
| att    | Indicates the activated Rlink of the RVG.                                                                                                                                                                                                                                                                                   |
| flags  | Indicates the flag of the RVG. In normal cases, the value is <b>closed primary enabled attached</b> .                                                                                                                                                                                                                       |
| 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 -VI**

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: <ul style="list-style-type: none"> <li>● <b>state</b> is set to <b>ACTIVE</b>.</li> <li>● <b>kernel</b> is set to <b>ENABLED</b>.</li> </ul>                                                                                                   |
| assoc      | Indicates the association information about the RVG. <ul style="list-style-type: none"> <li>● <b>datavols</b> indicates the data disk volume that the RVG contains.</li> <li>● <b>srl</b> indicates the SRLog disk volume that the RVG contains.</li> <li>● <b>rlinks</b> indicates the Rlink that the RVG contains.</li> </ul> |
| att        | Indicates the activated Rlink of the RVG.                                                                                                                                                                                                                                                                                       |
| flags      | Indicates the flag of the RVG. In normal cases, the value is <b>primary enabled attached clustered</b> .                                                                                                                                                                                                                        |

- 2 Run the following command to view the RVG status on the secondary site:

**vxprint -VI**

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 <rlinkName>
```

For example, run the following command to query the status of **datarlk**:

```
vxprint -Pl datarlk
```

A message similar to the following will be displayed:

```
Disk group: datadg

Rlink: datarlk
info: timeout=500 rid=0.1414
 latency_high_mark=10000 latency_low_mark=9950
 bandwidth_limit=none checksum=on
state: state=ACTIVE
 synchronous=off latencyprot=off srlprot=autodcm
assoc: rvg=datarvg
 remote_host=192.168.1.11 IP_addr=192.168.1.11 port=4145
 remote_dg=datadg
 remote_dg_dgid=1160936796.6.T522022456
 remote_rvg_version=30
 remote_rlink=datarlk
 remote_rlink_rid=0.1405
 local_host=192.168.1.10 IP_addr=192.168.1.10 port=4145
protocol: UDP/IP
flags: write enabled attached consistent connected asynchronous
```

[Table 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. <ul style="list-style-type: none"> <li>● <b>timeout</b> indicates the timeout period.</li> <li>● <b>rid</b> indicates the ID of the Rlink.</li> <li>● <b>latency_high_mark</b> indicates the highest delay flag.</li> <li>● <b>latency_low_mark</b> indicates the lowest delay flag.</li> <li>● <b>bandwidth_limit</b> indicates the bandwidth limit.</li> </ul> |                                               |
| state    | Indicates the status of the Rlink. In normal cases, the situations are as follows: <ul style="list-style-type: none"> <li>● <b>state</b> is set to <b>ACTIVE</b>.</li> <li>● <b>synchronous</b> is set to <b>off</b>.</li> <li>● <b>latencyprot</b> is set to <b>off</b>.</li> <li>● <b>srlprot</b> is set to <b>autodem</b>.</li> </ul>                                                                    |                                               |
| 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 <b>write enabled attached consistent connected asynchronous</b> .                                                                                                                                                                                                                                                                                   |                                               |

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. <ul style="list-style-type: none"> <li>● <b>timeout</b> indicates the timeout period.</li> <li>● <b>latency_high_mark</b> indicates the highest delay flag.</li> <li>● <b>latency_low_mark</b> indicates the lowest delay flag.</li> <li>● <b>bandwidth_limit</b> indicates the bandwidth limit.</li> </ul> |                                               |
| state    | Indicates the status of the Rlink. In normal cases, the situations are as follows: <ul style="list-style-type: none"> <li>● <b>state</b> is set to <b>ACTIVE</b>.</li> <li>● <b>synchronous</b> is set to <b>override</b>.</li> <li>● <b>latencyprot</b> is set to <b>off</b>.</li> <li>● <b>srlprot</b> is set to <b>autodcm</b>.</li> </ul>          |                                               |
| 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 <b>write attached consistent connected</b> .                                                                                                                                                                                                                                                   |                                               |

## 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 # **vxdg 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

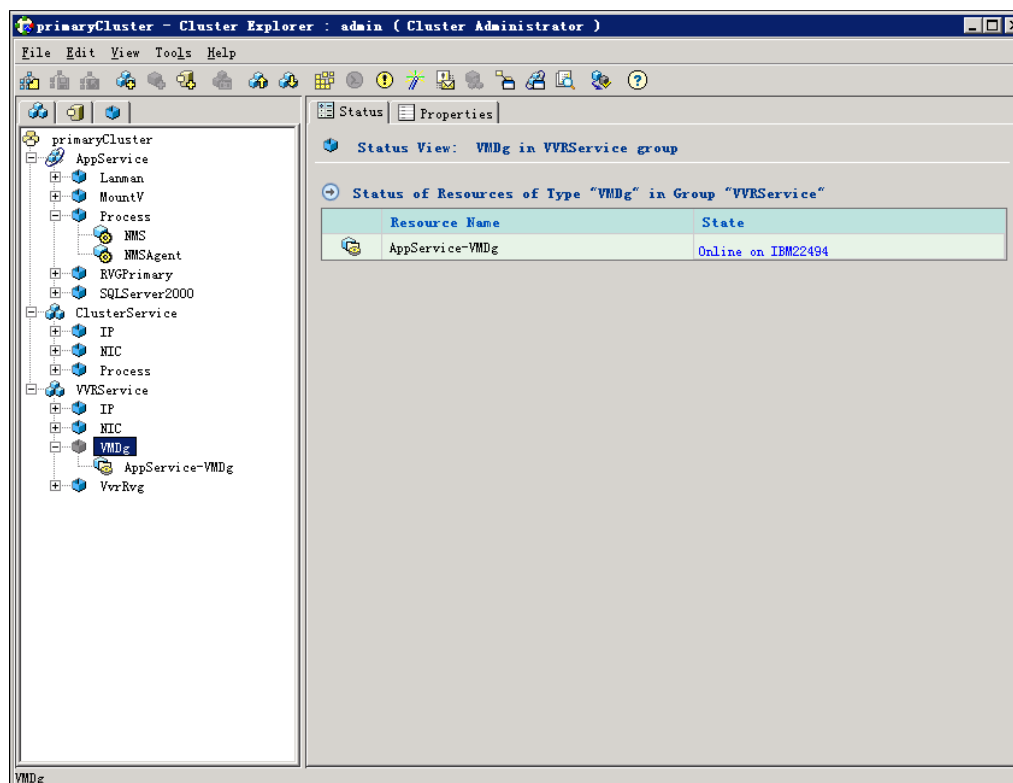
#### A.4.3.14 How to Solve the Problem That the VMDg Node Icon Becomes Grayed out After the High Availability System Is Established (Windows HA System)

##### 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

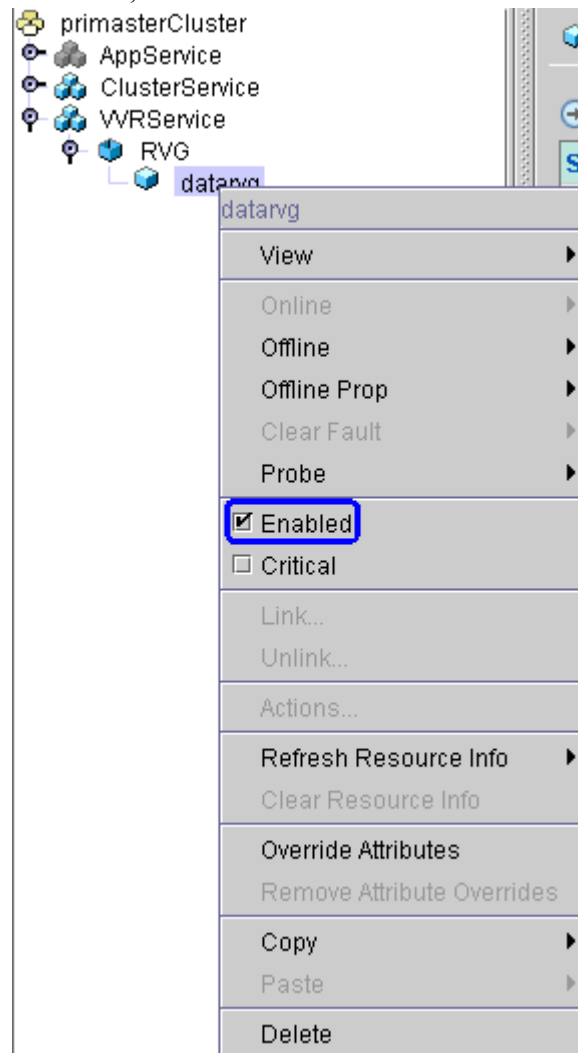
How to start/stop the NMS before synchronizing the primary and secondary sites of a high availability system?

##### 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.

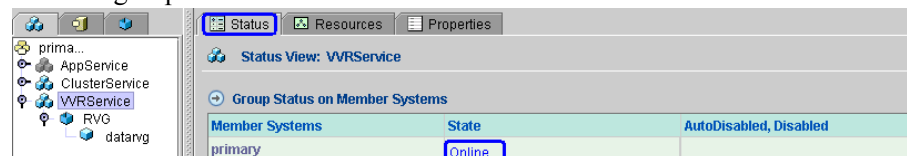
Right-click the datarvg resource and check whether the **Enabled** option is selected. If this option is checked, it has been enabled.



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.



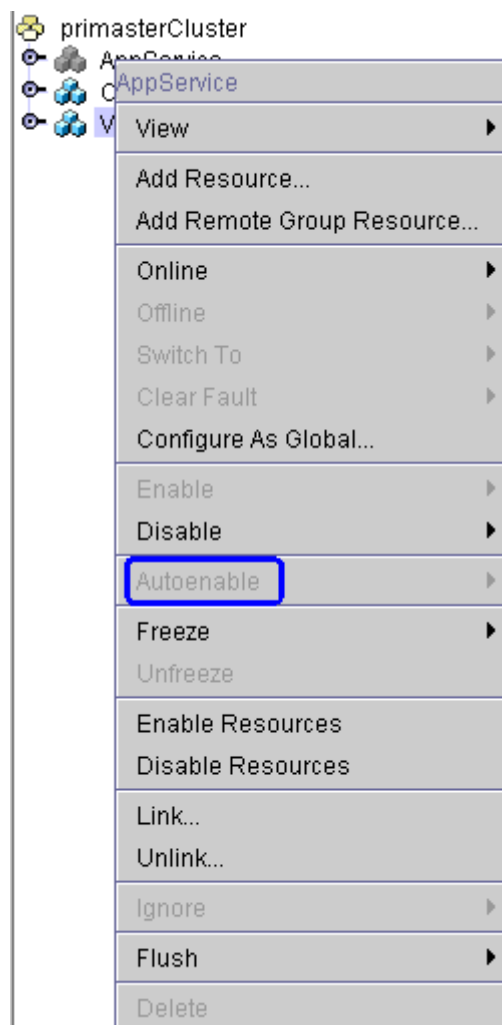
If the VVRService resource group has not been started, do as follows to start it:

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.

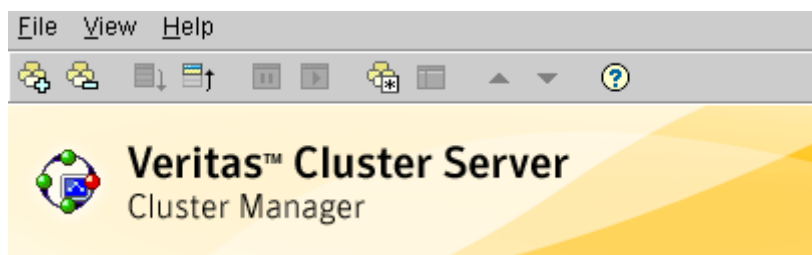
- 2 Click **Stop**.

- 3 Click **Yes**.

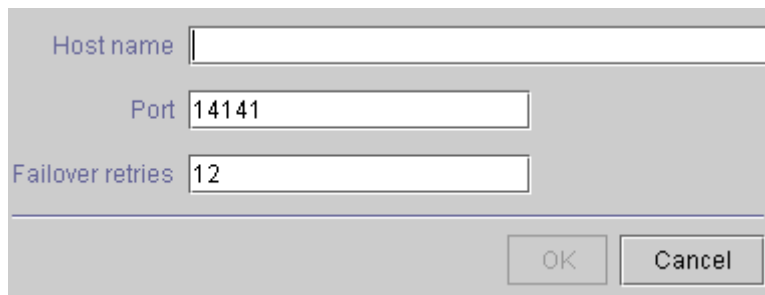
- 4 In the high availability system, log in to the OS as the user who has administrator rights.

- 5 Start the VCS client.

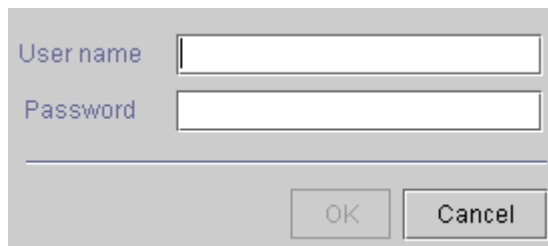
1. Choose **Start > Programs > Symantec > Veritas Cluster Server > Veritas Cluster Manager - Java Console** to start the VCS client.



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**

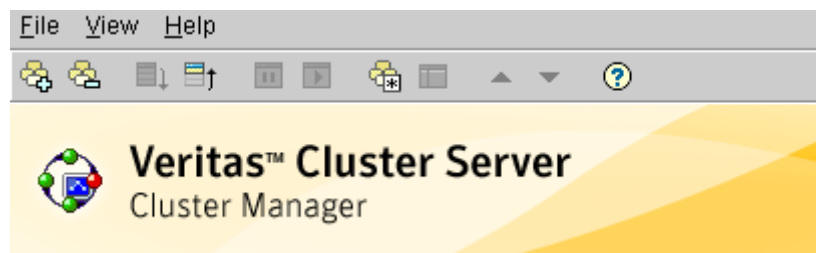
In normal cases, the SQL server database of the primary site are started but those of the secondary site are not started.

### Answer

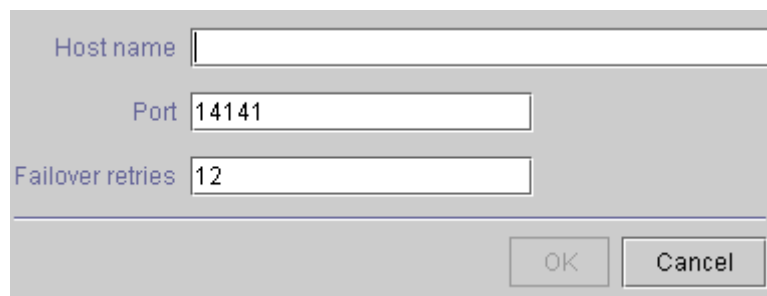
- 1 In the single-server system, choose **Start > Programs > Microsoft SQL Server > Service Manager**.

The **SQL Server Service Manager** dialog box is displayed.

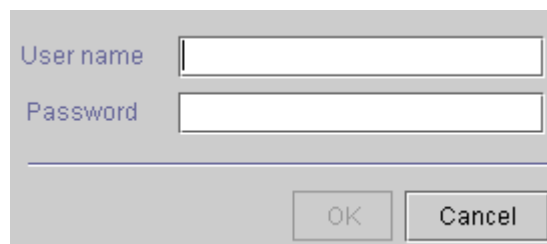
- 2 Click **Start/Continue**.
- 3 In the high availability system, log in to the OS as the user who has administrator rights.
- 4 Start the VCS client.
  1. Choose **Start > Programs > Symantec > Veritas Cluster Server > Veritas Cluster Manager - Java Console** to start the VCS client.



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 Check the Sybase Database Version](#)

[A.6.2.2 How to View the Server Name of the Sybase Database](#)

[A.6.2.3 How to Change the Password of User sa for the Sybase Database](#)



- [A.6.2.4 How to Clear the Password of the Sybase Database](#)
- [A.6.2.5 How to View the Bit Number of the Sybase Database](#)
- [A.6.2.6 How to View the Details of the Sybase Database](#)
- [A.6.2.7 How to View Data Tables](#)
- [A.6.2.8 How to Query a Database Table if Only Part of the Table Name Is Remembered](#)
- [A.6.2.9 How to Identify Database Errors Caused by Unexpected Powering-Off of the Workstation](#)
- [A.6.2.10 How to Expand Space for the master Database](#)
- [A.6.2.11 How to Set Up More User Connections to a Database](#)
- [A.6.2.12 How to Check for Database Errors Using the dbcc Tool](#)
- [A.6.2.13 How to Set the Network Transport Parameters of Databases](#)
- [A.6.2.14 How to Delete a Suspect Database](#)
- [A.6.2.15 How to Delete a Damaged User Database](#)
- [A.6.2.16 How to Delete a Database from the Sybase Database?](#)
- [A.6.2.17 How to View the Deadlock Information in the Database](#)

## A.6.2.1 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.6.2.2 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.6.2.3 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:

```
hagai &
```

In the **Cluster Monitor** window, click a server record in the information list.

In the login dialog box that is displayed, enter the user name and password of the VCS. Click **OK** to log in to the VCS client. The default user name and password of the VCS are **admin** and **password**.

Right-click **NMSServer** and choose **Offline > Host name** from the shortcut menu.

In the confirmation dialog box, click **Yes**.

#### NOTE

Ensure that the database is running.

- 2 Log in to the network management maintenance suite (MSuite) client.
  1. On the computer where the MSuite client is installed, double-click the **U2000 MSuite** shortcut icon on the desktop. Wait about one minute. The **Login** dialog box is displayed.
  2. Set the login parameters and click **OK**. The **NMS maintenance suite** window will be displayed.
    - IP Address: Indicates the system IP address of the computer where the MSuite server is installed.
    - Port No.: The default port ID is **12212**. There is no need to change the default value during login.
    - User Name and Password: The default user name and password are **admin**.
- 3 On the MSuite client, choose **Deploy > Change Database Administrator Password**. The **Change Database Administrator Password** dialog box is displayed.
- 4 Enter the old password and new password.

#### NOTE

A password must be 6-30 characters long and consists of letters or digits. Special characters are not allowed.

- 5 Click **OK**. The password is changed.

----End

### A.6.2.4 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.6.2.5 How to View the Bit Number of the Sybase Database

#### Question

How do I view the bit number of the Sybase database?

#### Answer

- 1 Run the following commands to view the bit number of the Sybase database:

```
cd /opt/sybase/OCS*/bin
```

```
./isql -SDBSVR -Usa -Pchangeme
```

```
1>select @@version
```

```
2>go
```

#### NOTE

- In the `./isql -SDBSVR -Usa -Pchangeme` command, *changeme* is the password of user **sa** of the Sybase database.
- There must be a space between **select** and **@** in the **select @@version** command.

The following message will be displayed:

```
Adaptive Server Enterprise/12.5.3/EBF 13325 ESD#5/P/Sun_svr4/OS 5.8/ase1253/193
9/64-bit/FBO/Tue Dec 6 09:13:20 2005
```

64-bit indicates the bit number of the Sybase database.

----End

## A.6.2.6 How to View the Details of the Sybase Database

### Question

How do I view the details about the Sybase database during routine maintenance?

### Answer

- 1 Run the following commands to view the details of all databases:

```
cd /opt/sybase/OCS*/bin
./isql -SDBSVR -Usa -Pchangeme
1>sp_helpdb
2>go
```

 **NOTE**

In the `./isql -SDBSVR -Usa -Pchangeme` command, *changeme* is the password of user **sa** of the Sybase database.

The information about the Sybase database will be displayed, including the name, size, owner, and status.

- 2 Run the following commands to view the details of a specific database:

```
1>sp_helpdb database_name
2>go
```

 **NOTE**

In the `sp_helpdb database_name` command, *database\_name* is the name of the Sybase database.

Database space used can also be viewed.

----End

## A.6.2.7 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.6.2.8 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.6.2.9 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.6.2.10 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.6.2.11 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.6.2.12 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.6.2.13 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.

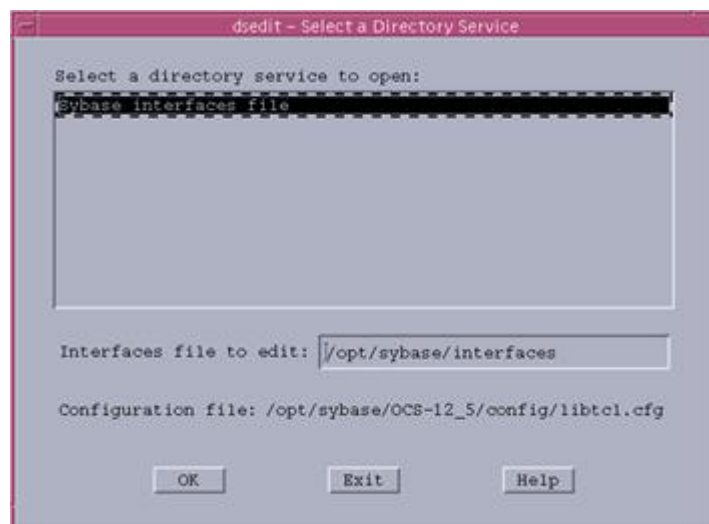
- 2 Log in to the server as user **root**. Open the terminal window and run the following commands:

```
./opt/sybase/SYBASE.sh
```

```
dsedit
```

- 3 In the dialog box as shown in [Figure A-2](#), click **OK**.

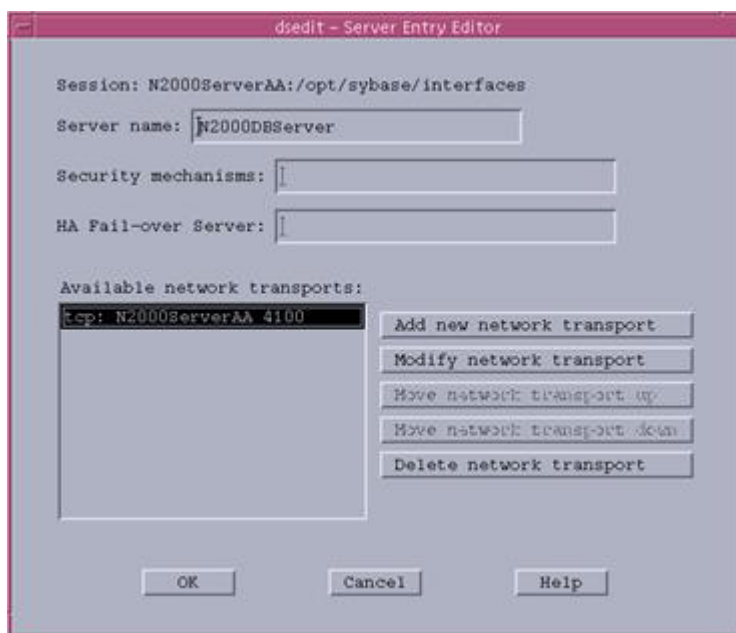
**Figure A-2** Selecting the service path



- 4 In the dialog box as shown in [Figure A-3](#), select **DBSVR** and click **Modify Server entry**.

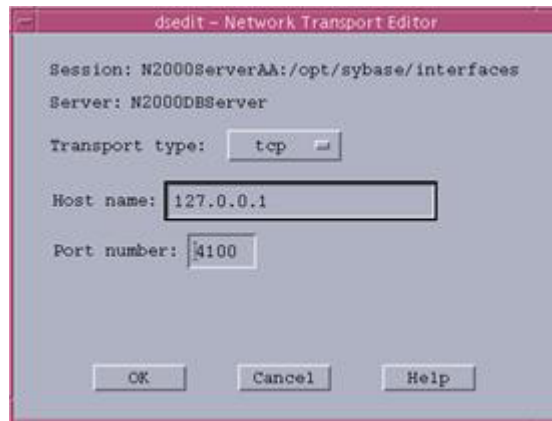
**Figure A-3** Selecting the database service

- 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.6.2.14 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.6.2.15 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:
- 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.6.2.16 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.6.2.17 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 the Version of the Oracle Database](#)

[A.7.2 How to Check the Name of the Oracle Database](#)

[A.7.3 How to Start the Oracle Database in the High Availability System](#)

[A.7.4 How Can I Start the Oracle Database \(Single-Server System\)?](#)

[A.7.5 How to Shut Down the Oracle Database \(High Availability System\)](#)

[A.7.6 How Can I Stop the Oracle Database \(Single-Server System\)?](#)

[A.7.7 How Can I Check Whether the Oracle Database Is Started?](#)

[A.7.8 How Can I Change the Password of an Oracle Database User?](#)

[A.7.9 How Can I Check Whether the Oracle Listener Is Started?](#)

### A.7.1 How to Check the Version of the Oracle Database

#### Question

How to check the version of the Oracle database?

#### Answer

See [A.7.7 How Can I Check Whether the Oracle Database Is Started?](#).

### A.7.2 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.7.3 How to Start the Oracle Database in the High Availability System

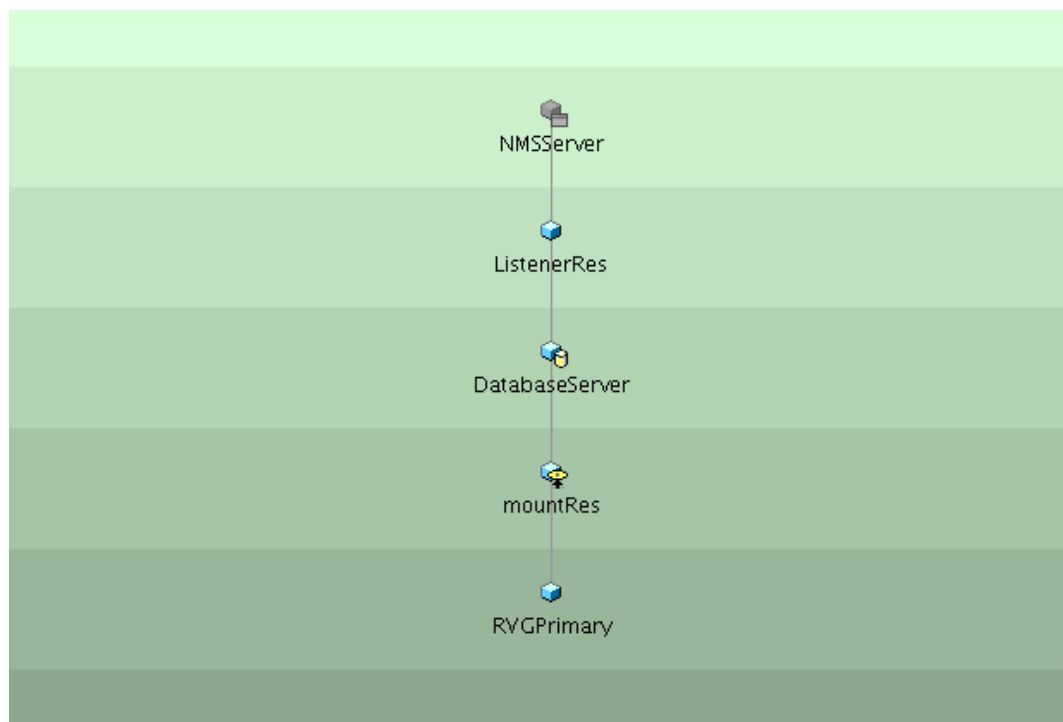
### Question

How do I start the Oracle database?

### Answer

- 1 Log in to the OS as user **root**.
- 2 Open the CLI.
- 3 To start the VCS client, run the following command:  

```
haGUI&
```
- 4 Choose **File > New Cluster**. Then, enter the server IP address and click **OK**.
- 5 Enter the default user name **admin** and default password **password** of the VCS client, and then click **OK**.
- 6 Select the **AppService** node. In the right-hand pane, click the **Resources** tab.
- 7 Right-click **ListenerRes** and choose **Online > host name** from the shortcut menu.  
Wait until information shown in the following figure is displayed indicating that the Oracle database is started.



----End

## A.7.4 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

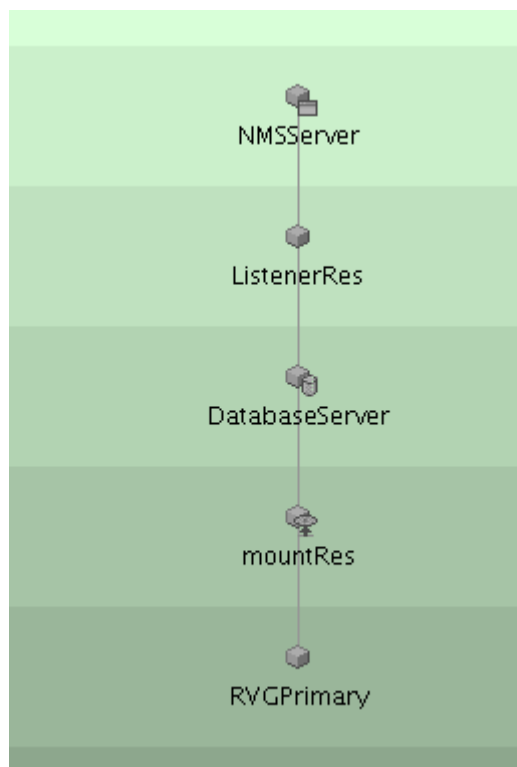
## A.7.5 How to Shut Down the Oracle Database (High Availability System)

### Question

How do I shut down the Oracle database?

### Answer

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



----End

## A.7.6 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.7.7 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.7.4 How Can I Start the Oracle Database \(Single-Server System\)?](#) to start the Oracle database. for HA system, see [A.7.3 How to Start the Oracle Database in the High Availability System](#) to start the Oracle database.

----End

## A.7.8 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.7.9 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 Change the System Time and Time Zone of the Single-Server System on Windows](#)
- [A.9.2 How to Change the System Time and Time Zone of the Single-Server System \(Solaris\)](#)
- [A.9.3 How to Change the System Time and Time Zone of the Single-Server System \(SUSE Linux-Distributed\)](#)
- [A.9.4 How to Change the System Time and Time Zone of the High Availability System on Windows](#)
- [A.9.5 How to Change the System Time and Time Zone of the High Availability System \(Solaris\)](#)
- [A.9.6 How to Change the System Time and Time Zone of the High Availability System \(SUSE Linux-Distributed\)](#)
- [A.9.7 How to Verify That the Processes of the U2000 Single-Server System Are Running on Windows](#)
- [A.9.8 How to Start the Processes of the U2000 Single-Server System on Windows](#)
- [A.9.9 How to End the Processes of the U2000 Single-Server System on Windows](#)
- [A.9.10 How to Verify That the Processes of the U2000 Single-Server System Are Running on Solaris](#)
- [A.9.11 How to Start the Processes of the U2000 Single-Server System on Solaris](#)
- [A.9.12 How to End the Processes of the U2000 Single-Server System on Solaris](#)
- [A.9.13 How to Verify That the Processes of the U2000 Single-Server System \(SUSE Linux-Distributed\) Are Running](#)
- [A.9.14 How to Start the Processes of the U2000 Single-Server System \(SUSE Linux-Distributed\)](#)
- [A.9.15 How to End the Processes of the U2000 Single-Server System \(SUSE Linux-Distributed\)](#)
- [A.9.16 How to Check Whether the U2000 Processes of the High Availability System \(Windows\) Are Started](#)
- [A.9.17 How to Start the U2000 Processes of the High Availability System \(Windows\)](#)
- [A.9.18 How to End the U2000 Processes of the High Availability System \(Windows\)](#)
- [A.9.19 How to Check Whether the U2000 Processes of the High Availability System \(Solaris\) Are Started](#)
- [A.9.20 How to Start the U2000 Processes of the High Availability System \(Solaris\)](#)
- [A.9.21 How to End the U2000 Processes of the High Availability System \(Solaris\)](#)
- [A.9.22 How to Check Whether the U2000 Processes of the High Availability System \(SUSE Linux-Distributed\) Are Started](#)
- [A.9.23 How to Start the U2000 Processes of the High Availability System \(SUSE Linux-Distributed\)](#)
- [A.9.24 How to End the U2000 Processes of the High Availability System \(SUSE Linux-Distributed\)](#)
- [A.9.25 What Factors Affect the Response Speed of the NMS](#)

- [A.9.26 How to Resolve the Problem Wherein Illegible Characters Occur in the NMS Window](#)
- [A.9.27 How to Add Components Incrementally](#)
- [A.9.28 How to Configure the ipmap.cfg Mapping File](#)
- [A.9.29 How to Check Whether the daem Process Is Started](#)
- [A.9.30 How to Start the daem Process](#)
- [A.9.31 How to End the daem Process](#)
- [A.9.32 How to Rectify the Application GUI Startup Failure Caused by User Switching](#)
- [A.9.33 How to Rectify the U2000 Startup Failure After the IP Address or Host Name of the Single-Server System \(Solaris\) Is Changed Manually](#)
- [A.9.34 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.9.35 How to View the U2000 and Sybase Database Installation Paths](#)
- [A.9.36 How to View Network Configurations for the Primary Site or Secondary Site Installed with a HA System](#)
- [A.9.37 How to Rectify the Mouse Detection Failure and Open the GUI After the T5220 Is Connected to the KVM](#)
- [A.9.38 How to Check Downloaded Software Packages by Using MD5 Software](#)
- [A.9.39 How to Rectify the Failure to Connect to the Sybase Database During U2000 Installation](#)
- [A.9.40 Reinstalling the U2000 on or Migrating the U2000 to Another Computer](#)
- [A.9.41 How to Set the Communication Mode on the U2000 server for the Single-Server System \(Windows\)](#)
- [A.9.42 How to Set the Communication Mode on the U2000 server for the Single-Server System \(Solaris\)](#)
- [A.9.43 How to Configure the Communication Mode for a Linux-based U2000 Server?](#)
- [A.9.44 How to Set the Communication Mode on the U2000 Server for the High Availability System \(Windows\)](#)
- [A.9.45 How to Set the Communication Mode of the Server in a High Availability System \(Solaris\)?](#)
- [A.9.46 How to Set the Communication Mode of the Server in a High Availability System \(SUSE Linux-Distributed\)](#)

## **A.9.1 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.9.2 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.9.3 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.9.4 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?



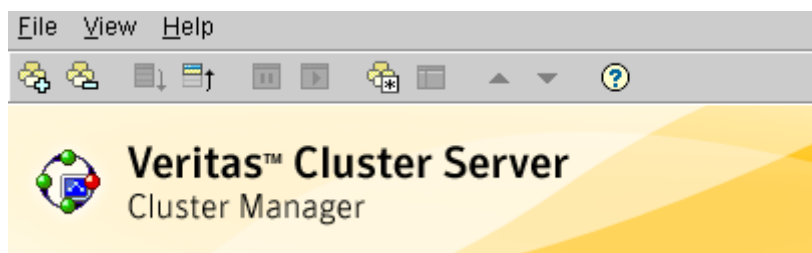
### CAUTION

When the U2000 services are running, do not change the system time.

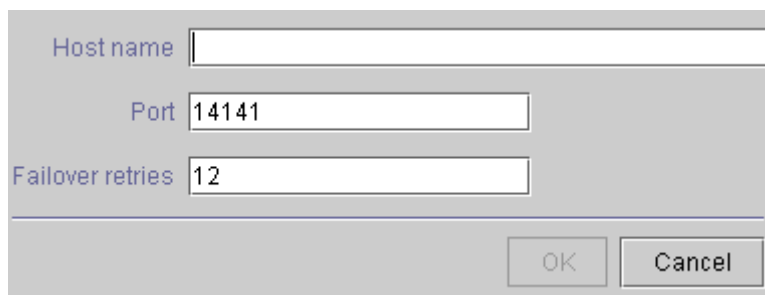
---

### Answer

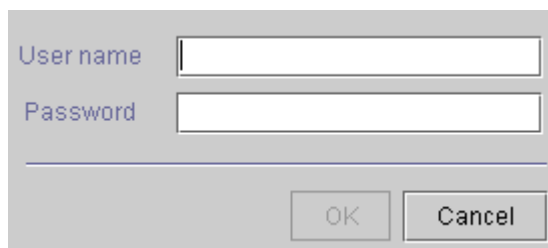
- 1 Stop the U2000 processes and the SQL Server database.
  1. Choose **Start > Programs > Symantec > Veritas Cluster Server > Veritas Cluster Manager - Java Console** to start the VCS client.



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.9.5 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:

```
hagrpf -offline AppService -sys host name of active site
```

For example, if the host name of the primary site is **Primaster**, run the # **hagrpf -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
hstop -all -force
sync;sync;sync;sync
shutdown -y -g0 -i6
```

#### 7 Log in to the MSuite client.



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.9.6 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:

```
hagr -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 **#hagr -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.



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.9.7 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.9.8 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.9.9 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.9.10 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.9.11 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.9.12 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.9.13 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/imapmb
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.9.14 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 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**

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.9.15 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.9.16 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?

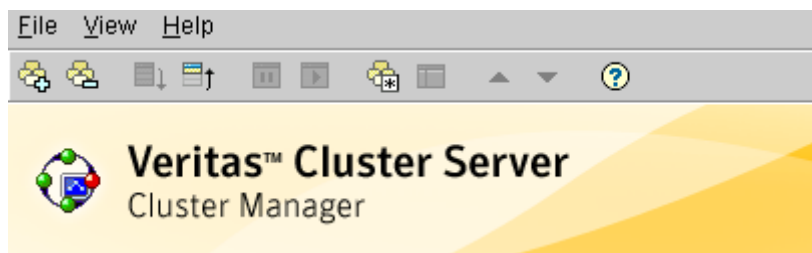
 **NOTE**

In normal cases, the U2000 processes of the primary site are started but those of the secondary site are not started.

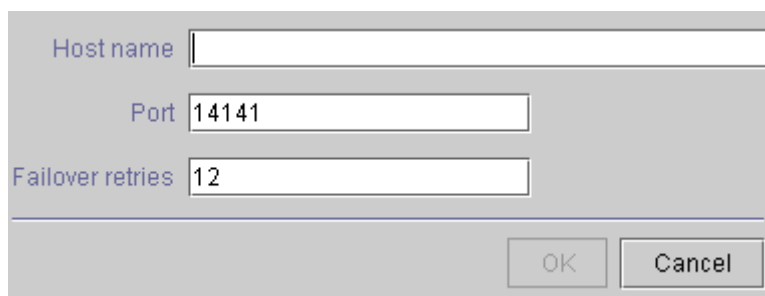
### Answer

- 1 Log in to the OS as a user with administrator rights.
- 2 Start the VCS client.

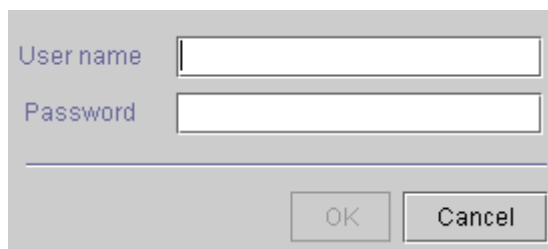
1. Choose **Start > Programs > Symantec > Veritas Cluster Server > Veritas Cluster Manager - Java Console** to start the VCS client.



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.9.17 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

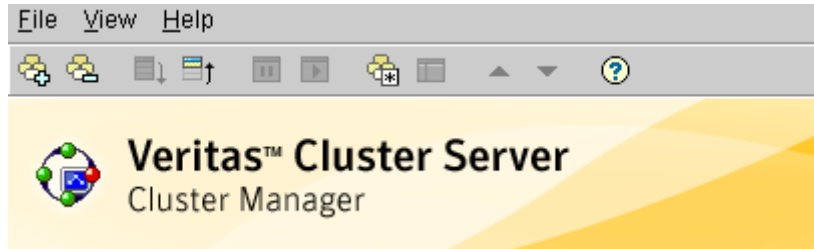
In normal cases, the U2000 processes of the primary site are started but those of the secondary site are not started.

### Answer

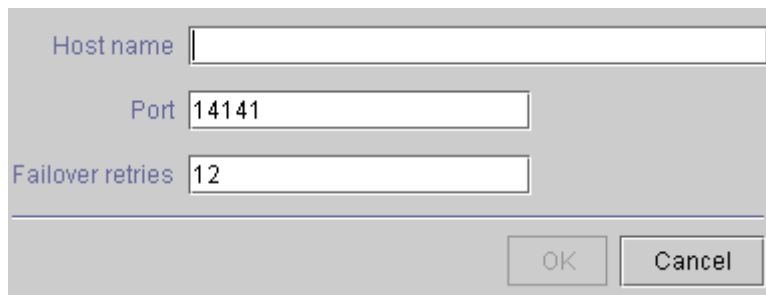
- 1 Log in to the OS as a user with **administrator** rights. The system automatically starts the database and U2000 service.



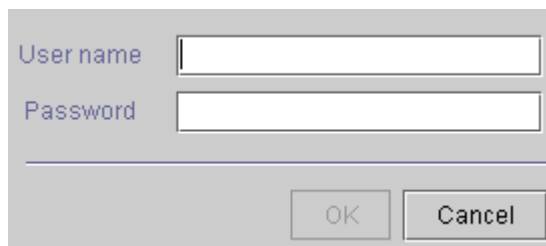
- 2 If the database and U2000 processes do not automatically start along with the OS, run the following command to manually start them:
  1. Choose **Start > Programs > Symantec > Veritas Cluster Server > Veritas Cluster Manager - Java Console** to start the VCS client.



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



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.9.18 How to End the U2000 Processes of the High Availability System (Windows)

### Question

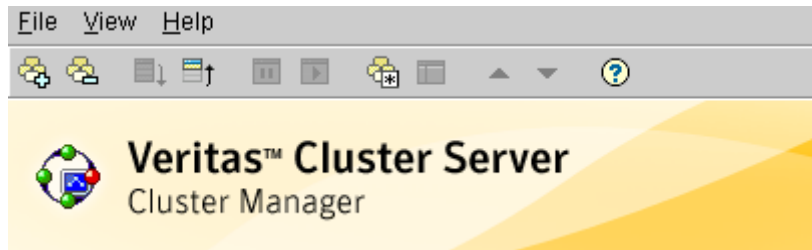
How do I end the U2000 processes of the high availability system (Windows)?

#### NOTE

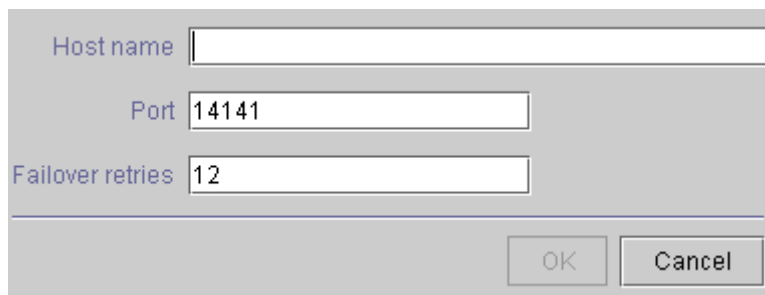
In normal cases, the U2000 processes of the primary site are started but those of the secondary site are not started.

## Answer

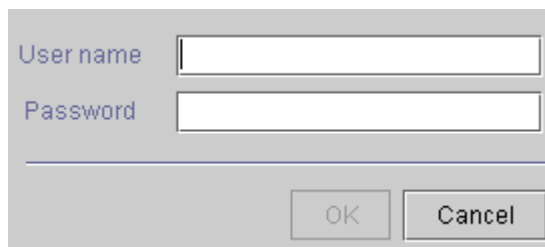
- 1 Log in to the OS as a user with administrator rights.
- 2 End the U2000 processes of the Veritas high availability system.
  1. Choose **Start > Programs > Symantec > Veritas Cluster Server > Veritas Cluster Manager - Java Console** to start the VCS client.



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.9.19 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.9.20 How to Start the U2000 Processes of the High Availability System (Solaris)

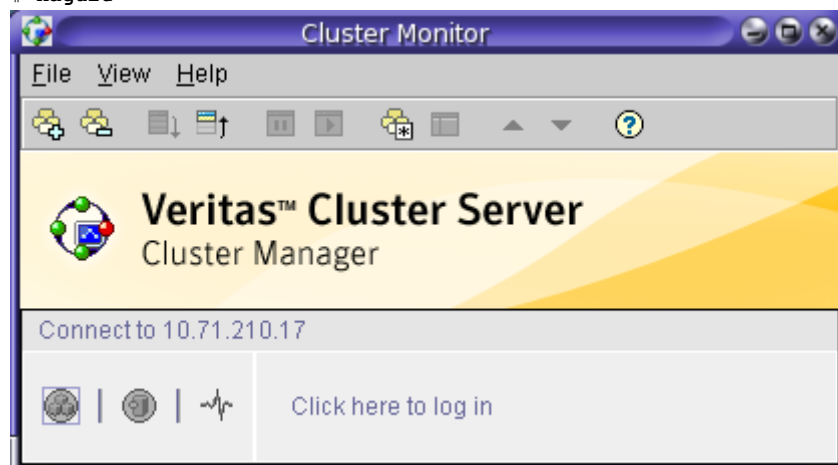
### Question

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:

```
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

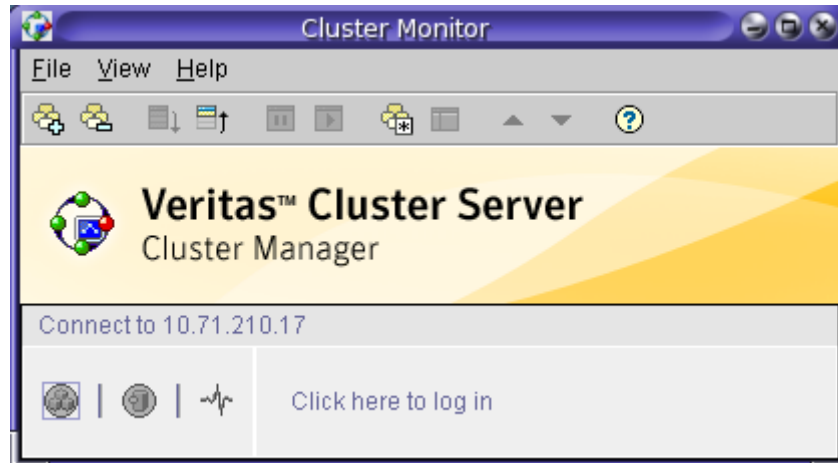
## A.9.21 How to End the U2000 Processes of the High Availability System (Solaris)

### Question

How do I end the U2000 processes of the high availability system (Solaris)?

### Answer

- 1 Log in to the OS of the active site as the **root** user.
- 2 Log in to the VCS.
  1. Open a terminal window, run the following command:  
# **hagui &**



 **NOTE**

If the login window fails to be displayed and the terminal displays a message indicating that the current status is "STALE\_ADMIN\_WAIT", run the **# hasys -force host name of node** command.

2. Click **Connect to Cluster name**.

 **NOTE**

If you are logging in to the VCS for the first time, you need to create a new Cluster.

- a. Click **File > New Cluster**.
- b. Enter the IP address of application network.
- c. Click **OK**.

3. Enter *User Name* and *Password*.

 **NOTE**

The default user name of the VCS is **admin** and the password is **password**. For system security, modify the password and remember the new password.

- 3 Select the **AppService** resource group from the navigation tree, right-click, and choose **Offline > Host name** from the shortcut menu.

Wait about three minutes. If **Group Status on Member Systems** is displayed as **Offline**, it indicates that the U2000 processes are ended.

----End

## A.9.22 How to Check Whether the U2000 Processes of the High Availability System (SUSE Linux-Distributed) Are Started

### Question

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

### Answer

- 1 Log in to the OS of the master server on the active site as the **root** user.
- 2 Check the U2000 processes.

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

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

 **NOTE**

Leave a space between the dot (.) and the command **svc\_profile.sh**.

Information similar to the following is displayed:

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

 **NOTE**

The U2000 is running if the displayed information contains **imap\_sysmonitor -cmd start**.

----End

## A.9.23 How to Start the U2000 Processes of the High Availability System (SUSE Linux-Distributed)

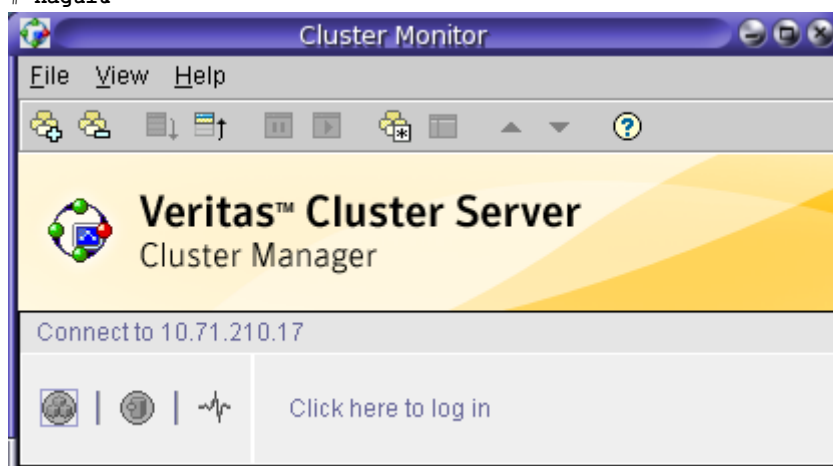
### Question

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:

```
hagai&
```



 **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

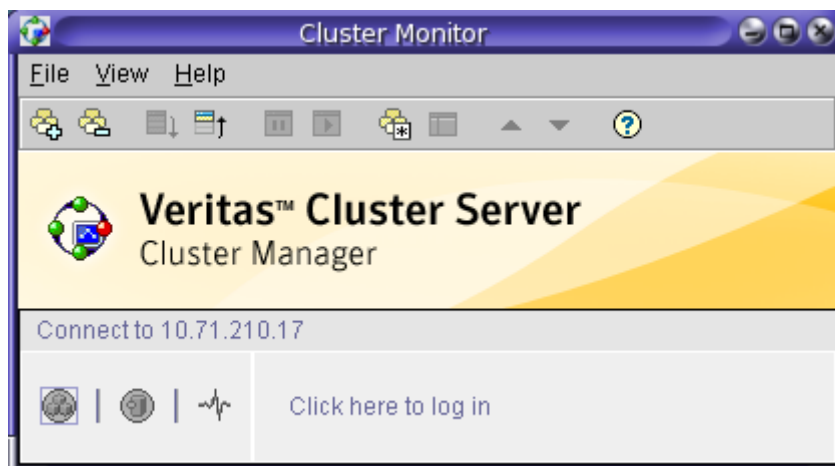
## A.9.24 How to End the U2000 Processes of the High Availability System (SUSE Linux-Distributed)

### Question

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

### Answer

- 1 Log in to the OS of the master server on the active site as user **root**.
- 2 Log in to the VCS.
  1. Open a terminal window, run the following command:  
# **hagui &**



**NOTE**

If the login window fails to be displayed and the terminal displays a message indicating that the current status is "STALE\_ADMIN\_WAIT", run the **# hasys -force host name of node** command.

2. Click **Connect to Cluster name**.

**NOTE**

If you are logging in to the VCS for the first time, you need to create a new Cluster.

- a. Click **File > New Cluster**.
  - b. Enter the IP address of application network.
  - c. Click **OK**.
3. Enter *User Name* and *Password*.

**NOTE**

The default user name of the VCS is **admin** and the password is **password**. For system security, modify the password and remember the new password.

- 3 Select the **AppService** resource group from the navigation tree, right-click, and choose **Offline > Host name** from the shortcut menu.

Wait about three minutes. If **Group Status on Member Systems** is displayed as **Offline**, it indicates that the U2000 processes are ended.

----End

## A.9.25 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.9.26 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.9.27 How to Add Components Incrementally

### Question

The U2000 is installed by using the software package, but only the single-domain component is installed, for example, only the component of the transport domain is uploaded to the server for decompression and installation. The components of other domains, however, need to be added later. How do I add them?

### Answer

- 1 Verify that the following paths have sufficient remaining space.
  - On Solaris or SUSE Linux, verify that the following paths have sufficient remaining space.

 **TIP**

You can run the **df -hk** command to view the remaining space. For example, to view the remaining space of the **/opt/U2000** path, run the **df -hk /opt/U2000** command.

**Table A-8** Space requirement for Solaris or SUSE Linux

| Directory        | Small-Scale Network<br>(Less Than 2000 Equivalent NEs)                                                                                      | Medium-Scale Network<br>(2000 to 6000 Equivalent NEs)                                                                                         | Large-Scale Network<br>(6000 to 15000 Equivalent NEs)                                                                                         |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| /opt/U2000       | <ul style="list-style-type: none"> <li>● Transport domain: 1.5 GB</li> <li>● Access domain: 1.0 GB</li> <li>● IP domain: 0.8 GB</li> </ul>  | <ul style="list-style-type: none"> <li>● Transport domain: 1.5 GB</li> <li>● Access domain: 1.0 GB</li> <li>● IP domain: 0.8 GB</li> </ul>    | <ul style="list-style-type: none"> <li>● Transport domain: 1.5 GB</li> <li>● Access domain: 1.0 GB</li> <li>● IP domain: 0.8 GB</li> </ul>    |
| /opt/sybase/data | <ul style="list-style-type: none"> <li>● Transport domain: 7.6 GB</li> <li>● Access domain: 7.4 GB</li> <li>● IP domain: 14.5 GB</li> </ul> | <ul style="list-style-type: none"> <li>● Transport domain: 10.8 GB</li> <li>● Access domain: 13.0 GB</li> <li>● IP domain: 23.0 GB</li> </ul> | <ul style="list-style-type: none"> <li>● Transport domain: 35.0 GB</li> <li>● Access domain: 43.0 GB</li> <li>● IP domain: 54.0 GB</li> </ul> |

- On Windows, verify that the following paths have sufficient remaining space.

**Table A-9** Space requirement for Windows

| Directory                                      | Small-Scale Network<br>(Less Than 2000 Equivalent NEs)                                                                                      | Medium-Scale Network<br>(2000 to 6000 Equivalent NEs)                                                                                         | Large-Scale Network<br>(6000 to 15000 Equivalent NEs)                                                                                         |
|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| Database file path<br>For example, C:\data     | <ul style="list-style-type: none"> <li>● Transport domain: 7.6 GB</li> <li>● Access domain: 7.4 GB</li> <li>● IP domain: 14.5 GB</li> </ul> | <ul style="list-style-type: none"> <li>● Transport domain: 10.8 GB</li> <li>● Access domain: 13.0 GB</li> <li>● IP domain: 23.0 GB</li> </ul> | <ul style="list-style-type: none"> <li>● Transport domain: 35.0 GB</li> <li>● Access domain: 43.0 GB</li> <li>● IP domain: 54.0 GB</li> </ul> |
| NMS installation path<br>For example, d:\U2000 | <ul style="list-style-type: none"> <li>● Transport domain: 1.5 GB</li> <li>● Access domain: 1.0 GB</li> <li>● IP domain: 0.8 GB</li> </ul>  | <ul style="list-style-type: none"> <li>● Transport domain: 1.5 GB</li> <li>● Access domain: 1.0 GB</li> <li>● IP domain: 0.8 GB</li> </ul>    | <ul style="list-style-type: none"> <li>● Transport domain: 1.5 GB</li> <li>● Access domain: 1.0 GB</li> <li>● IP domain: 0.8 GB</li> </ul>    |

- 2 Upload the software package of the component to be added to any directory on the U2000 server.
  - On Solaris or SUSE Linux, upload the software package to any directory, for example, /opt/install.
  - On Windows, upload the software package to any directory, for example, D:\install of the server. The directory should be as short as possible. The directory can contain only letters,

numbers, or underlines. Ensure that the directory does not contain any spaces, brackets, or Chinese characters.



## CAUTION

In an HA system, perform this operation at both the primary and secondary sites.

---

- 3 Decompress the software package into the current directory. In an HA system, perform this operation at both the primary and secondary sites.



### NOTE

On Solaris or SUSE Linux, run the following commands to decompress the software package as user

**root**:

```
cd directory for saving the software package
tar xvf name of the installation software package
```

- 4 To handle the corresponding configuration file, run the following command.

- On Windows, run the following commands through a CLI:

```
cd c:\HWENGR\engineering\HWICMR
pre_addDomainInstallPackage.bat directory for saving the software package, for example, D:\install
```

- On Solaris or SUSE Linux, run the following commands through a CLI:

```
cd /opt/HWENGR/engineering/HWICMR
./pre_addDomainInstallPackage.sh directory for saving the software package
```



## CAUTION

In an HA system, perform this operation at both the primary and secondary sites.

---

- 5 Perform the following operations to restart the MSuite server 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
```

- 6 Log in to the MSuite client.

- 7 Synchronize NMS data.

- In a single-server system, for details about how to synchronize NMS data, see [C.3.2 Synchronizing the NMS Information](#).
- In an HA system, for details about how to synchronize NMS data, see [C.3.3 Synchronizing the NMS Information \(High Availability System\)](#).

- 8 Log out of the MSuite client.

- 9 Perform the following operations to restart the MSuite server 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
```
- 10 Log in to the MSuite client.
- 11 Add the component.

**CAUTION**

In an HA system, perform this operation at the active site.

---

1. On the MSuite client, choose **Deploy > Add Component**. The **Add Component** dialog box is displayed.
  2. 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.
3. Wait until the dialog box is displayed to prompt the message **The component is successfully added**.
  4. Click **OK**.
- 12 After adding components incrementally, uninstall all independent U2000 clients and then install U2000 clients in network mode. For details about how to install a U2000 client, see the section "Installing the U2000 Client in Network Mode" in the *iManager U2000 Client Software Installation Guide*.

----End

## A.9.28 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-10** 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.9.29 How to Check Whether the daem Process Is Started

### Question

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

### Answer

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

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

Information similar to the following is displayed:

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

Or a message similar to the following will be displayed:

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



#### NOTE

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

----End

## A.9.30 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.9.31 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.9.32 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.9.33 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 [11.3 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.9.34 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 [11.4 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.9.35 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::instNMS_request,tasks::single_network_request,tasks::modify_sys_paras,tasks::enable_multi_path,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.9.36 How to View Network Configurations for the Primary Site or Secondary Site Installed with a HA System

### Question

How do I view network configurations for the primary site or secondary site installed with a high availability (HA) system?

### Answer

#### NOTE

The following uses viewing configurations for the primary site as an example. Viewing configurations for the secondary site is similar to that for the primary site.

- 1 Log in to the OS of the primary site as user **root**.
- 2 View the **vcs\_net\_config.cfg** file. Saving this file to a local disk is recommended.

Run the following commands to view the **vcs\_net\_config.cfg** file:

```
cd /etc/ICMR/netCfg/VCS/
more vcs_net_config.cfg
```

A message similar to the following will be displayed:

...

```
#The following are meanings of configuration item
ClearFlag=yes
SystemIP=10.78.218.52
SystemHostname=primary
SystemNetmask=255.255.255.0
SystemNic=bge0
```

```

SystemRouter=10.78.218.1

...
HBCFG=no
HBIP=10.78.218.52
HBHostname=primary
HBNetmask=255.255.255.0
...
To use another NIC to back up PHBNic, configure the following parameters.
HBIsIPMP=no

HBStandbyNic=
HBStandbyIP=
HBStandbyNetmask=255.255.255.0
HBStandbyHostname=HBSlave

#VVR network configure, support the IPMP
VVRCFG=no

VVRIP=
VVRHostname=VVRService
VVRNetmask=255.255.255.0

VVRMasterNic=
VVRMasterIP=
VVRMasterHostname=VVRMaster
VVRMasterNetmask=255.255.255.0

To use another NIC to back up PHBNic, configure the following parameters.
VVRIsIPMP=

VVRStandbyNic=
VVRStandbyIP=
VVRStandbyHostname=VVRSlave
VVRStandbyNetmask=255.255.255.0

#APP network configure, support the IPMP
APPCfg=yes

APPIP=10.78.218.52
APPHostname=primary
APPNetmask=255.255.255.0
APPMasterNic=bge0

APPMasterIP=
APPMasterHostname=APPMaster
APPMasterNetmask=255.255.255.0
 # To use anther NIC to back up the HBNic, configure the following
parameters.
 APPIsIPMP=no
 APPStandbyNic=
 APPStandbyIP=
 APPStandbyNetmask=255.255.255.0
 APPStandbyHostname=APPSlave

```

The preceding information shows the system IP address, the host name, the subnet mask, the default route, and the relationships between the system IP address and the heartbeat network, replication network, and NMS application network. Details are as follows:

- **SystemIP=10.78.218.52**: The system IP address is **10.78.218.52**.
- **SystemHostname=primary**: The system host name is **primary**.
- **HBCFG=no**: The system IP address is used as the heartbeat IP address (there is no need to set a heartbeat IP address).
- **HBIsIPMP=no**: IPMP is not configured for the heartbeat IP address.

- **VVRCFG=no**: The heartbeat IP address is used as the replication IP address (there is no need to set a replication IP address).
- **APPCfg=yes**: The application IP address needs to be set.

3 Run the following command to view and record routing information:

```
netstat -rn
```

A message similar to the following will be displayed:

```
Routing Table: IPv4
 Destination Gateway Flags Ref Use Interface

default 10.78.218.1 UG 1 129077
10.78.218.0 10.78.218.52 U 1 1776 bge0
224.0.0.0 10.78.218.52 U 1 0 bge0
127.0.0.1 127.0.0.1 UH 12 1243318 lo0
```

----End

## A.9.37 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.9.38 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 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.9.39 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.9.40 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.9.41 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.9.42 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.9.43 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 daem process.  

```
/etc/init.d/u2kdaem stop
```
  2. Run the following command to configure the slave server communication mode.  

```
ssl_adm -cmd setmode mode parameter
```

 **NOTE**

In the preceding command, *mode parameter* can be **normal**, **ssl**, or **both**. The description of each value is as follows:

- **normal**: Indicates that the U2000 server communicates with clients only in normal mode without security assurance.
- **ssl**: Indicates that the U2000 server communicates with clients only in security mode. This mode ensures the communication security.
- **both**: Indicates that both the normal and SSL modes are applicable to the U2000 server to communicate with clients.

#### 5 Restart the daem process.

 **NOTE**

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

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

#### 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.9.44 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.

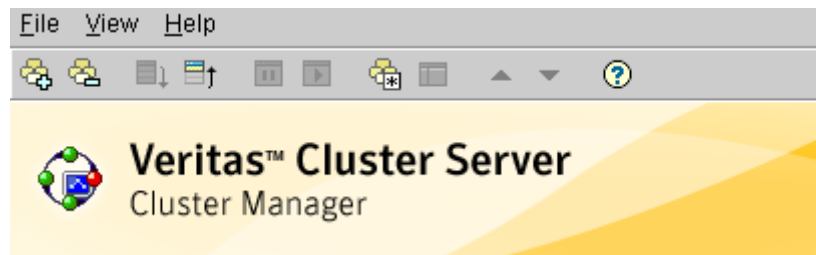
## Answer

- 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:

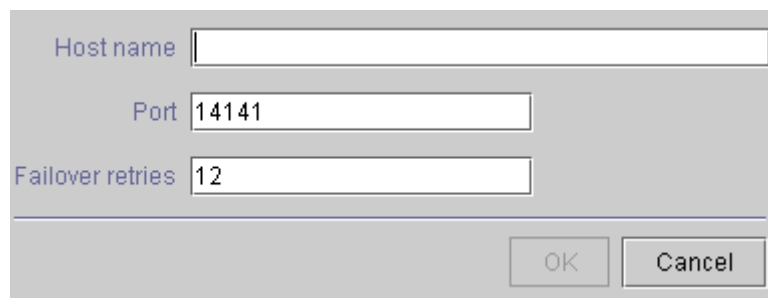
Choose **Start > Run**. In the **Run** dialog box, enter **cmd** to open the command line interface (CLI). Enter **ssl\_adm -cmd query** to query the communication mode that the U2000 server is using.

- 2 On the primary site, do as follows to stop U2000 processes:

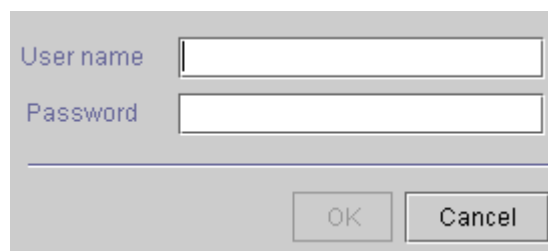
1. Choose **Start > Programs > Symantec > Veritas Cluster Server > Veritas Cluster Manager - Java Console** to start the VCS client.



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.

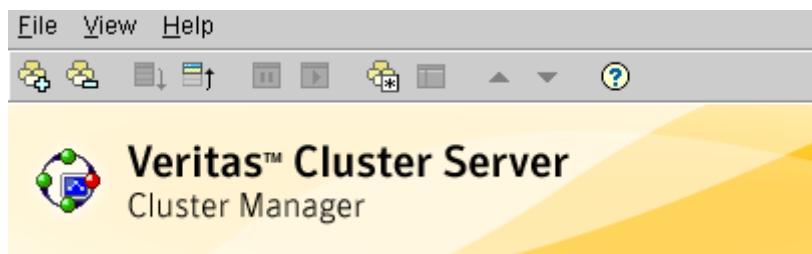
#### NOTE

The available options for *mode parameter* are **normal**, **ssl**, and **both**.

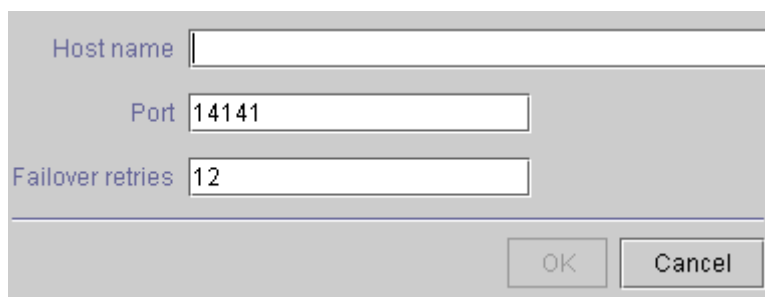
- **normal**: indicates that the U2000 server and client can communicate with each other only in common mode.
- **ssl**: indicates that the U2000 server and client can communicate with each other only in SSL mode. In this mode, communication security is guaranteed between the U2000 server and client.
- **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:

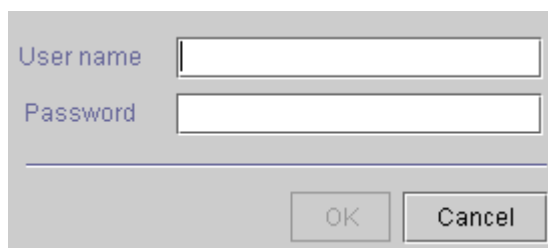
1. Choose **Start > Programs > Symantec > Veritas Cluster Server > Veritas Cluster Manager - Java Console** to start the VCS client.



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.9.45 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`.

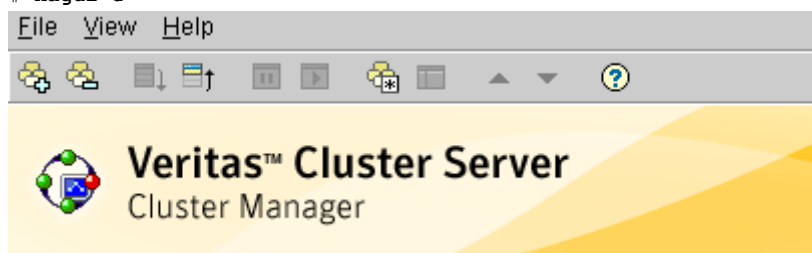
- 2 Stop the U2000 processes.

The U2000 processes consist of the U2000 server process and the Sybase process.

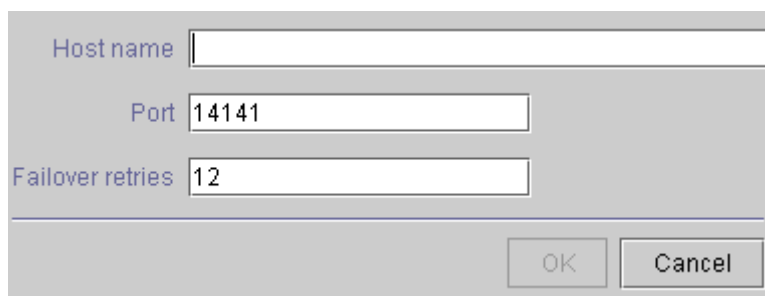
Check whether the U2000 processes are stopped and perform the following operations:

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:

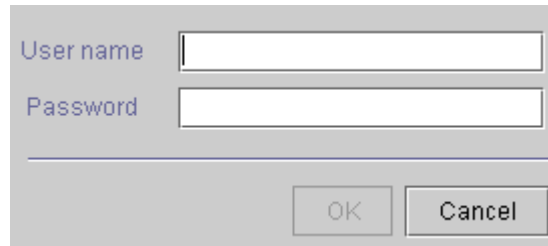
```
hagu &
```



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.9.46 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
```

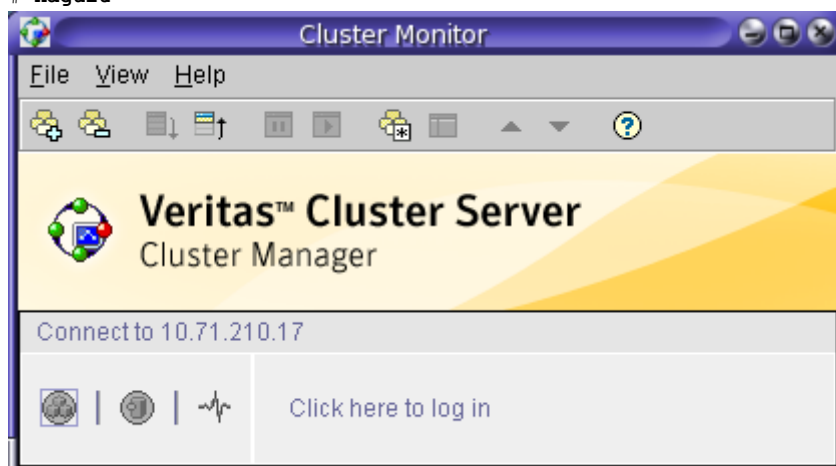


#### NOTE

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 U2000 Utilities

This topic describes the common applications of the U2000. The U2000 provides certain simple applications so that you can conveniently perform operations on the U2000.

**Table B-1** shows the common applications provided by the U2000 in the Windows OS.

**Table B-2** shows the common applications provided by the U2000 in the Solaris OS.

**Table B-3** shows the common applications provided by the U2000 in the SUSE Linux OS.

**Table B-1** Common applications in the Windows OS

| Application                   | Function                                 | Path                                              |
|-------------------------------|------------------------------------------|---------------------------------------------------|
| startup_all_global.bat        | Starts the U2000 client.                 | D:\U2000\client<br>\startup_all_global.bat        |
| startnms.bat                  | Starts the U2000 server.                 | D:\U2000\server\bin\startnms.bat                  |
| startup_sysmonitor_global.bat | Starts the System Monitor.               | D:\U2000\client<br>\startup_sysmonitor_global.bat |
| stopnms.bat                   | Stops the U2000 server.                  | D:\U2000\server\bin\stopnms.bat                   |
| startserver.bat               | Starts the NMS maintenance tool service. | C:\HWENGR\engineering<br>\startserver.bat         |
| stopserver.bat                | Stops the NMS maintenance tool service.  | C:\HWENGR\engineering<br>\stopserver.bat          |
| startclient.bat               | Starts the NMS maintenance tool client.  | D:\U2000\engineering<br>\startclient.bat          |

**Table B-2** Common applications in the Solaris OS

| Application           | Function                 | Path                                        |
|-----------------------|--------------------------|---------------------------------------------|
| startup_all_global.sh | Starts the U2000 client. | /opt/U2000/client/<br>startup_all_global.sh |

| Application                  | Function                                 | Path                                           |
|------------------------------|------------------------------------------|------------------------------------------------|
| startnms.sh                  | Starts the U2000 server.                 | /opt/U2000/server/bin/startnms.sh              |
| startup_sysmonitor_global.sh | Starts the System Monitor.               | /opt/U2000/client/startup_sysmonitor_global.sh |
| stopnms.sh                   | Stops the U2000 server.                  | /opt/U2000/server/bin/stopnms.sh               |
| startserver.sh               | Starts the NMS maintenance tool service. | /opt/HWENGR/engineering/startserver.sh         |
| stopserver.sh                | Stops the NMS maintenance tool service.  | /opt/HWENGR/engineering/stopserver.sh          |
| startclient.sh               | Starts the NMS maintenance tool client.  | /opt/U2000/engineering/startclient.sh          |

**Table B-3** Common applications in the SUSE Linux OS

| Application                  | Function                                 | Path                                           |
|------------------------------|------------------------------------------|------------------------------------------------|
| startnms.sh                  | Starts the U2000 server.                 | /opt/U2000/server/bin/startnms.sh              |
| startup_sysmonitor_global.sh | Starts the System Monitor.               | /opt/U2000/client/startup_sysmonitor_global.sh |
| stopnms.sh                   | Stops the U2000 server.                  | /opt/U2000/server/bin/stopnms.sh               |
| startserver.sh               | Starts the NMS maintenance tool service. | /opt/HWENGR/engineering/startserver.sh         |
| stopserver.sh                | Stops the NMS maintenance tool service.  | /opt/HWENGR/engineering/stopserver.sh          |
| startclient.sh               | Starts the NMS maintenance tool client.  | /opt/U2000/engineering/startclient.sh          |



This topic describes the related concepts and common operations of the MSuite.

#### [C.1 Overview](#)

This topic describes the system structure, functions, features, and certain basic concepts of the MSuite.

#### [C.2 Starting and Stopping the MSuite](#)

This topic describes how to start and stop the MSuite.

#### [C.3 System Management](#)

This topic describes how to use the system management functions of the MSuite.

#### [C.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.

#### [C.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.

#### [C.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.

#### [C.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.

#### [C.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.

#### [C.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.

## C.1 Overview

This topic describes the system structure, functions, features, and certain basic concepts of the MSuite.

### [C.1.1 Basic Concepts](#)

This topic describes the basic concepts related to the MSuite.

### [C.1.2 System Architecture of the MSuite](#)

This topic describes the system architecture of the MSuite.

### [C.1.3 Function Overview](#)

This topic describes the functions and application scenarios of the MSuite.

### [C.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.

### [C.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.

## C.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 [C.1.2 System Architecture of the MSuite](#). For the functions and features of the MSuite, see [C.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

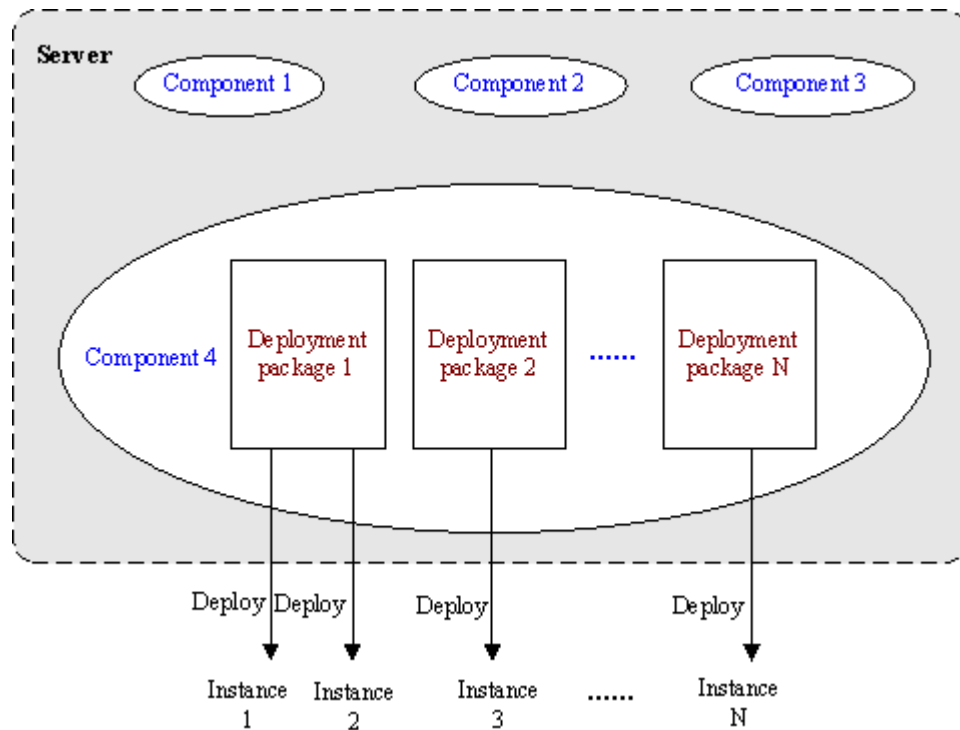
Instance names are irrelevant with process names queried on the System Monitor. You can change instance names by using the MSuite.

- **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 C-1** shows the relationships between the component, deployment package, and instance.

**Figure C-1**



**NOTE**

- The U2000 consists of multiple components. Each component implements one function of the U2000. For example, as shown in **Figure C-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 C-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 C-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.

## C.1.2 System Architecture of the MSuite

This topic describes the system architecture of the MSuite.

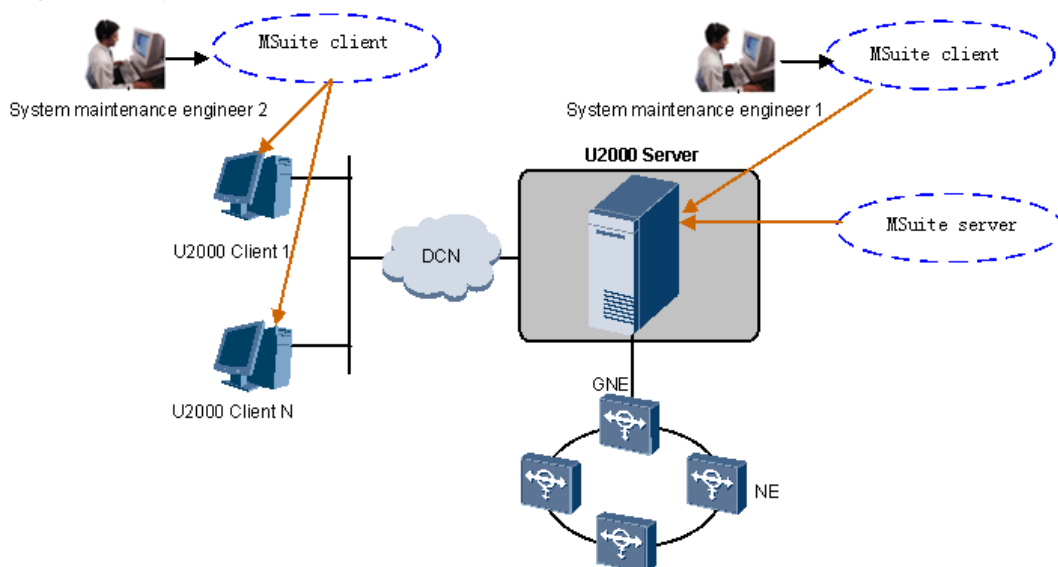
The MSuite adopts the client/server model. The client communicates with the server through the TCP/IP protocol. After receiving a request from the client, the server completes the specific task, and then sends the result back to the client. [Figure C-2](#) shows the system architecture.



### 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 C-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 C-2](#), maintenance engineers 1 and 2 cannot log in to the MSuite client at the same time to operate the U2000.

## C.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 C-1** Functions of the MSuite

| Type                              | Function                          | Description                                                                  |
|-----------------------------------|-----------------------------------|------------------------------------------------------------------------------|
| Managing the NMS                  | Refreshing the NMS information    | For details, see <a href="#">C.3.1 Refreshing the NMS Information</a> .      |
|                                   | Synchronizing the NMS information | For details, see <a href="#">C.3.2 Synchronizing the NMS Information</a> .   |
|                                   | Changing the password             | For details, see <a href="#">C.3.4 Changing the Password of the MSuite</a> . |
|                                   | Logging out of the MSuite client  | For details, see <a href="#">C.2.3 Exiting from the MSuite client</a> .      |
|                                   | Exiting from the MSuite client    | For details, see <a href="#">C.2.3 Exiting from the MSuite client</a> .      |
| Deploying and maintaining the NMS | Adding a component                | For details, see <a href="#">C.4.1 Adding a Component</a> .                  |
|                                   | Deleting a component              | For details, see <a href="#">C.4.2 Deleting a Component</a> .                |
|                                   | Adding an instance                | For details, see <a href="#">C.4.3 Adding an Instance</a> .                  |

| Type                                                           | Function                                                   | Description                                                                                                       |
|----------------------------------------------------------------|------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
|                                                                | Deleting an instance                                       | For details, see <a href="#">C.4.5 Deleting an Instance</a> .                                                     |
|                                                                | Modifying the instance name and description                | For details, see <a href="#">C.4.6 Changing the Name and Remarks of an Instance</a> .                             |
|                                                                | Modifying the system time and time zone                    | For details, see <a href="#">C.4.7 Setting the System Time and Time Zone</a> .                                    |
|                                                                | Changing the password of the administrator of the database | For details, see <a href="#">C.4.8 Changing the Password of the Administrator of the Database</a> .               |
|                                                                | Changing the password of the NMS user of the database      | For details, see <a href="#">C.4.9 Changing the Password of the User of the Database</a> .                        |
|                                                                | Configuring NTP                                            | For details, see <a href="#">C.4.10 Configuring the NTP Service</a> .                                             |
| Maintaining the high availability system (Veritas hot standby) | Synchronizing the primary and secondary sites              | For details, see <a href="#">C.6.1 Establishing the HA Relationship Between the Primary and Secondary Sites</a> . |

| Type                               | Function                                                | Description                                                                                                   |
|------------------------------------|---------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
|                                    | Separating the primary and secondary sites              | For details, see <a href="#">C.6.2 Deleting the HA Relationship Between the Primary and Secondary Sites</a> . |
|                                    | Deleting replication relations                          | For details, see <a href="#">C.6.3 Deleting Replication Relations</a> .                                       |
|                                    | Configuring the local site as the primary site forcibly | For details, see <a href="#">C.6.4 Configuring the Current Server as the Active Server Forcibly</a> .         |
|                                    | Performing the dual-active operation                    | For details, see <a href="#">C.6.5 Performing the Dual-Active Operation</a> .                                 |
| Maintaining the distributed system | Adding a slave server                                   | For details, see <a href="#">C.7.1 Adding a Slave Server</a> .                                                |
|                                    | Deleting a slave server                                 | For details, see <a href="#">C.7.2 Deleting a Slave Server</a> .                                              |
|                                    | Migrating an instance                                   | For details, see <a href="#">C.7.3 Migrating an Instance</a> .                                                |
| Managing the database              | Backing up the system database                          | For details, see <a href="#">C.9.1 Backing Up the System Database</a> .                                       |

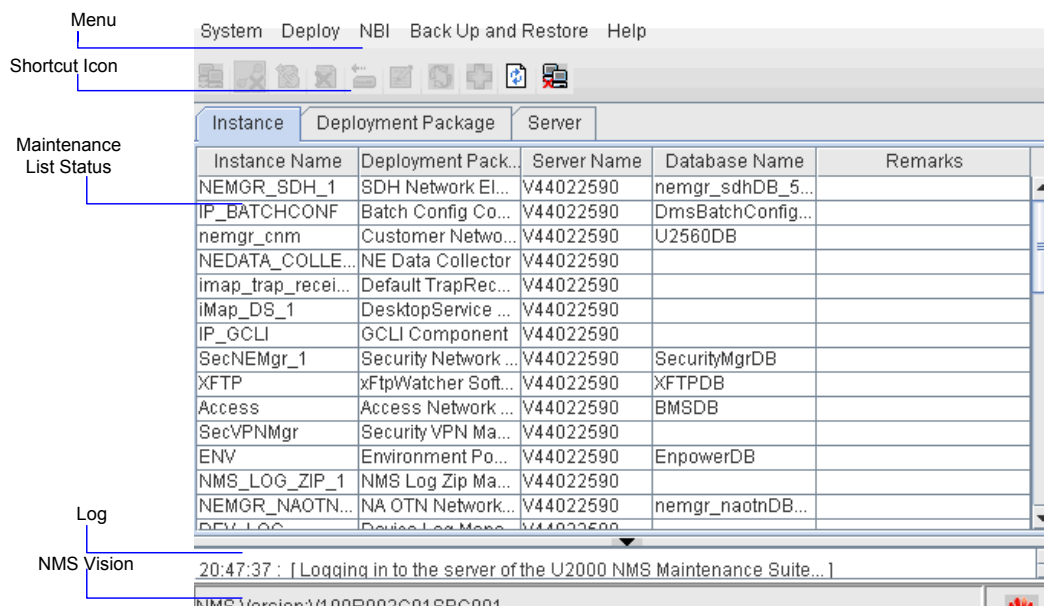
| Type                      | Function                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                           | Restoring the system database           | For details, see: <ul style="list-style-type: none"> <li>● <a href="#">C.9.2 Restoring Data of a U2000 Single-Server System (Windows)</a></li> <li>● <a href="#">C.9.3 Restoring U2000 Single-Server System (Solaris) Data</a></li> <li>● <a href="#">C.9.4 Restoring U2000 Single-Server System (SUSE Linux-Distributed) Data</a></li> <li>● <a href="#">C.9.5 Restoring U2000 High Availability System (Windows) Data</a></li> <li>● <a href="#">C.9.6 Restoring U2000 High Availability System (Solaris) Data</a></li> <li>● <a href="#">C.9.7 Restoring U2000 High Availability System (SUSE Linux-Distributed) Data</a></li> </ul> |
|                           | Initializing the U2000 database         | For details, see <a href="#">C.9.9 Initializing the U2000 Database</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Adjusting the NMS         | Changing the host name and IP address   | For details, see <a href="#">C.5.1 Changing the Host Name and IP Address</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|                           | Configuring routes                      | For details, see <a href="#">C.5.2 Configuring Routes</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|                           | Synchronizing the network configuration | For details, see <a href="#">C.5.3 Synchronizing Network Configurations</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Configuring NBI instances | -                                       | For details, see <a href="#">C.8 Configuring the Northbound Interface Instance</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## C.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 C-3** shows the GUI of the MSuite client.

**Figure C-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           | <p>Serves as a shortcut to enter the GUI of the corresponding function. The same function can be accessed through the corresponding menu.</p> <p><b>TIP</b></p> <p>Move the pointer over the shortcut icon. The system prompts you the function of the shortcut icon.</p>                                                                                                                                                                                                                         |
| Maintenance list column | <ul style="list-style-type: none"> <li>On the <b>Instance</b> tab page, you can view the names, running status, related deployment packages, related host names, and database names of all instances.</li> <li>On the "Deployment package" tab page, you can view the names, types, descriptions, and number of instances of all deployment packages.</li> <li>On the <b>Server</b> tab page, you can view the hostnames, IP addresses, NMS status, and resource usage of all servers.</li> </ul> |
| Log bar                 | Displays the log information when a task is executed.                                                                                                                                                                                                                                                                                                                                                                                                                                             |

| Component      | Meaning                     |
|----------------|-----------------------------|
| NMS vision bar | Displays the U2000 version. |

## C.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 C-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 C-2** Common CLI commands for the MSuite

| Syntax of Command Line                                                                                                                                                                            | Meaning                                                                                                                                                                                                                                  |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>./startclient.sh deploy -ip 127.0.0.1 -port 12212 -username admin -password admin query -type <i>querytype</i></code>                                                                       | Query information.<br><ul style="list-style-type: none"> <li>Querying instance information: query -type 0</li> <li>Querying deployment package information: query -type 1</li> <li>Querying server information: query -type 2</li> </ul> |
| <code>./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></code> | 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
```

## C.2 Starting and Stopping the MSuite

This topic describes how to start and stop the MSuite.

### [C.2.1 Starting the Process of the MSuite Server](#)

This topic describes how to start the process of the MSuite server.

### C.2.2 Logging In to the MSuite Client

This topic describes how to log in to the MSuite client.

### C.2.3 Exiting from the MSuite client

This topic describes how to exit from the MSuite client.

### C.2.4 Ending the Process of the MSuite Server

This topic describes how to end the process of the MSuite server.

## C.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

## C.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 [C.5.3 Synchronizing Network Configurations](#).

## C.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

## C.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

## C.3 System Management

This topic describes how to use the system management functions of the MSuite.

### C.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.

### C.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.

### C.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.

### C.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.

### C.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.

## C.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 [C.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

## C.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 [C.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

### C.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 [C.3.5 Logging Out of the MSuite Client](#).
  6. Switch the U2000 service to the standby site. For details, see [9.6.1 Manual Switchover Between Active and Standby Sites](#).
  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. For details, see [9.6.1 Manual Switchover Between Active and Standby Sites](#).
- 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 [C.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
```

## C.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 [C.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

## C.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

## C.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.

### [C.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.

### [C.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.

### [C.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.

#### [C.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.

#### [C.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.

#### [C.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.

#### [C.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.

#### [C.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.

#### [C.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.

#### [C.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.

## C.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. For details about how to add components in this scenario, see [A.9.27 How to Add Components Incrementally](#).
- 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 [C.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 [C.4.3 Adding an Instance](#).

## C.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 [C.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 [C.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

## C.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 [C.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 [C.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.

## C.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, see [3.3 Updating 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 [C.4.1 Adding a Component](#).

## Procedure

- 1 Log in to the MSuite client. For details, see [C.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 [C.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

## C.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 [C.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
```

## C.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 [C.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

## C.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 [2 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 [C.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.

## C.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.9.9 How to End the Processes of the U2000 Single-Server System on Windows](#).
  - For the Single-Server System (Solaris), see [A.9.12 How to End the Processes of the U2000 Single-Server System on Solaris](#).
  - For the Single-Server System (SUSE Linux-Distributed), see [A.9.15 How to End the Processes of the U2000 Single-Server System \(SUSE Linux-Distributed\)](#).
  - For the High Availability System (Windows), see [A.9.18 How to End the U2000 Processes of the High Availability System \(Windows\)](#).
  - For the High Availability System (Solaris), see [A.9.21 How to End the U2000 Processes of the High Availability System \(Solaris\)](#).
  - For the High Availability System (SUSE Linux-Distributed), see [A.9.24 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.7.4 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.7.3 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. For details, see [C.2.2 Logging 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
```

## C.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. For details, see [C.2.2 Logging 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

## C.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 [2 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 [C.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.

## C.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.

### C.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.

### C.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.

## C.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  
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 |       |          |        |       |      |        |         |           |

- 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 [C.5.1.1 How to Change the IP Address of the Single-Server System on Windows](#) and [C.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 [C.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 [C.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 [C.5.1.5 How to Modify the Server IP Address of High Availability System \(Windows\)](#) and [C.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 [C.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 [C.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.

## C.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

## C.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

### C.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

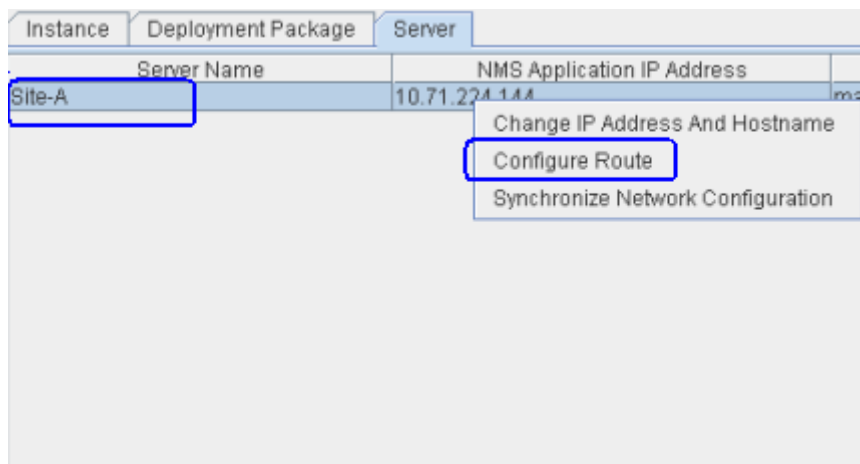
**NOTE**

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.





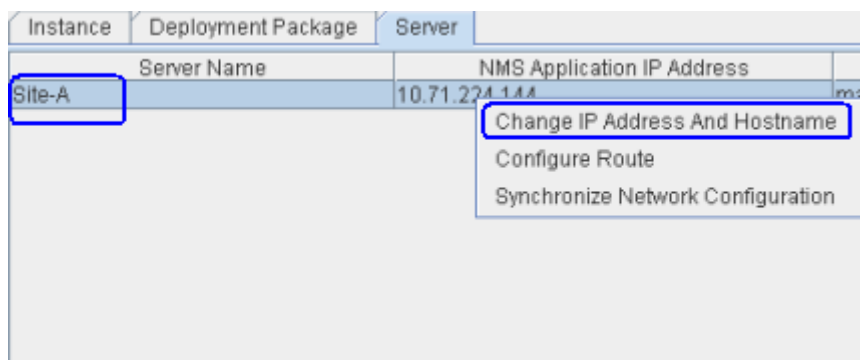
2. In the dialog box that is displayed, click **Add** or **Delete** according to actual route conditions to re-configure the route.

| 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

### C.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**

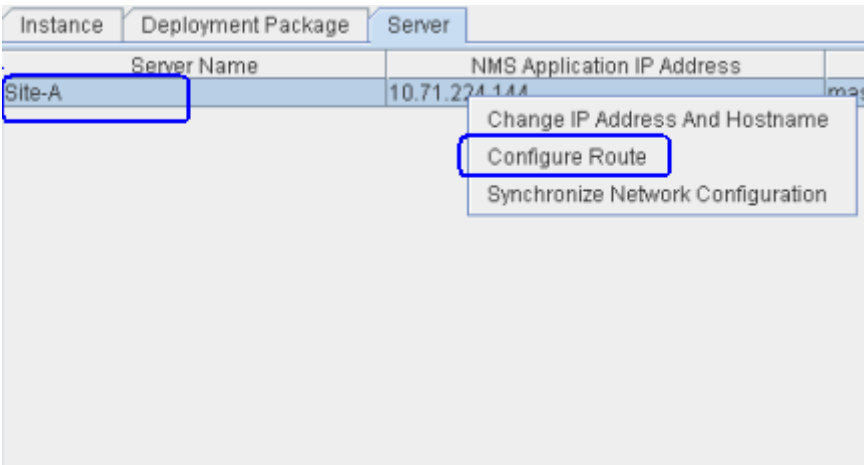
If multiple slave servers are installed, perform this step on every slave server.

- 4 After the **daem** process is ended, **log in to the MSuite client**.

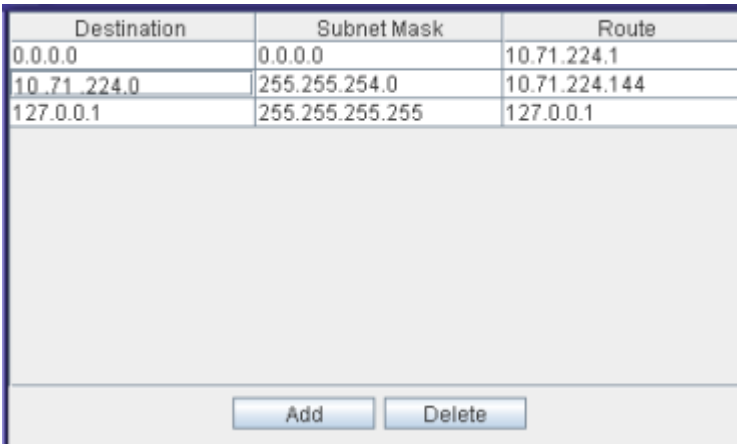
**NOTE**

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.



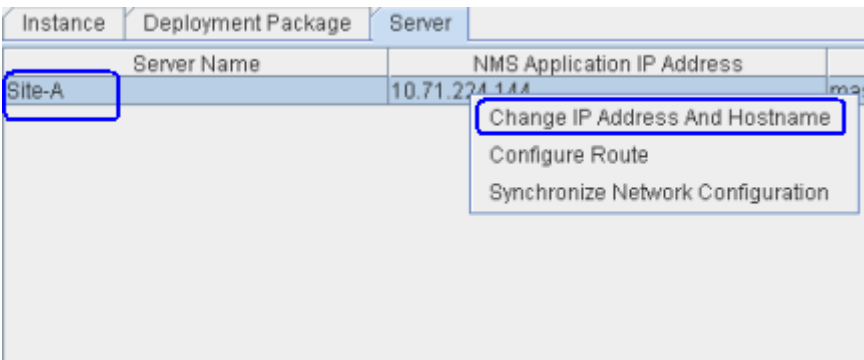
2. In the dialog box that is displayed, click **Add** or **Delete** according to actual route conditions to re-configure the route.



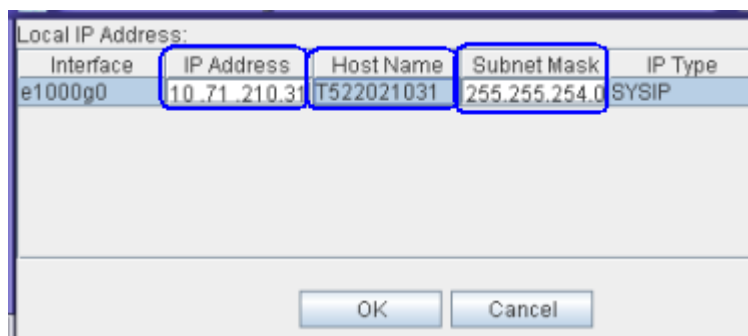
3. Click **OK**.

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.9.28 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

## C.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.

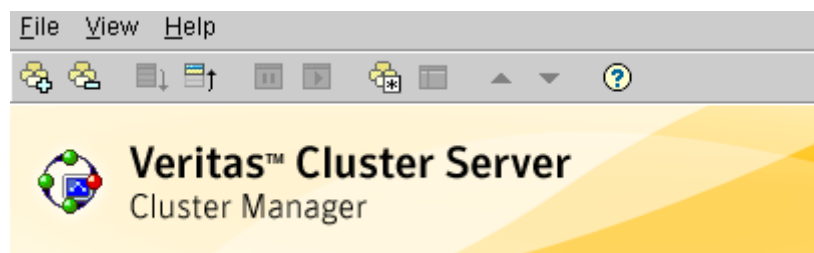
Changing an IP address includes the following major steps:

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.

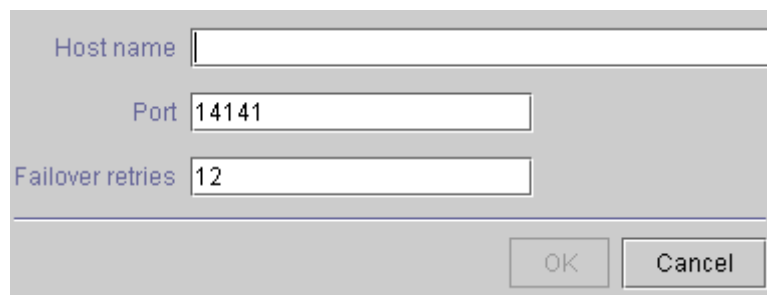
4. Change the IP address of the U2000 server.
5. Change the system IP address that is set in the VCS.
6. Start the U2000 MSuite server.
7. Log in to the U2000 MSuite client and synchronize IP address changes in configuration files. If the IP address changes are not synchronized, the U2000 fails to start 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

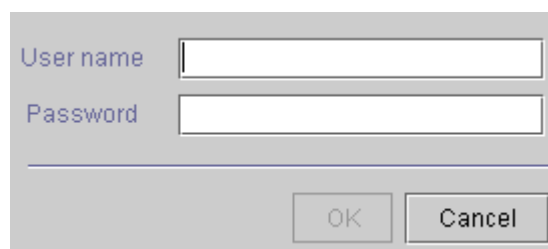
- 1 Log in to the NMS maintenance tool client. Choose **Deploy > Separate the primary and secondary sites**. The **Separate the primary and secondary sites** dialog box is displayed.
- 2 Click **OK**. The progress bar is displayed indicating the status of separating the primary and secondary sites. Wait 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.

## C.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.

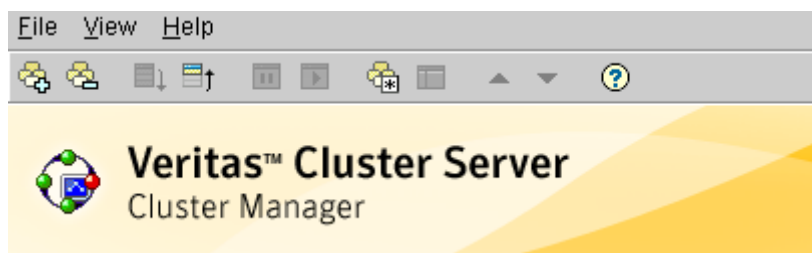
Do not change an IP address and a host name at the same time. Otherwise, the U2000 fails to be started.

Changing the host name includes the following major steps:

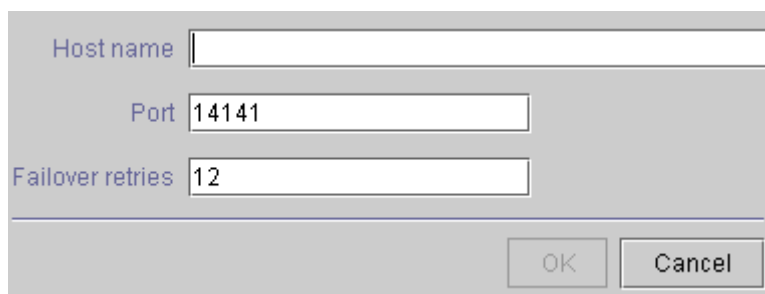
1. Shut down the U2000 server and client.
2. Stop the VCS service and communication.
3. Change the host name changes in configuration files.
4. Change the host name of the U2000 server.
5. Restart the OS.
6. Log in to the U2000 MSuite client and synchronize host name changes in configuration files. If the host name changes are not synchronized, the U2000 fails to start properly.

## Answer

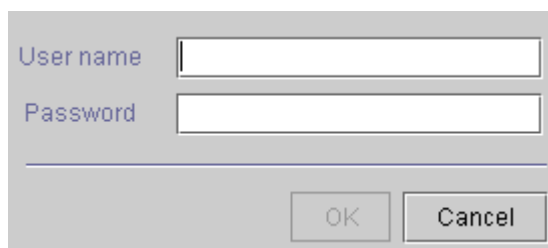
- 1 Log in to the OS as a user with administrator rights.
- 2 At the primary site, perform the following operations to end the U2000 processes:
  1. Choose **Start > Programs > Symantec > Veritas Cluster Server > Veritas Cluster Manager - Java Console** to start the VCS client.



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

### C.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



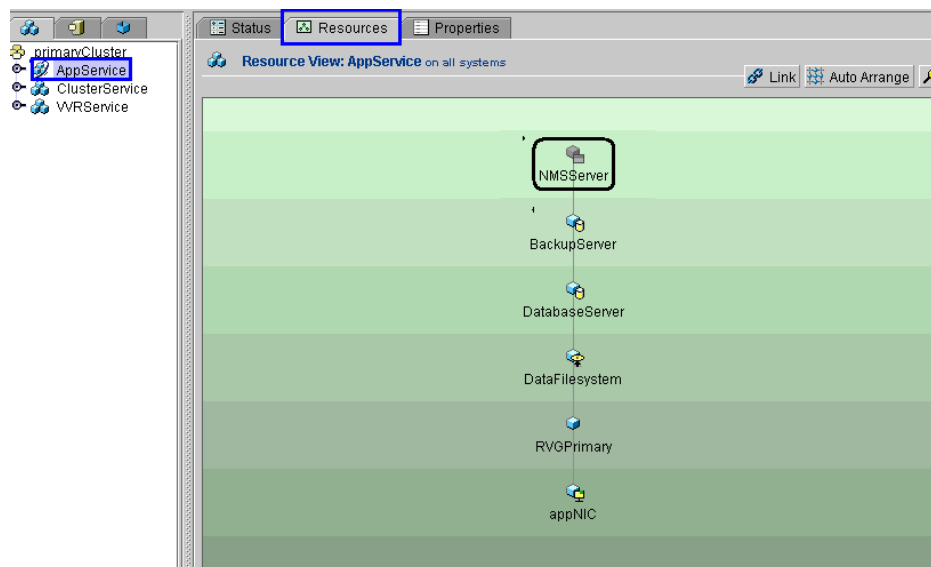
##### NOTE

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 [C.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 C-4** High Availability System (Solaris) resources



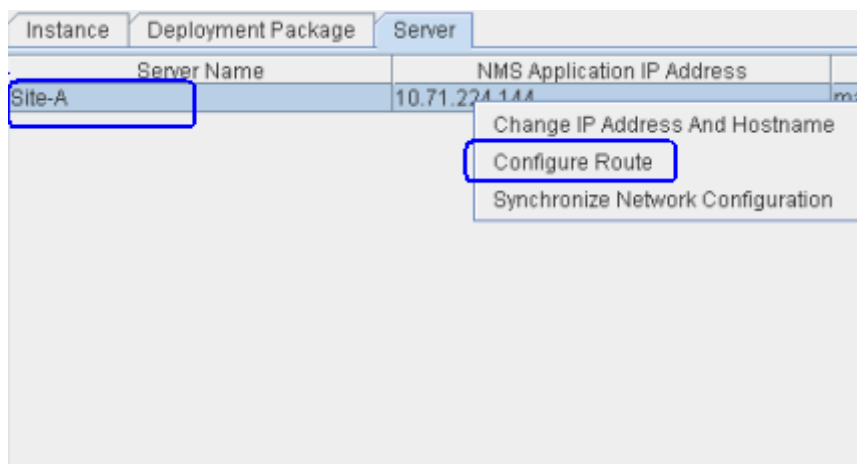
**NOTE**

- 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.



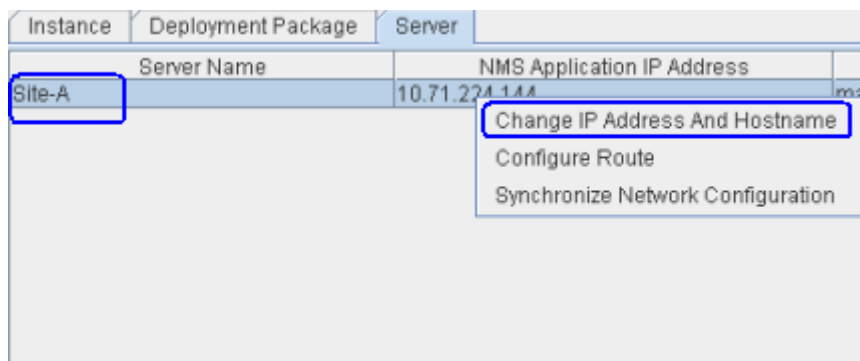
- In the dialog box that is displayed, click **Add** or **Delete** according to actual route conditions to re-configure the route.

| 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.

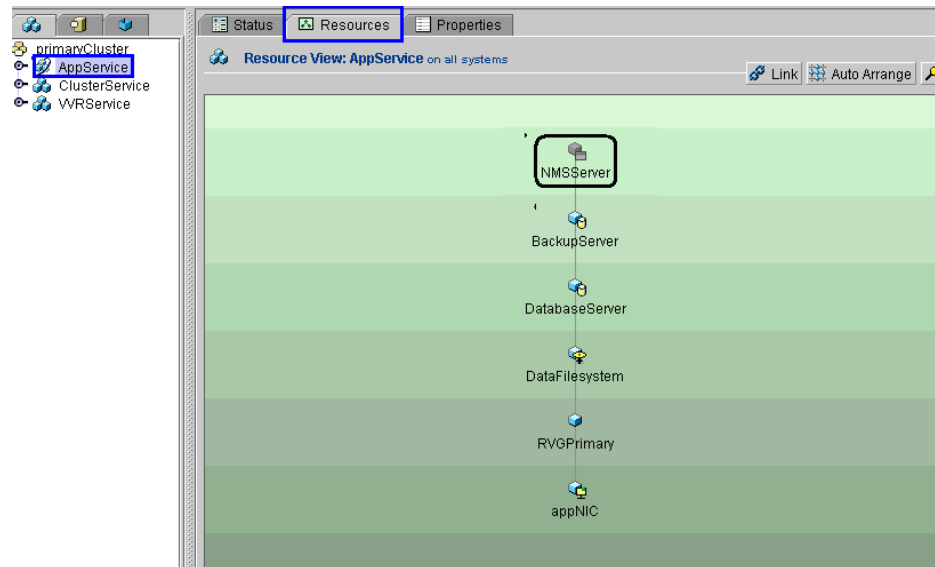
4. After the configuration is complete, the **Message** dialog box is displayed, asking you to restart the OS and back up the database in time. click **OK**.

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.

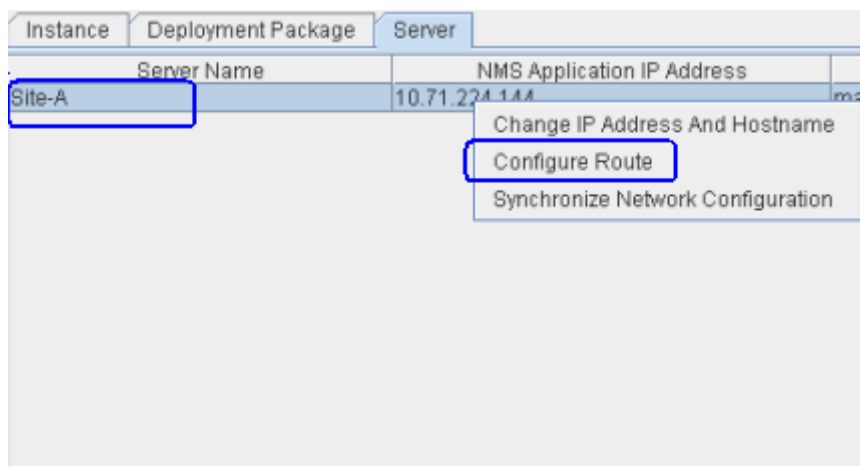
**Figure C-5** High Availability System (Solaris) resources



**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.



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     |

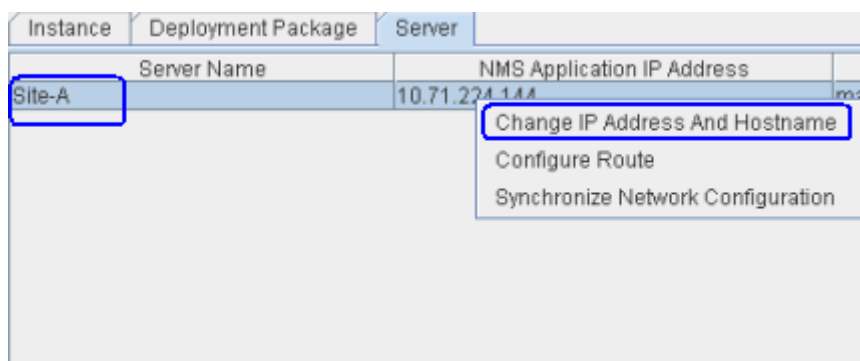
Add

Delete

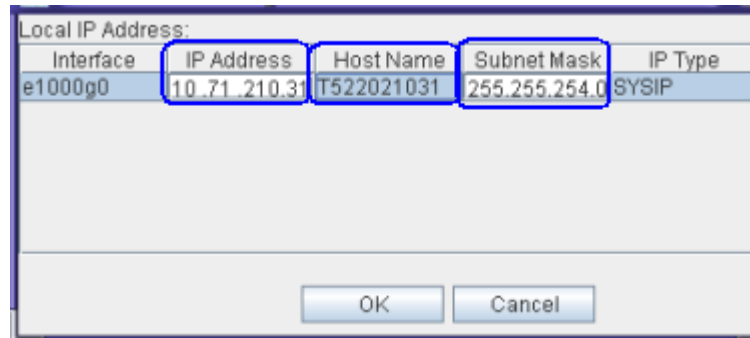
3. Click **OK**.

#### 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.



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 [C.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

### C.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.

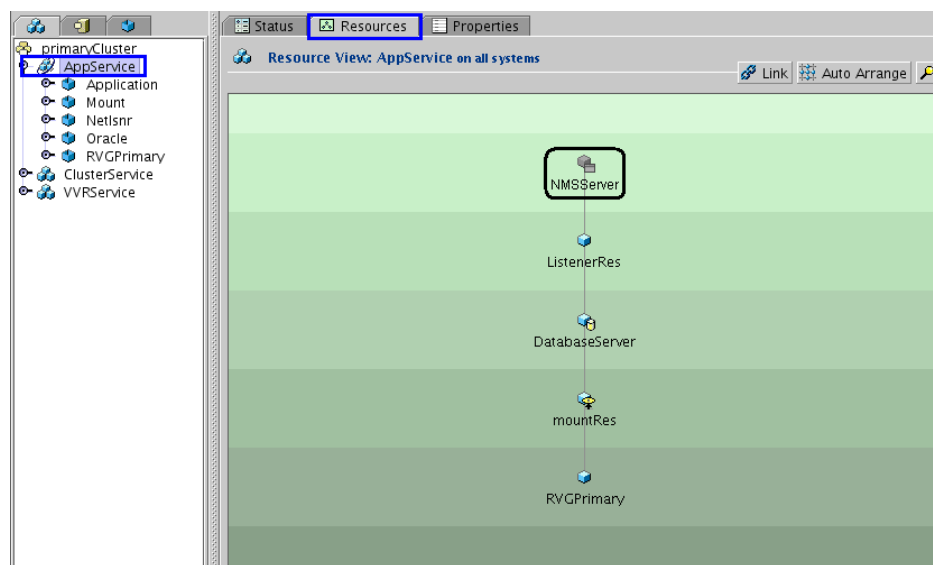
### 1 Log in to the MSuite client of the master server the primary site

#### 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 [C.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 C-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**.

- 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:

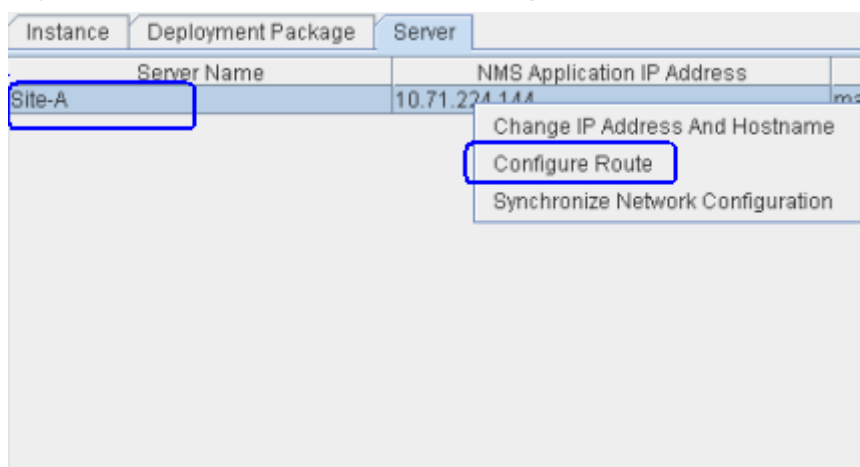
```
/etc/init.d/u2kdaem stop
```



**CAUTION**

There must be a space between the dot (.) and **svc\_profile.sh**.

- On the MSuite client, click the **Server** tab.
- 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.



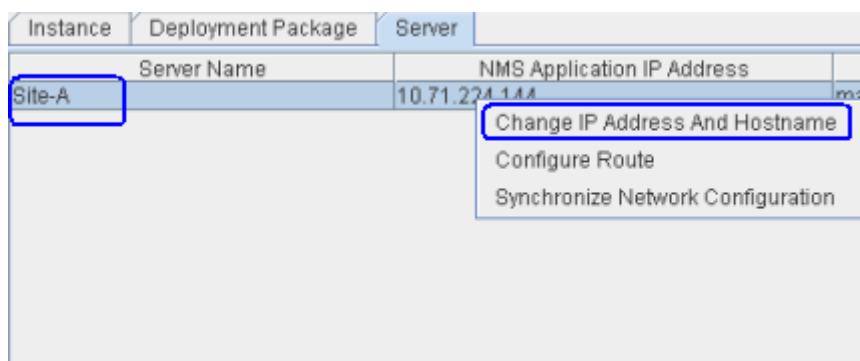
- In the dialog box that is displayed, click **Add** or **Delete** according to actual route conditions to re-configure the route.

| 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**.

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.

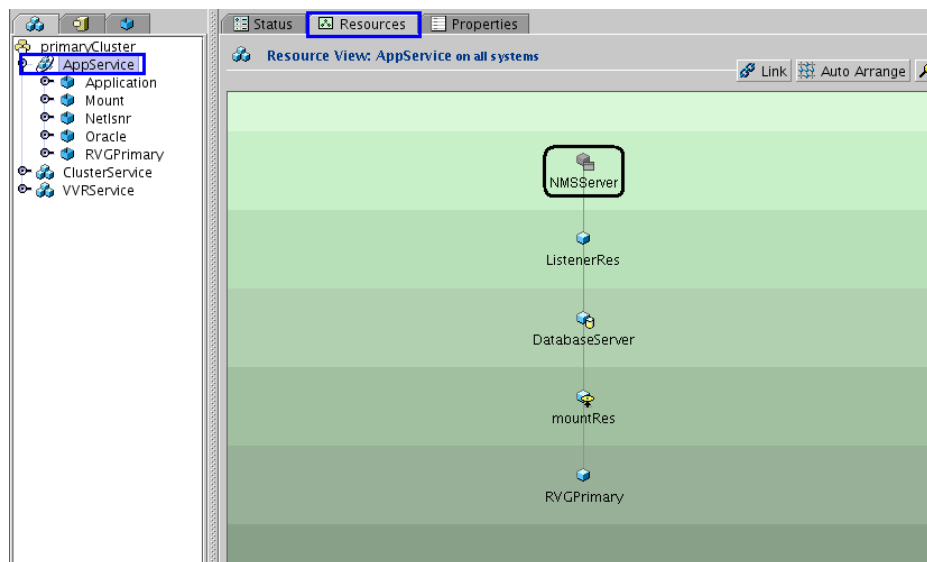
4. After the configuration is complete, the **Message** dialog box is displayed, asking you to restart the OS and back up the database in time. click **OK**.

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 C-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.](#)

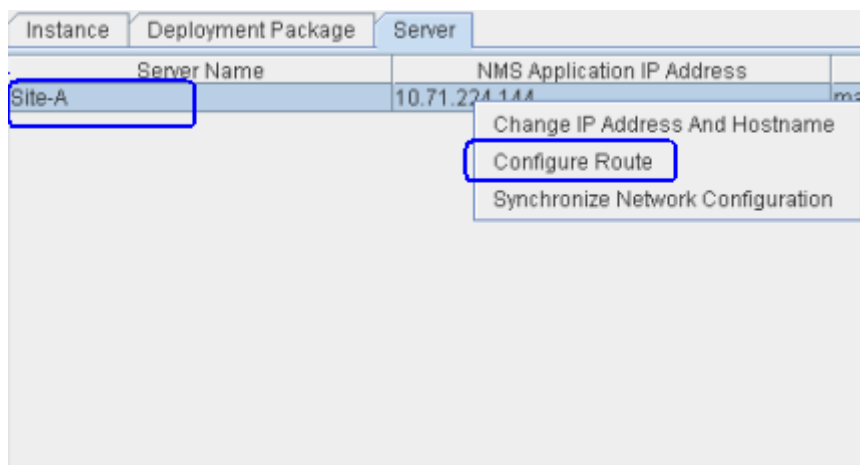
**NOTE**

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.

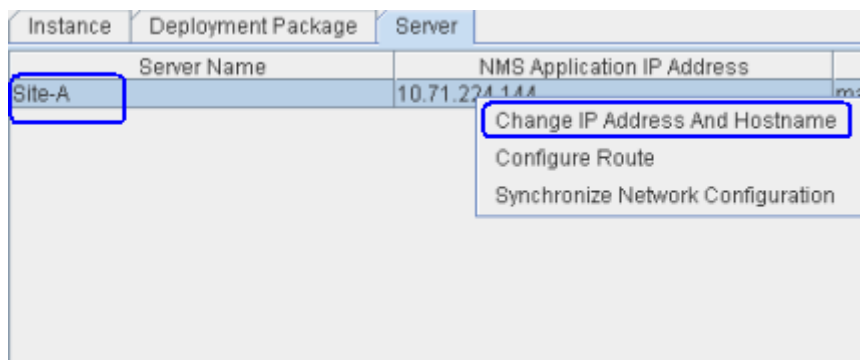
| Destination | Subnet Mask     | Route         |
|-------------|-----------------|---------------|
| 0.0.0.0     | 0.0.0.0         | 10.71.224.1   |
| 10.71.224.0 | 255.255.254.0   | 10.71.224.144 |
| 127.0.0.1   | 255.255.255.255 | 127.0.0.1     |

Buttons: Add, Delete

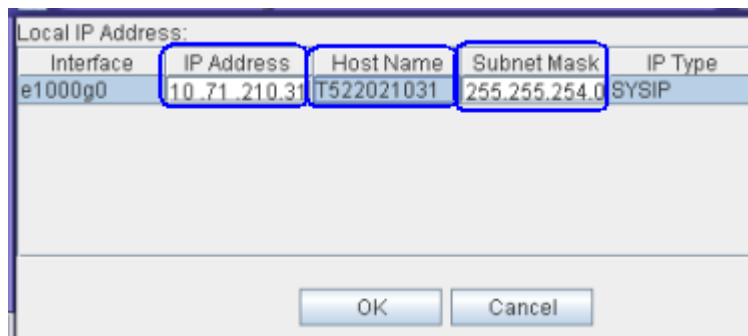
3. Click **OK**.

- 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 [C.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.9.28 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

## C.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 [C.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

## C.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 [C.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 [C.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 [C.6.1 Establishing the HA Relationship Between the Primary and Secondary Sites](#).

## C.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.

### [C.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.

### [C.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.

### [C.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.

### [C.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.

### [C.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.

## C.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. For details, see [C.2.2 Logging 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
```

## C.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. For details, see [C.2.2 Logging 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. For details, see [C.6.1 Establishing the HA Relationship Between the Primary and Secondary Sites](#).

## C.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. For details, see [C.2.2 Logging 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 [C.6.4 Configuring the Current Server as the Active Server Forcibly](#).

## C.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. For details, see [C.2.2 Logging 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

## C.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. For details, see [C.2.2 Logging 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 [C.6.4 Configuring the Current Server as the Active Server Forcibly](#).

# C.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.

### [C.7.1 Adding a Slave Server](#)

This topic describes how to connect the slave server to the master server to form a distributed system.

### [C.7.2 Deleting a Slave Server](#)

This topic describes how to delete a slave server.

### [C.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.

## C.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.

## C.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

## C.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 [C.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

## C.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.

## C.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.

### [C.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.

### [C.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.

### [C.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.

### [C.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.

### [C.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.

### [C.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.

### [C.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.

### [C.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.

### [C.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.

## C.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.

### C.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.

### C.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.

### C.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 [C.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**

### C.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 [C.2.2 Logging In to the MSuite Client](#).
- 2 On the MSuite client, choose **Backup and Restore > Backup system data** from the main menu.

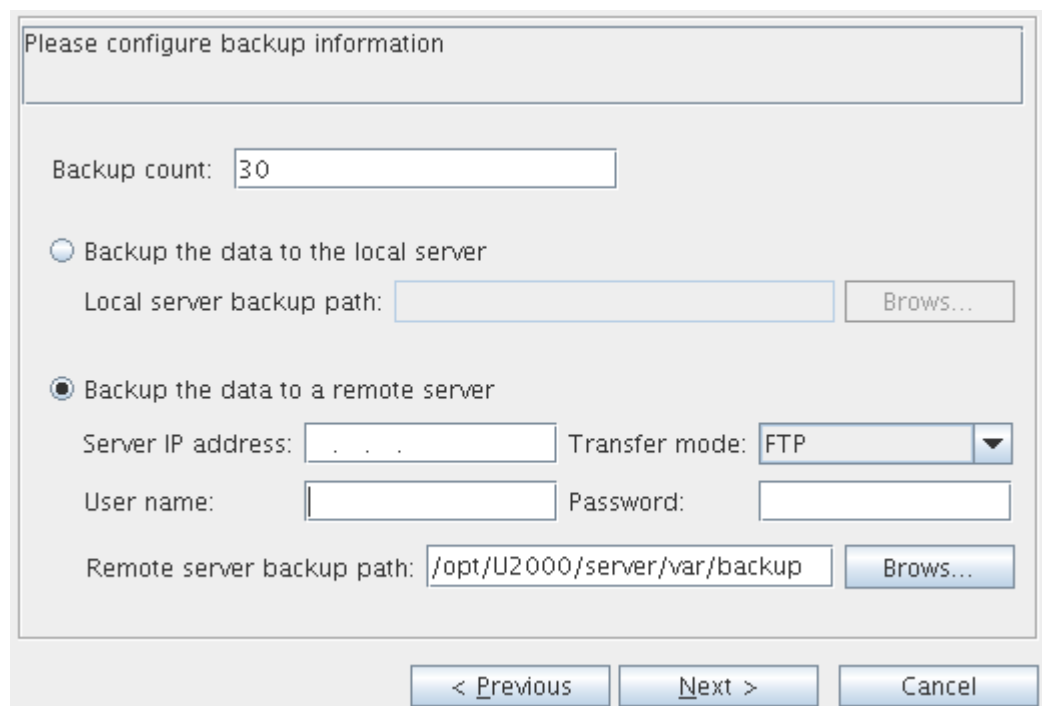
3 Select **Data Backup-Binary Mode(Recommended)**, and then click **Next**.

 **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.



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.

## C.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.

### [C.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.

### [C.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.

### C.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.9.9 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 [C.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**.

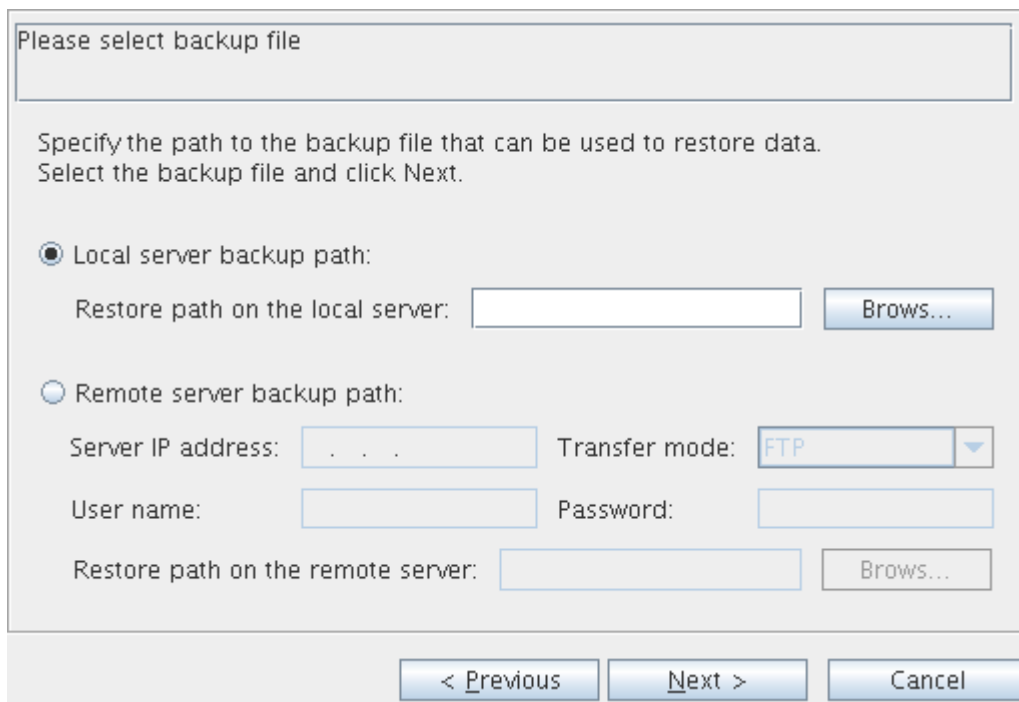
 **NOTE**

**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 [C.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.9.8 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.

## C.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.9.9 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.

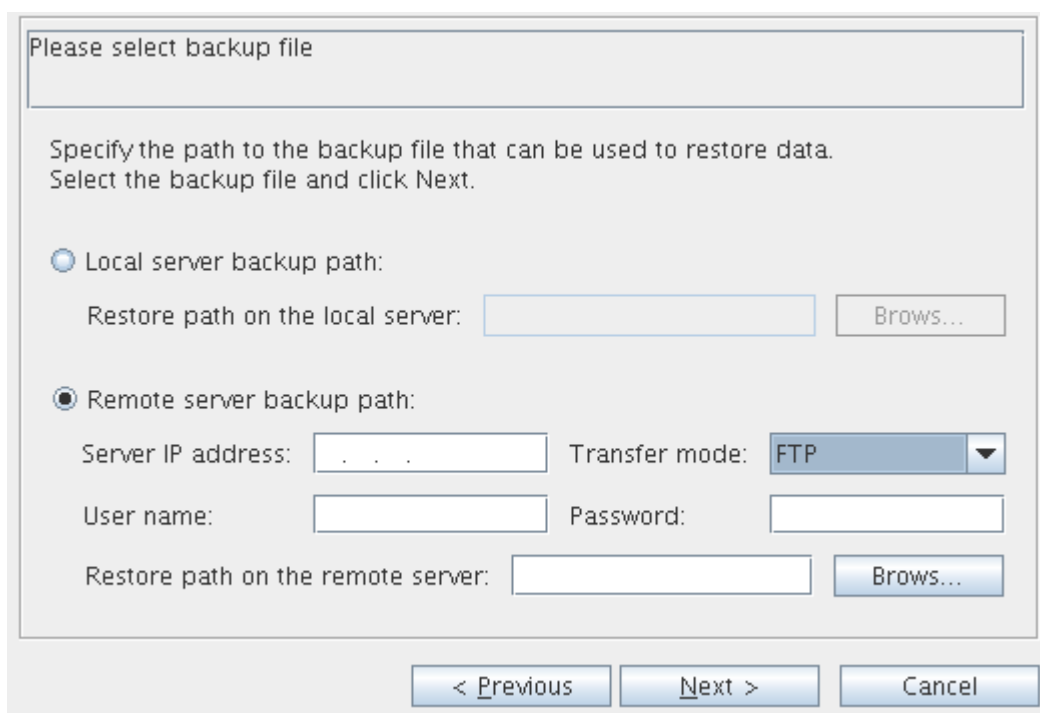
## Procedure

- 1 Log in to the MSuite client. For details, see [C.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 [C.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.9.8 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.

## C.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.

### [C.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.

### [C.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.



### C.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.9.12 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 [C.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 [C.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.9.11 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.

## C.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.9.12 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`

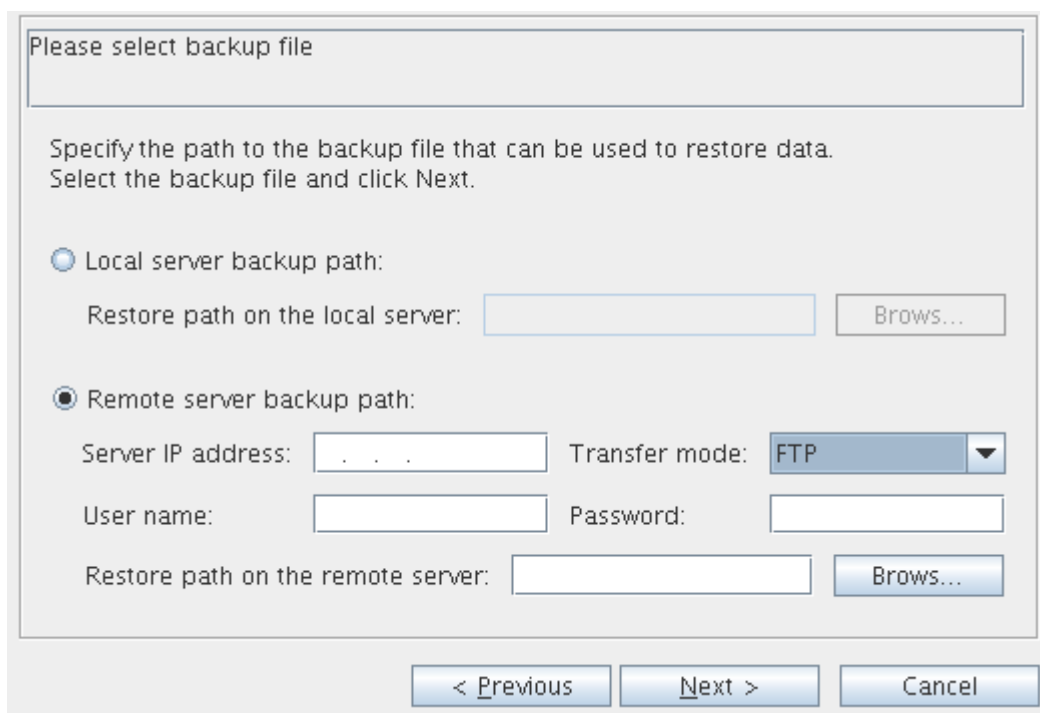
## Procedure

- 1 Log in to the MSuite client. For details, see [C.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 [C.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.9.11 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.

## C.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.

### C.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.

### C.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.

### C.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.9.15 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:  

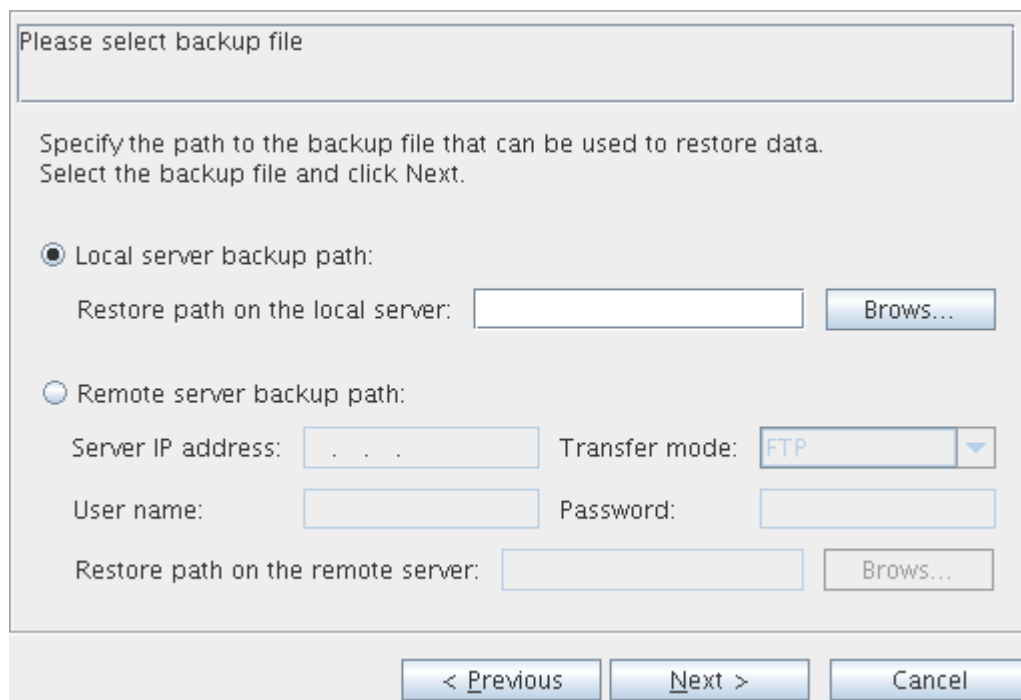
```
/etc/init.d/u2kdaem stop
```
- The database must be running. If the database is not running, see [A.7.4 How Can I Start the Oracle Database \(Single-Server System\)?](#).

#### Procedure

- 1 Log in to the MSuite client on the master server of active site. For details, see [C.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 [C.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.9.30 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.9.14 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.

## C.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.9.15 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.7.4 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.

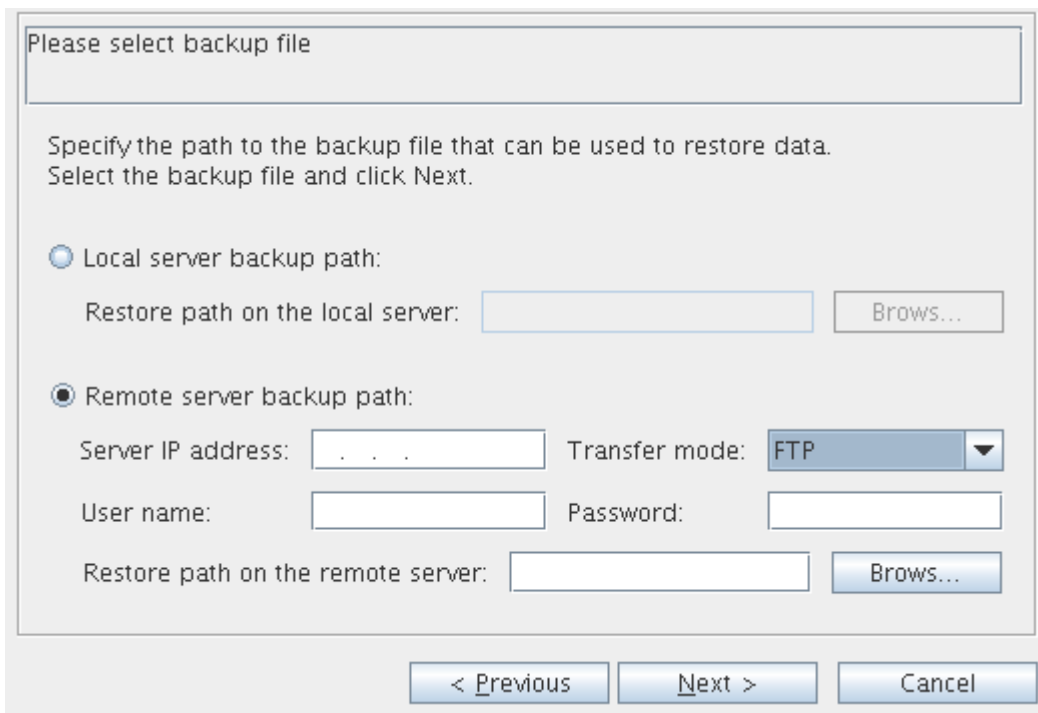


 **NOTE**

- 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 [C.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 [C.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.9.30 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.9.14 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.

## C.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.

### C.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.

### C.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.

### C.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.9.18 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 [5.12 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 [C.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 [C.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.9.17 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.

## C.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.9.18 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 [5.12 Restoring Data of a U2000 High Availability System \(Cross-U2000\)](#).

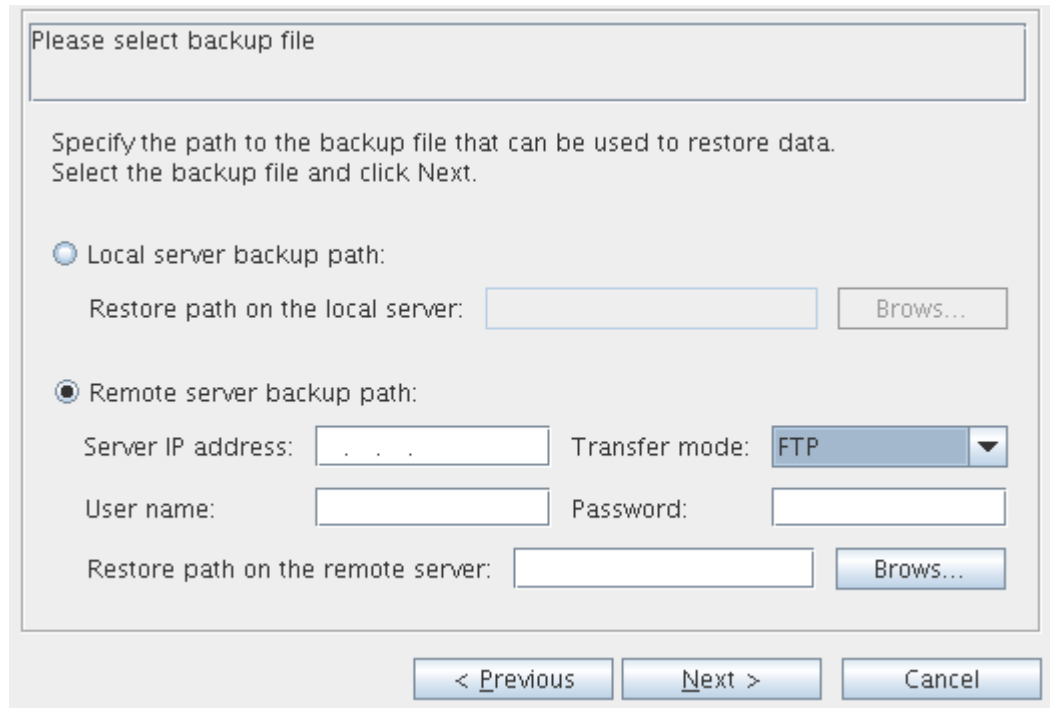
## Procedure

- 1 Log in to the MSuite client on the active site. For details, see [C.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 [C.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.9.17 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.

## C.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.

### [C.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.

### [C.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.

### C.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.9.21 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 [5.12 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 [C.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 [C.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.9.20 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.

## C.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.9.21 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 [5.12 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 [C.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 [C.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.9.20 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.

## C.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.

### C.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.

### C.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.

### C.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.9.24 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.7.4 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 [5.12 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 [C.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 [C.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.9.30 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 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.

### C.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.9.24 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.7.4 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 [5.12 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 [C.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 [C.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.9.30 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 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.

## C.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 [C.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 [5.9 Restoring U2000 High Availability System \(Windows\) Data](#).
  - For details about restoring data for the High Availability System (Solaris), see [5.10 Restoring U2000 High Availability System \(Solaris\) Data](#).
  - For details about restoring data for the High Availability System (SUSE Linux-Distributed), see [5.11 Restoring U2000 High Availability System \(SUSE Linux-Distributed\) Data](#).
- 3 Connect the primary and secondary sites. For details, see [C.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.

## C.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.9.9 How to End the Processes of the U2000 Single-Server System on Windows](#).
  - For the Single-Server System (Solaris), see [A.9.12 How to End the Processes of the U2000 Single-Server System on Solaris](#).
  - For the Single-Server System (SUSE Linux-Distributed), see [A.9.15 How to End the Processes of the U2000 Single-Server System \(SUSE Linux-Distributed\)](#).
  - For the High Availability System (Windows), see [A.9.18 How to End the U2000 Processes of the High Availability System \(Windows\)](#).

- For the High Availability System (Solaris), see [A.9.21 How to End the U2000 Processes of the High Availability System \(Solaris\)](#).
  - For the High Availability System (SUSE Linux-Distributed), see [A.9.24 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.7.4 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.7.3 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. For more information, see [9.3.3 Locking a 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 [C.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. For more information, see [9.3.4 Unlocking a Resource Group](#).

----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. For more information, see [1 Starting the U2000 System](#).

---

# D Reference of Solaris/Linux Commands

---

This describes the utility commands provided by the Solaris/Linux system, including the commands for operating directories, the commands for operating folders, the commands for viewing files, the commands for managing Solaris/Linux users, the commands for managing the system resource, and the commands for network communication.

## [D.1 Commands for Operating Solaris or Linux Folders](#)

This describes the commands for operating Solaris or Linux folders. This also gives function descriptions and examples.

## [D.2 Commands for Operating Solaris or Linux Files](#)

This describes the usage of the operation commands commonly used for files in the Solaris or Linux operating system, including function description and application examples.

## [D.3 Commands for Viewing Solaris or Linux Text Files](#)

This section describes the commands used for viewing Solaris or Linux text files, their functions, along with examples.

## [D.4 Commands for Managing Solaris or Linux Users](#)

This describes the user management commands that are frequently used in the Solaris or Linux operating system. This also describes the functions of these commands and gives some examples. Only the user root and the authorized users can add, modify, or delete users and user groups.

## [D.5 Commands for Managing Solaris or Linux System Resources](#)

This describes the commands for managing Solaris or Linux operating system resources. This also describes the functions of these commands and gives some examples.

## [D.6 Commands for Network Communications in the Solaris or Linux System](#)

This section describes the commands for network communication in the Solaris or Linux system. It also describes the functions of these commands and gives some examples.

## D.1 Commands for Operating Solaris or Linux Folders

This describes the commands for operating Solaris or Linux folders. This also gives function descriptions and examples.

### [D.1.1 pwd Command](#)

This topic describes the pwd command used for viewing the current working folder.

### [D.1.2 cd Command](#)

This topic describes the cd command used for switching the current folder to another folder.

### [D.1.3 mkdir Command](#)

This topic describes the mkdir command used for creating a folder.

### [D.1.4 rmdir Command](#)

This topic describes the rmdir command used for deleting an empty folder that is no longer useful.

### [D.1.5 ls Command](#)

This topic describes the ls command used for listing the files and subfolders in a specific folder.

## D.1.1 pwd Command

This topic describes the pwd command used for viewing the current working folder.

### Function

View the current working folder.

### Example

```
pwd
/export/home
```

## D.1.2 cd Command

This topic describes the cd command used for switching the current folder to another folder.

### Function

The cd command is used to switch the current folder to another folder. This command applies to both absolute and relative paths.

### Example

- To switch to the home folder, run the following command:  
# cd
- To switch to the system root directory, run the following command:  
# cd /
- To switch back one folder, run the following command:



```
cd ..
```

- To switch back two folders, run the following command:

```
cd ../../
```

- To switch to the **/export/home** folder by the absolute path, run the following command:

```
cd /export/home
```

#### NOTE

If you run the **cd** command that is not followed by any parameter, the system is switched back to the home folder.

## D.1.3 mkdir Command

This topic describes the **mkdir** command used for creating a folder.

### Function

The **mkdir** command is used to create a folder. When the path to the created folder is determined, absolute and relative paths can be used.

### Command Format

**mkdir** *option* *directory*

### Option Description

**Table D-1** Option description of the **mkdir** command

| Option    | Description                                                                                                                                                                                        |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>-p</b> | Creating a folder through recursion. If the upper-level folder of the folder to be created does not exist, the command creates the upper-level folder and then the folder that you want to create. |

### Example

To create a subfolder **data** in **/home1/omc**, run the following command:

```
mkdir /home1/omc/data
```

If the current folder is **/home1/omc**, run the following command:

```
mkdir data
```

If the current folder is **/home1** and the folder **omc** does not exist, run the following command to create the folder **omc** and then the folder **dir1**:

```
mkdir -p /home1/omc/dir1
```

## D.1.4 rmdir Command

This topic describes the `rmdir` command used for deleting an empty folder that is no longer useful.

### Function

The **`rmdir`** command is used to delete an empty folder.

To delete a non-empty folder, run the **`rm -r`** command. For details, see [D.2.4 rm Command](#).



### CAUTION

- If the folder to be deleted is not empty, you must delete the files in the folder before running the `rmdir` command.
  - To delete the current folder, you must switch to the upper-level folder.
- 

### Example

To delete the **`data`** subfolder in the **`/home1/omc`** folder, run the following command:

```
rmdir /home1/omc/data
```

If the current folder is **`/home1/omc`**, run the following command:

```
rmdir data
```

## D.1.5 ls Command

This topic describes the `ls` command used for listing the files and subfolders in a specific folder.

### Function

The **`ls`** command is used to list the files and subfolders in a folder. Run the **`ls`** command without any parameter to list the content of the current folder. Run the **`ls`** command with parameters to list the information about the size, type, and privileges of the file, and the date when the file was created and modified.

### Command Format

**`ls`** *Option* *Directory or File*

### Option Description

Several individual options and a combination of options can be used for the `ls` command. Place the prefix `-` before the options. [Table D-2](#) lists some common options.

**Table D-2** Option description of the **ls** command

| Option    | Description                                                                                                                                                                                                                                                          |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>-a</b> | Lists all files including the hidden files, that is, the files starting with a dot ., for example, the <b>.login</b> file.                                                                                                                                           |
| <b>-F</b> | Specifies the type of a file by suffix signs.<br>The meaning of the suffixes are as follows: <ul style="list-style-type: none"><li>● /: for folder files</li><li>● =: for pipe files</li><li>● @: for sign-linking files</li><li>● *: for executable files</li></ul> |
| <b>-l</b> | Lists the detailed information about a file, such as the file type, privileges, number of links, owner, file group, file size, file name, and the date of the last modification.                                                                                     |

If the file is a sign-linking file, then the **->** sign is added at the end of the file name for pointing to the linked file.

## Example

To view the long-form content of the files in the current folder, run the following command:

```
ls -l | more
```

```
total 11094632
drwxr-xr-x 2 sybase staff 1024 Sep 5 2001 bin
drwxr-xr-x 14 sybase staff 512 Sep 5 2001 charsets
drwxr-xr-x 3 sybase staff 512 Sep 5 2001 collate
drwxr-xr-x 2 sybase staff 512 Sep 5 2001 config
-rw-r--r-- 1 sybase staff 2048000000 Mar 6 09:50 data_dev.dat
drwxr-xr-x 2 sybase staff 512 Sep 5 2001 devlib
drwxr-xr-x 7 sybase staff 512 Sep 5 2001 diag
drwxr-xr-x 2 sybase staff 512 Sep 5 2001 hs_data
drwxr-xr-x 2 sybase staff 512 Sep 5 2001 include
drwxr-xr-x 7 sybase staff 512 Sep 5 2001 init
drwxr-xr-x 3 sybase staff 512 Sep 5 2001 install
-rw-r--r-- 1 sybase staff 268 Sep 5 2001 interf.old
-rw-r--r-- 1 sybase staff 402 Oct 29 15:25 interfaces
drwxr-xr-x 2 sybase staff 1024 Sep 5 2001 lib
drwxr-xr-x 2 sybase staff 512 Sep 5 2001 license
drwxr-xr-x 6 sybase staff 512 Sep 5 2001 locales
-rw-r--r-- 1 sybase staff 2048000000 Mar 6 10:51 log_dev.dat
-rw-r--r-- 1 sybase staff 2048000000 Mar 6 10:36 log_dev1.dat
drwxr-xr-x 5 sybase staff 512 Sep 5 2001 pad
-rw-r--r-- 1 sybase staff 5242880 Feb 19 10:10 phase2.dat
drwxr-xr-x 8 sybase staff 512 Sep 5 2001 sample
--More--
```

After you run the **ls -l** command, the result may be displayed in several screens. To view the file contents, one screen at a time, run one of the following commands:

- **# ls -la | more**
- **\$ ls -la>ccc**

Save the command output to the **ccc** file, and then run the following command to view the output on screen at a time:

```
more ccc
```

After you run the **ls -l** command, seven columns of information are displayed, which are described as follows:

- The first column consists of 10 characters. The first character indicates the file type. For example, the character **-** refers to a common file and the character **d** refers to a folder. The following nine characters are three triplets indicating the access privileges of the file owner. The first triplet pertains to the owner, the middle triplet pertains to members of the user group, and the right-most one pertains to other users in the system. For example, the characters **r**, **w**, and **x** indicate that the user has the privileges to read, write, and execute a file, whereas the character **-** indicates that the user does not have any relevant privileges for the file.
- The second column indicates the number of links of the file.
- The third and fourth columns display information such as the owner of the file, and the user group to which the file belongs.
- The fifth column shows the size of the file in bytes.
- The sixth column shows the time and date when the file is last modified.
- The seventh column shows the file name.

## D.2 Commands for Operating Solaris or Linux Files

This describes the usage of the operation commands commonly used for files in the Solaris or Linux operating system, including function description and application examples.

### [D.2.1 vi Command](#)

This topic describes the **vi** command used for creating and modifying text files.

### [D.2.2 cp Command](#)

This topic describes the **cp** command used for copy the contents of a file to another file.

### [D.2.3 mv Command](#)

This topic describes the **mv** command used for moving and renaming a file.

### [D.2.4 rm Command](#)

This topic describes the **rm** command used for deleting a specific file.

### [D.2.5 chmod Command](#)

This topic describes the **chmod** command used for changing the access rights of a directory or a file.

### [D.2.6 chown Command](#)

This topic describes the **chown** command used for changing the owner of a file.

### [D.2.7 chgrp Command](#)

This topic describes the **chgrp** command used for moveing all files from the user group to which you belong to another user group.

### [D.2.8 find Command](#)

This topic describes the **find** command used for searching for a file that meets the preset conditions in the specified folders and subfolders.

### [D.2.9 tar Command](#)

This topic describes the tar command used for combining several files into one archive and save it to a tape or disk.

#### [D.2.10 gtar Command](#)

This topic describes the gtar command used for combining multiple files into an archive and storing it in a tape or disk.

#### [D.2.11 compress Command](#)

This topic describes the compress command used for compressing files.

#### [D.2.12 uncompress Command](#)

This topic describes the uncompress command used for decompressing files.

#### [D.2.13 pack Command](#)

This topic describes the pack command used for compressing files and saving memory space.

#### [D.2.14 unpack Command](#)

This topic describes the unpack command used for extracting files.

#### [D.2.15 pkgadd Command](#)

This topic describes the pkgadd command used for sending a file package to the system for execution.

#### [D.2.16 pkgrm Command](#)

This topic describes the pkgrm command used for removing a package from the system.

## D.2.1 vi Command

This topic describes the vi command used for creating and modifying text files.

### Function

As a powerful text editing tool, the vi editor is used to create and modify text files.

The vi editor works in two modes:

- Text input mode: to enter the text
- Command mode: to enter the control command

### Format

- To start the vi editor, enter the following command:  
**vi** *file name*
- [Table D-3](#) lists the operations in the text input mode.

**Table D-3** Operations in the text input mode

| Command  | Function                                                                         |
|----------|----------------------------------------------------------------------------------|
| <b>a</b> | Insert text immediately after the cursor (append).                               |
| <b>A</b> | Insert text at the end of the line where the cursor is.                          |
| <b>i</b> | Insert text immediately before the cursor (insert).                              |
| <b>I</b> | Insert text before the first nonblank character in the line where the cursor is. |

| Command  | Function                                                        |
|----------|-----------------------------------------------------------------|
| <b>o</b> | Insert a new line below the current one and insert text (open). |
| <b>O</b> | Insert a new line above the current one and insert text.        |

- **Table D-4** lists the operations related to moving the cursor in the text input mode.

**Table D-4** Operations related to moving the cursor in the text input mode

| Command           | Function                                                                                                      |
|-------------------|---------------------------------------------------------------------------------------------------------------|
| <b>h</b>          | Move the cursor one character left.                                                                           |
| <b>j</b>          | Move the cursor one character down.                                                                           |
| <b>k</b>          | Move the cursor one character up.                                                                             |
| <b>l</b>          | Move the cursor one character right.                                                                          |
| <b>Line No. G</b> | Move the cursor to a specified line. For example, <b>1G</b> means that the cursor is moved to the first line. |
| <b>G</b>          | Move the cursor to the end of the text.                                                                       |

- **Table D-5** lists the operation for exiting the text input mode and switching to the command mode.

**Table D-5** Operation for exiting the text input mode and switching to the command mode

| Command    | Function                                                   |
|------------|------------------------------------------------------------|
| <b>ESC</b> | Exit the text input mode and switches to the command mode. |

- **Table D-6** lists the operations related to deleting characters in the command mode.

**Table D-6** Operations related to deleting characters in the command mode

| Command   | Function            |
|-----------|---------------------|
| <b>x</b>  | Delete a character. |
| <b>dd</b> | Delete a line.      |

- Exit the vi editor.  
All the commands that exit vi editor must be run in the command mode. Therefore press **ESC** before running the commands. **Table D-7** describes the commands for exiting the vi editor.

**Table D-7** Commands for exiting the vi editor

| Command    | Function                                             |
|------------|------------------------------------------------------|
| <b>:wq</b> | Save a file and exit the vi editor.                  |
| <b>:q</b>  | Exit from the vi editor without saving the file.     |
| <b>:q!</b> | Exit from the vi editor and discard all the changes. |
| <b>:w</b>  | Save a file other than exit the vi editor.           |

## D.2.2 cp Command

This topic describes the **cp** command used for copy the contents of a file to another file.

### Function

The **cp** command is used to copy the contents of a file to another file.

### Command Format

**cp** *option source file object file*

### Option Description

The option **-r** indicates recursively copying a folder. That is, when copying a folder, copy the files and subfolders included in the folder, and files and subfolders in the subfolders until the last level of the folder.

### Example

To copy the **old\_filename** file in the current folder to the file **new\_filename**, run the following command:

```
cp old_filename new_filename
```

## D.2.3 mv Command

This topic describes the **mv** command used for moving and renaming a file.

### Function

The **mv** command is used to move and rename a file.



### CAUTION

- After you run the **mv** command, only the target file instead of the source file exists.
  - After you run the **cp** command, the source file still exists and the target file is generated.
-

## Command Format

**mv** *source file object file*

## Example

To move the **old\_filename** file in the root directory to the **/home1/omc** folder, and rename the source file to **new\_filename**, run the following command:

```
mv old_filename /home1/omc/new_filename
```

## D.2.4 rm Command

This topic describes the **rm** command used for deleting a specific file.

### Function

The **rm** command is used to delete a file.



### CAUTION

- In the SolarisSUSE Linux system, a file, once deleted, cannot be restored. Therefore, use the **-i** option to avoid the deletion of a file by mistake.
  - To delete a folder, run either of the following commands: **rmdir** or **rm -r**. The difference between the two commands is: **rmdir** deletes only empty folders but **rm -r** deletes any folder.
- 

## Command Format

**rm** *Option file*

## Option Description

- **-i**: refers to interactive operations. Your confirmation is required before a command is run.
- **-r**: recursively deletes a folder. That is, when deleting a folder, delete the files and subfolders included in the folder, and files and subfolders in the subfolders until the root folder.
- **-f**: removes all files (whether write-protected or not) in a directory without prompting the user.

## Example

To delete the **old\_filename** file in the current folder, run the following command:

```
rm -i old_filename
```

## D.2.5 chmod Command

This topic describes the **chmod** command used for changing the access rights of a directory or a file.



## Function

The **chmod** command is used to change the access rights of a directory or a file.

## Format

**chmod option** *directory or file*

Based on different notation methods of the option in the command, two modes are available:

- Symbol mode  
**chmod objectoperator rights**
- Digit mode  
**chmod lmn** *file*

## Option Description

- Symbol mode  
[Table D-8](#) lists common options in symbol mode of the **chmod** command.

**Table D-8** Common options in symbol mode of the **chmod** command

| Option          | Option Detail | Description                                                                                |
|-----------------|---------------|--------------------------------------------------------------------------------------------|
| <b>Object</b>   | <b>u</b>      | Owner of a file                                                                            |
|                 | <b>g</b>      | Users sharing the same group with the file owner                                           |
|                 | <b>o</b>      | Other users except the file owner and the users sharing the same group with the file owner |
|                 | <b>a</b>      | All users                                                                                  |
| <b>Operator</b> | <b>+</b>      | Add a right                                                                                |
|                 | <b>-</b>      | Cancel a right                                                                             |
|                 | <b>=</b>      | Set a right                                                                                |

- Digit mode  
The option **lmn** represents the following digits:
  - **l**: the rights of the owner
  - **m**: the rights of the users sharing the same group with the owner
  - **n**: the rights of other users in the system

The value of each digit is equal to the sum of the values of r (read right), w (write right), x (execute right), or - (no right) in each group. In each group, r = 4, w = 2, x = 1, and - = 0. In the following example `-rwxr-xr-- 1 rms sbsrms 46098432 May 12 16:02 sdh*`, the access rights of the file **sdh** is represented by the symbols `rwxr-xr--`. The nine symbols are divided into three groups, with three symbols as a group. The three groups represent the rights of the file owner, the rights of the users sharing the same group with the file owner, and the rights of other users in the system. The three groups can

be represented in digits 754, which is calculated according to the formulas:  $7 = 4 + 2 + 1$ ,  $5 = 4 + 0 + 1$ , and  $4 = 4 + 0 + 0$ .

## Parameter Description

*Directory or File*: indicates the name of the directory or file whose rights are changed.

## Example

- Symbol mode

Authorize the **file1** owner with the read, write, and execute rights. Authorize the users sharing the same group with the file owner with the read and execute rights. Authorize other users with the read and execute rights. Run the following command:

```
chmod u=rwx,go=rx file1
```

To authorize all the users with the read and write rights, run the following command:

```
chmod a=rw file2
```

- Digit mode

Authorize the **file1** owner with the read, write, and execute rights. Authorize the users sharing the same group with the file owner with the read and execute rights. Authorize other users with the read and execute rights. Run the following command:

```
chmod 755 file1
```

To authorize all the users with the read and write rights, run the following command:

```
chmod 666 file2
```

 **NOTE**

- To configure the rights of a file for users in a group and other users in the system in symbol mode, you must authorize these users with the execute right of the directory where a file exists. Run the following command for the directory that requires you to set rights:

```
chmod u=rw,+x .
```

You can also run the following command:

```
chmod u=rwx,go=x .
```

In this command, the symbol "." indicates the current directory.

- In digit mode,  $r = 4$ ,  $w = 2$ ,  $x = 1$ , and  $- = 0$ . These mappings are set according to the binary mode. For the three symbols in a group, which represent the read right, the write right, and the execute right, assign the binary value 1 if a symbol has the corresponding right and assign the binary value 0 if a symbol does not have the corresponding rights. Take the previous file **sdh** as an example. The file rights are represented by the symbols **rwxr-xr--**. After converting the symbols into a binary value, you can obtain "111101100". The binary value is divided into three 3-digit groups, with each group representing a file right. After converting the binary value of each group into a decimal value, you can obtain three values: 7, 5, and 4.

## D.2.6 chown Command

This topic describes the **chown** command used for changing the owner of a file.

### Function

The **chown** command is used to modify the owner of a file. In most SolarisSUSE Linux systems, this command can be run only by the super user.

## Command Format

**chown** **Option** *owner file*

### Option Description

- **-f**: runs the command forcibly without displaying errors
- **-R**: recursive folder

### Parameter Description

- *Owner*: the modified owner
- *File*: the file of the owner to be modified

### Example

- Assume that there is a user **new\_owner** and a **file** in the system. Run the following command to change the owner of the **file** to **new\_owner**:  
# **chown** *new\_owner file*
- Assume that there is a user **test** in the system. Change the owner of all files in the **/export/home** folder and the subfolders to **test**:  
# **chown -R** *test /export/home*

## D.2.7 chgrp Command

This topic describes the **chgrp** command used for moving all files from the user group to which you belong to another user group.

### Function

The **chgrp** command is used to move all files from the user group to which you belong, to another user group. That is, you belong to at least two user groups at the same time.

## Command Format

**chgrp** **Option** *group file*

### Option Description

- **-f**: runs the command forcibly without displaying errors
- **-R**: recursive folder

### Parameter Description

- *Group*: the modified user group
- *File*: the file the user group of which is to be modified

### Example

To change the user group **file** to **new\_group**, run the following command:

```
chgrp new_group file
```

**CAUTION**

The new user group to which a file is moved should be created. Run the **groups** command to list the groups to which you belong. For details on how to create a user group, see [D.4 Commands for Managing Solaris or Linux Users](#).

After the owner or group of a folder is changed, the folder does not belong to that user or user group any more. The attributes of the subfolders and files in the folder, however, are retained.

Run the **chown** command to modify the owner and the user group of a file at the same time:

```
chown omc:staff file1
```

For example, run the command to modify the owner of **file1** to omc and the group to staff.

## D.2.8 find Command

This topic describes the **find** command used for searching for a file that meets the preset conditions in the specified folders and subfolders.

### Function

The **find** command is used to search for a file that meets the preset conditions in the specified folders and subfolders. By using this command, you can find the file even if you forget the correct path of the file.

### Command Format

```
find folder condition
```

### Parameter Description

- **Folder**: indicates the folder to be searched. You can enter multiple folder names. Separate the folder names by using spaces.
- **Condition**: indicates the conditions for file search, such as the file name, owner, and time of the last modification.

[Table D-9](#) describes the conditions for file search.

**Table D-9** Conditions for file search

| Condition                | Description                                                                                                |
|--------------------------|------------------------------------------------------------------------------------------------------------|
| <b>-name</b> <i>name</i> | The name of the file or folder to be searched. Wildcards, such as <b>-name</b> <i>'*.c'</i> , can be used. |
| <b>-print</b>            | Prints the path that meets the conditions.                                                                 |
| <b>-size</b> <i>n</i>    | Searches for the files that use <i>n</i> blocks.                                                           |

| Condition                        | Description                                                                                                                                                                                                                                       |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>-type</b> <i>x</i>            | Searches for files by file type. The file type <i>x</i> includes: <ul style="list-style-type: none"><li>● <b>d</b>: directory</li><li>● <b>f</b>: file</li><li>● <b>b</b>: block</li><li>● <b>c</b>: character</li><li>● <b>p</b>: pipe</li></ul> |
| <b>-user</b> <i>user</i>         | Searches all files of user. The value of user can be a user name or UID.                                                                                                                                                                          |
| <b>-group</b> <i>group</i>       | Searches all files of the user group. The value of group can be a user group name or GID.                                                                                                                                                         |
| <b>-links</b> <i>n</i>           | Searches all files with the number of links as <i>n</i> .                                                                                                                                                                                         |
| <b>-atime</b> <i>n</i>           | Searches the files accessed before <i>n</i> days.                                                                                                                                                                                                 |
| <b>-mtime</b> <i>n</i>           | Searches the files modified before <i>n</i> days.                                                                                                                                                                                                 |
| <b>-exec</b> <b>command</b> { \; | Uses the found file as the object of the command to be run. Put the parameters to be used in the command execution between { and }.                                                                                                               |

**Table D-10** describes the logical operators of conditions.

**Table D-10** Logical operators of conditions

| Logical Operator | Meaning                                                                                    | Example                      | Description                                                     |
|------------------|--------------------------------------------------------------------------------------------|------------------------------|-----------------------------------------------------------------|
| <b>!</b>         | non                                                                                        | <b>! -name</b> <i>"*.c"</i>  | All the files except those with the extension name as <i>.c</i> |
| <b>-o</b>        | or                                                                                         | <b>-size +10 -o -links 3</b> | All the files with more than 10 blocks or with 3 links          |
|                  | and<br>Condi<br>tions in<br>and<br>relatio<br>nships<br>are<br>separat<br>ed by<br>spaces. | <b>-size +10 -links 3</b>    | All the files with more than 10 blocks and with 3 links         |

In the preceding table, +10 stands for more than 10 blocks and -10 for fewer than 10 blocks.

## Example

To search for files in the **/tmp** folder with the file name starting with **c**, and then print the paths, run the following command:

```
find /tmp -name "c*" -print
```

```
/tmp/ctisql_0WBjgt
/tmp/ctisql_0dznJ_
/tmp/ctisql_0CpW34
/tmp/ctisql_0FO4vs
```

To search the file **test** in the current folder and then print the paths, run the following command:

```
find . -name test -print
```

```
./Report/reloc/resin1.2.0/conf/test
./Report/reloc/resin1.2.0/doc/examples/login/WEB-INF/classes/test
./Report/reloc/resin1.2.0/doc/examples/tags/WEB-INF/classes/test
```

### NOTE

- The search may take several minutes. To save time, you can run this command in the background. That is, the output for the command is exported to a file for later query. End the command line with **&** so that the system runs the command in the background. For example:  

```
find / -name "abc*" -print> abc.file &
```
- After the search is complete, run the following command to view the result of the search:  

```
cat abc.file
```
- Different users may have different privileges for the same file. Therefore, ordinary users may find only some files of the system. To list all the files that meet the set conditions, log in as a super user and search from the root directory.

## D.2.9 tar Command

This topic describes the **tar** command used for combining several files into one archive and save it to a tape or disk.

### Function

The **tar** command is used to combine several files into one archive and save it to a tape or disk. When one of the files is required, obtain the file directly from an archive.

### Command Format

```
tar function options modification options file
```

### Option Description

- **function options**: sets the actions, such as read and write, of the tar command
- **modification options**: modifies the actions of the tar command

**Table D-11** describes the options of the tar command.

**Table D-11** Option description for the **tar** command

| Option               | Specified Option | Description                                                                                                                                   |
|----------------------|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| Function options     | <b>r</b>         | Adds the specified file to an archive.                                                                                                        |
|                      | <b>x</b>         | Reads a file in an archive. If the file name is a folder, this option reads the subfolders included in the folder. This option is often used. |
|                      | <b>c</b>         | Creates an archive. This option is often used.                                                                                                |
|                      | <b>g</b>         | Creates a file at the beginning of an archive rather than add the file in the last file.                                                      |
| Modification options | <b>v</b>         | Activates the display mode. The names of all the processed files are displayed. This option is often used.                                    |
|                      | <b>w</b>         | Activates the confirmation mode. Your confirmation is required before each file is processed.                                                 |
|                      | <b>f</b>         | Indicates that an archive is a file. If this parameter is skipped, the preset tape or disk is used as the object. This option is often used.  |

## Example

- Run the **tar** command to back up files.  
To back up all the files and subfolders in the **/export/home** folder in the current folder to the default device and view the file information during the backup, run the following command:  

```
tar cv /export/home
```

  
In current folder, back up all the files and subfolders in the **/export/home** folder to the **databak.tar** file, and to view the file information during the backup, run the following command:  

```
tar cvf databak.tar /export/home
```
- Use **tar** to restore files.  
To restore the files in the default device to a hard disk, and to view the file information during the restoration, run the following command:  

```
tar xv
```

  
In current folder, restore the **databak.tar** file to the **/export/home** folder, and to view the file information during the restoration, run the following command:  

```
tar xvf databak.tar
```

**CAUTION**

- Do not enter "-" on the left of the function and modification options in the **tar** command.
- Run the following **tar** command to pack several files into a package:  

```
tar cvf filebak.tar file1 file2 file3
```
- Run the previous command to pack **file1**, **file2**, and **file3** into a package named **filebak.tar**.
- The names of the disk and tape devices used in file backup and restoration in the **tar** command may vary according to the SolarisSUSE Linux system. Check carefully before running the command.

## D.2.10 gtar Command

This topic describes the **gtar** command used for combining multiple files into an archive and storing it in a tape or disk.

### Function

The **gtar** command can merge multiple files into an archive and store it in tapes or disks. You can obtain the required files from an archive, if required.

### Format

**gtar function options modification options file to be backed up or restored**

### Option Description

- Function option: sets the actions of the **gtar** command, such as read or write.
- Modification option: modifies the actions of the **gtar** command.

**Table D-12** lists some options.

**Table D-12** Descriptions of **gtar** command options

| Option              | Example | Description                                                                                                          |
|---------------------|---------|----------------------------------------------------------------------------------------------------------------------|
| Function option     | r       | Adds the specified file to end of an archive.                                                                        |
|                     | x       | Reads a file in the archive. If the name is a directory, its sub directories are also read. This option is common.   |
|                     | c       | Creates a new archive. This option is common.                                                                        |
|                     | g       | Creates a file from the beginning of the archive instead of the end of the last file.                                |
| Modification option | v       | Starts the display mode. The <b>gtar</b> command can display all names of the processed file. This option is common. |
|                     | w       | Activates the confirm mode. The <b>gtar</b> command requests you to confirm before processing each file.             |



| Option | Example | Description                                                                                                                                |
|--------|---------|--------------------------------------------------------------------------------------------------------------------------------------------|
|        | f       | Indicates that the archive is a file. Omission of this option indicates that the object is the preset disk or tape. This option is common. |

## Instance

- Run the **gtar** command to back up files.  
In the current directory, back up all the files and folders in **/export/home/sybdev** to the default device. During the backup, the file information is displayed.  
# **gtar cv** /export/home/sybdev  
In the current directory, back up all the files and folders in **/export/home/sybdev** and save them as **databak.tar**. During the backup, the file information is displayed.  
# **gtar cvf databak.tar** /export/home/sybdev
- Run the **gtar** command to restore files.  
Restore the files of default devices in the backup files to a hard disk. During the restoration, the file information is displayed.  
# **gtar xv**  
In the current directory, decompress the backup file **databak.tar** to **/export/home/sybdev**. During the restoration, the file information is displayed.  
# **gtar xvf databak.tar**



### CAUTION

- There is no - symbol before the function option and modification option of **gtar**.
  - The **gtar** command can pack multiple files. The command is as follows:  
# **gtar cvf filebak.tar file1 file2 file3**
  - This command packs the three files, that is, **file1**, **file2**, and **file3**, into the file named **filebak.tar**.
  - Under different Solaris systems, when using **gtar** to back up or restore files, note that names of the floppy disk and tape are different. Ensure that you use the right names.
- 

## D.2.11 compress Command

This topic describes the compress command used for compressing files.

### Function

The compress command is used to compress files and save the memory space. The name of the compressed files ends with **.Z**. The command for decompressing such files is **uncompress**.

### Command Format

**compress** *file*

## Example

To compress a **file**, run the following command:

```
compress file
```



### CAUTION

The difference between the **tar** command and the file compressing commands is as follows:

The **tar** command packs or combines files and packs many folders or files into a package. To compress the combined files **\*.tar**, use the **compress** or **pack** command.

---

## D.2.12 uncompress Command

This topic describes the uncompress command used for decompressing files.

### Function

The uncompress command is used to decompress the compressed files. The command for compressing files is **compress**.

### Command Format

```
uncompress compressed file ending with ".Z"
```

## Example

To decompress the **file.Z** file, run the following command:

```
uncompress file.Z
```

## D.2.13 pack Command

This topic describes the pack command used for compressing files and saving memory space.

### Function

Run the pack command to compress files. The name of the compressed files ends with **.Z**. The space achieved through compression depends on file types. To extract files, use the **unpack** command.

### Command Format

```
pack file
```

## Example

To pack a **file**, run the following command:

```
pack file
```



## CAUTION

- Do not run the **pack** command to compress files of small sizes. To compress such files, use the pack command with the option **-f** for forced compression.  
# **pack -f filename**
  - The difference between the **tar** command and the file compression commands is as follows:  
The **tar** command packs or combines files and packs many folders or files into a package. To compress the combined files **\*.tar**, use the **compress** or **pack** command.
- 

## D.2.14 unpack Command

This topic describes the unpack command used for extracting files.

### Function

The unpack command is used to extract the packed files. To pack files, use the **pack** command.

### Command Format

**unpack** *compressed file ending with ".Z"*

### Example

To extract the **file.Z** file, run the following command:

```
unpack file.Z
```

## D.2.15 pkgadd Command

This topic describes the pkgadd command used for sending a file package to the system for execution.

### Function

The pkgadd command is used to send a file package to the system for execution. To remove a package from the system, run the **pkgrm** command.

### Command Format

**pkgadd** *option file package name*

### Option Description

**-d device**: to install or copy a package from the device. The device can be an absolute path, the identifier of a tape, or a disk such as **/var/tmp** or **/floppy/floppy\_name**, or a device name such as **/floppy/floppy0**.

### Example

To send a file package in the current folder to the **file1** file, run the following command:

```
pkgadd -d .file1
```

The dot in the command indicates that the folder is the current folder.

## D.2.16 pkgrm Command

This topic describes the pkgrm command used for removing a package from the system.

### Function

The pkgrm command is used to remove a package from the system. To pack and send a package to the system, use the pkgadd command.

### Command Format

```
pkgrm option file package name
```

### Example

To remove the **file1** file, run the following command:

```
pkgrm file1
```

## D.3 Commands for Viewing Solaris or Linux Text Files

This section describes the commands used for viewing Solaris or Linux text files, their functions, along with examples.

### [D.3.1 echo Command](#)

This topic describes the echo command used for sending a character string to a standard output device such as the monitor screen.

### [D.3.2 cat Command](#)

This topic describes the cat command used for viewing the contents of a text file.

### [D.3.3 more Command](#)

This topic describes the more command used for displaying the content of a large file in different pages.

### [D.3.4 head Command](#)

This topic describes the function, format, and example of the head command.

### [D.3.5 tail Command](#)

This topic describes the tail command used for viewing the last few lines of a text.

### [D.3.6 clear Command](#)

This topic describes the clear command used for clearing the contents on the screen.

### [D.3.7 grep Command](#)

This topic describes the grep command used for searching for a character string in a text file.

## D.3.1 echo Command

This topic describes the echo command used for sending a character string to a standard output device such as the monitor screen.

## Function

The echo command is used to send a character string to a standard output device such as the monitor screen.

## Command Format

**echo** *character string* **option**

## Option Description

**Table D-13** lists five options that are frequently used.

**Table D-13** Option description of the echo command

| Option | Description                                  |
|--------|----------------------------------------------|
| \c     | The RETURN character is not displayed.       |
| \0n    | <i>n</i> is an 8-digit ASCII character code. |
| \t     | The TAB character is displayed.              |
| \n     | The RETURN character is displayed.           |
| \v     | The vertical TAB character is displayed.     |

## Example

```
echo $HOME
```

```
/export/home
```

**/export/home** displayed on the screen is the meaning of the character string "\$HOME".

To prevent the system from displaying RETURN, run the following command:

```
echo $HOME "\c"
```

```
/export/home
```

Or:

```
echo "$HOME \c"
```

```
/export/home
```

### NOTE

The options \c, \0n, \t, \n, and \v are displayed in the character string enclosed in quotation marks. The quotation marks can quote either one option or multiple options.

## D.3.2 cat Command

This topic describes the cat command used for viewing the contents of a text file.

## Function

The cat command is used to view the contents of a text file.

## Command Format

**cat** *option file*

## Option Description

- **-n**: number of each line of the displayed text
- **-v**: to view nonprinting characters rather than TAB and RETURN

## Example

To view the contents of the **cat\_Table.txt** file, run the following command:

```
cat cat_Table.txt
```

| Name         | Object_type | Owner |
|--------------|-------------|-------|
| tbl128Addr   |             | cat   |
| user table   |             |       |
| tbl128IP     |             | cat   |
| user table   |             |       |
| tbl128Name   |             | cat   |
| user table   |             |       |
| tblAdapterIP |             | cat   |
| user table   |             |       |
| tblAdjCell   |             | cat   |
| user table   |             |       |
| ...          | ...         | ...   |

### NOTE

To view several files at the same time, run the following command:

```
cat file1 file2 file3
```

## D.3.3 more Command

This topic describes the more command used for displaying the content of a large file in different pages.

## Function

You can use this command to view a file on screen at a time. You can also use this command to browse the previous screens and to search for character strings.

## Command Format

**more** *option file*

## Option Description

Remember to insert the prefix - before the options when multiple options and combination of options are used. **Table D-14** lists four options that are frequently used.

**Table D-14** Option description of the more command

| Option               | Description                                                                               |
|----------------------|-------------------------------------------------------------------------------------------|
| <b>-c</b>            | Clears the screen before the content is displayed.                                        |
| <b>-w</b>            | Indicates that the system does not exit at the end of the input but waits for the prompt. |
| <b>-lines</b>        | Displays the number of lines on each screen.                                              |
| <b>+/<i>mode</i></b> | Searches for files in a preset mode.                                                      |

## Example

To view the contents of the **cat\_Table.txt** file on screen at a time, run the following command:

```
more cat_Table.txt
```

```
Name Object_type Owner

tbl128Addr user table cat
tbl128IP user table cat
tbl128Name user table cat
tblAdapterIP user table cat
tblAdjCell user table cat
...
```

### NOTE

- To view a file on screen at a time, press the following keys to perform relevant operations:
  - Space key**: to view the next screen
  - Enter key**: to view the next line
  - q**: to exit
  - h**: to view the online help
  - b**: to switch back to the previous screen
  - /word**: to search the character string "word" backward
- SolarisSUSE Linux commands can be used in combinations. For example, add **|more** after other commands to view relevant results on several screens.

## D.3.4 head Command

This topic describes the function, format, and example of the head command.

### Function

The head command is used to view the first few lines of a text file. By default, the first 10 lines are displayed.

## Command Format

**head** *value file*

### Example

To view the first three lines of the **Table.txt** file, run the following command:

```
head -3 Table.txt
```

| Name  | Object_type | Owner |
|-------|-------------|-------|
| ----- |             |       |

## D.3.5 tail Command

This topic describes the tail command used for viewing the last few lines of a text.

### Function

The tail command is used to view the last few lines of a text. By default, the last 10 lines are displayed.

## Command Format

**tail** *value file*

### Example

To view the last ten lines of the **cat\_Table.txt** file, run the following command:

```
tail cat_Table.txt
```

| Name         | Object_type | Owner |
|--------------|-------------|-------|
| -----        |             |       |
| -----        |             |       |
| tbl128Addr   |             | cat   |
| user table   |             |       |
| tbl128IP     |             | cat   |
| user table   |             |       |
| tbl128Name   |             | cat   |
| user table   |             |       |
| tblAdapterIP |             | cat   |
| user table   |             |       |
| tblAdjCell   |             | cat   |
| user table   |             |       |
| ...          | ...         | ...   |

#### NOTE

A special function of the tail command is to view the latest changes of a log file, because all the latest changes are added at the end of the log file. The command format is as follows:

```
tail -f commdrv.log
```

The option **-f** refers to the function of monitoring a file.

## D.3.6 clear Command

This topic describes the clear command used for clearing the contents on the screen.



## Function

The clear command is used to clear the contents on the screen.

## Example

To clear the screen, run the following command:

```
clear
```

## D.3.7 grep Command

This topic describes the grep command used for searching for a character string in a text file.

## Function

The grep command is used to search for a character string in a text file and to print all the lines that contain the character string.

## Command Format

```
grep character string file
```

## Example

To search the character string operation in the **ifconfig.txt** file, run the following command:

```
grep operation ifconfig.txt
```

```
used to control operation of dhcpagent(1M), the DHCP client
operation, be used to modify the address or characteristics
dhcpagent wakes up to conduct another DHCP operation on the
given, and the operation is one that
requested operation will continue.
```

To search the character string "The following options are supported" in the **ifconfig.txt** file, run the following the command:

```
grep "The following options are supported" ifconfig.txt
```

```
The following options are supported:
```



### NOTE

The character string "The following options are supported" includes spaces. Remember to enclose the character string within quotation marks in the command line.

## D.4 Commands for Managing Solaris or Linux Users

This describes the user management commands that are frequently used in the Solaris or Linux operating system. This also describes the functions of these commands and gives some examples. Only the user root and the authorized users can add, modify, or delete users and user groups.

### D.4.1 useradd Command

The useradd command is used to add a user in the Solaris or Linux system.

### D.4.2 userdel Command

This topic describes the **userdel** command used for deleting a specific user of the Solaris or Linux operating system.

#### [D.4.3 usermod Command](#)

This topic describes the **usermod** command used for modifying the user login information.

#### [D.4.4 passwd Command](#)

This topic describes the **passwd** command used for setting or changing a password for a user.

#### [D.4.5 groupadd Command](#)

This topic describes the **groupadd** command used for adding a user group in the Solaris or Linux system.

#### [D.4.6 groupdel Command](#)

This topic describes the **groupdel** command used for deleting a user group in the Solaris or Linux system.

#### [D.4.7 groupmod Command](#)

This topic describes the **groupmod** command used for modifying the information about a user group..

## D.4.1 useradd Command

The **useradd** command is used to add a user in the Solaris or Linux system.

### Function

The **useradd** command is performed to add a user in the Solaris or Linux system.

### Command Format

**useradd option new user name**

### Option Description

You can combine options of the **useradd** command. Add the prefix - before these options. [Table D-15](#) lists the common options.

**Table D-15** option description of the **useradd** command

| Option                     | Remark                                                                              |
|----------------------------|-------------------------------------------------------------------------------------|
| <b>-c</b> <i>comment</i>   | Indicate the comment.                                                               |
| <b>-d</b> <i>directory</i> | Indicate the home folder.                                                           |
| <b>-m</b>                  | Indicate the automatic creation of a home folder if the home folder does not exist. |
| <b>-g</b> <i>group</i>     | Indicate the user group that the user belongs to.                                   |
| <b>-s</b> <i>shell</i>     | Indicate the shell that the user uses.                                              |

## Example

Create a user named `omc1` in the Solaris or Linux system. The user `omc1` belongs to the `staff` user group and the home folder is `/home1/omc` that is created automatically. In addition, the comment is `Test User` and `B` shell is applied. To create a user named `omc1` in the Solaris or Linux system, run the following commands:

```
useradd -c "Test User" -d /home1/omc -m -g staff -s /usr/bin/sh omc1
```



### CAUTION

After a user is added, set the password for the added user. For details of setting the password, refer to [D.4.4 passwd Command](#). After the password is set, the user can log in as a new user.

---

## D.4.2 userdel Command

This topic describes the **userdel** command used for deleting a specific user of the Solaris or Linux operating system.

### Function

The **userdel** command is used to delete a user. Some Solaris or Linux operating systems do not allow deleting users completely. Run the **userdel** command to revoke the privileges granted to the user.

### Command Format

```
userdel user name
```

### Option Description

**-r**: Remove the user's home directory from the system. This directory must exist. The files and directories under the home directory will no longer be accessible following successful execution of the command.

- **-r**: Remove the whole home directory and the mail spool of the specified account. Files located in other directories will have to be searched for and deleted manually.
- **-f**: Work with **-r**. This option is used to force the removal of files, even if not owned by the account.

## Example

Assume that there is user `omc1` in the system. To delete the user `omc1`, run the following command:

```
userdel omc1
```

**CAUTION**

If the user has logged in, running the **userdel** command to delete the user fails. The system prompts that the user account is in use.

## D.4.3 usermod Command

This topic describes the usermod command used for modifying the user login information.

### Function

The usermod command is used to modify the user login information.

### Command Format

**usermod option** *user name*

### Option Description

The combined option of the usermod command can be used. Add the prefix - before the options. [Table D-16](#) lists the common options.

**Table D-16** Option description of the usermod command

| Option                       | Description                                                          |
|------------------------------|----------------------------------------------------------------------|
| <b>-c</b> <i>comment</i>     | Modified comment                                                     |
| <b>-d</b> <i>directory</i>   | Modified home folder                                                 |
| <b>-m</b>                    | Create a home folder automatically if the home folder does not exist |
| <b>-g</b> <i>group</i>       | Modified user group                                                  |
| <b>-s</b> <i>shell</i>       | Used shell                                                           |
| <b>-l</b> <i>new_logname</i> | Modified user name                                                   |

### Example

In SolarisSUSE Linux, modify the login information of the user **omc1**. Run the following command to change the user name to **test**, owner group to **new\_group**, main directory to **/home**, and comment to **Tester**:

```
usermod -c "Test User" -d /home1 -g new_group -l test omc1
```



## CAUTION

With the different operation system, do not run the **usermod** command to modify a user when the user has logged in, or you must reboot operation system for some settings when perform the command.

---

## D.4.4 passwd Command

This topic describes the `passwd` command used for setting or changing a password for a user.

### Function

The `passwd` command is used to set a password for an added user or to change the user password.

### Command Format

**passwd** *user name*

### Example

Assume that the user `omc1` is added. To set the password of `omc1`, run the following command:

```
passwd omc1
```



### NOTE

Enter and confirm the password according to prompts. The entered password is displayed in cipher text.

## D.4.5 groupadd Command

This topic describes the `groupadd` command used for adding a user group in the Solaris or Linux system.

### Function

The `groupadd` command is used to add a user group in the Solaris or Linux system.

### Command Format

**groupadd** *user group name*

### Example

To add the user group `staff1` in the Solaris or Linux system, run the following command:

```
groupadd staff1
```

## D.4.6 groupdel Command

This topic describes the `groupdel` command used for deleting a user group in the Solaris or Linux system.

## Function

The `groupdel` command is used to delete a user group in the Solaris or Linux system.

## Command Format

**groupdel** *user group name*

## Example

To delete the user group `staff1`, run the following command:

```
groupdel staff1
```

## D.4.7 groupmod Command

This topic describes the `groupmod` command used for modifying the information about a user group..

## Function

The `groupmod` command is used to modify the information about a user group.

## Command Format

**groupmod** *user group name*

## Parameter Description

**-n** *name*: the name of the modified user group

## Example

To modify the name of the user group `staff1` to `staff2`, run the following command:

```
groupmod -n staff2 staff1
```

## D.5 Commands for Managing Solaris or Linux System Resources

This describes the commands for managing Solaris or Linux operating system resources. This also describes the functions of these commands and gives some examples.

### [D.5.1 man Command](#)

This topic describes the `man` command used for viewing the online help about a command.

### [D.5.2 df Command](#)

This topic describes the `df` command used for viewing the free disk space.

### [D.5.3 du Command](#)

This topic describes the `du` command used for viewing the disk space used by a specific folder or file.

### [D.5.4 ps Command](#)

This topic describes the `ps` command used for viewing the status of the processes currently running in the system.

#### [D.5.5 kill Command](#)

This topic describes the `kill` command used for terminating one or more processes.

#### [D.5.6 who Command](#)

This topic describes the `who` command used for reporting the login information about all the users in the current system.

#### [D.5.7 which Command](#)

This topic describes the `which` command used for viewing the location where a command is run.

#### [D.5.8 hostname Command](#)

This topic describes the `hostname` command used for viewing or setting the host name.

#### [D.5.9 uname Command](#)

This topic describes the `uname` command used for viewing the information about the operating system.

#### [D.5.10 ifconfig Command](#)

This topic describes the `ifconfig` command used for viewing the IP address of the host.

#### [D.5.11 script Command](#)

This topic describes the `script` command used for recording in a script file all the screen input and output that occur from the time when the script command is run to the time when the exit command is entered.

#### [D.5.12 date Command](#)

This topic describes the `date` command used for viewing the current date and time of the system.

#### [D.5.13 bc Command](#)

This topic describes the `bc` command used for simple calculation.

#### [D.5.14 prtconf Command](#)

This topic describes the `prtconf` command used for checking the system configuration.

#### [D.5.15 prstat Command](#)

This topic describes the `prstat` command used for viewing the CPU usage.

## D.5.1 man Command

This topic describes the `man` command used for viewing the online help about a command.

### Function

The `man` command is used to view the online help about a command.

### Command Format

**man option command**

### Example

To view the online help about the `pwd` command, run the following command:

```
man pwd
```

Reformatting page. Wait... done

User Commands

pwd(1)

NAME

pwd - return working directory name

SYNOPSIS

/usr/bin/pwd

DESCRIPTION

pwd writes an absolute path name of the current working directory to standard output.

Both the Bourne shell, sh(1), and the Korn shell, ksh(1), also have a built-in pwd command.

ENVIRONMENT

See environ(5) for descriptions of the following environment variables that affect the execution of pwd: LC\_MESSAGES and NLSPATH.

EXIT STATUS

--More-- (30%)



#### NOTE

Not all parameters in the **man** command are command names. For example, the **man ascii** command displays all the ASCII characters and their expressions. The **man shell\_builtins** command displays the built-in command list and the shell using the commands.

## D.5.2 df Command

This topic describes the df command used for viewing the free disk space.

### Function

The df command is used to view the free disk space. The system administrator runs this command frequently to check the usage of the disk space to avoid disk failure due to data overflow.

### Command Format

**df option file system**

### Option Description

- **-l**: the local file system
- **-k**: to view the free disk space (unit: KB)
- **-h**: to print sizes in human readable format

### Example

To check the free disk space, run the following command:

# **df -k**

| Filesystem        | kbytes   | used    | avail    | capacity | Mounted on   |
|-------------------|----------|---------|----------|----------|--------------|
| /dev/dsk/c0t0d0s0 | 2053605  | 997684  | 994313   | 51%      | /            |
| /proc             | 0        | 0       | 0        | 0%       | /proc        |
| fd                | 0        | 0       | 0        | 0%       | /dev/fd      |
| /dev/dsk/c0t1d0s7 | 35009161 | 2562019 | 32097051 | 8%       | /export/home |
| swap              | 3431792  | 6664    | 3425128  | 1%       | /tmp         |



| Filesystem | 1K-blocks | Used     | Available | Use% | Mounted on |
|------------|-----------|----------|-----------|------|------------|
| /dev/sda4  | 81242124  | 31102496 | 50139628  | 39%  | /          |
| udev       | 3044112   | 704      | 3043408   | 1%   | /dev       |
| /dev/sda1  | 136384    | 8420     | 127964    | 7%   | /boot/efi  |
| /dev/sda3  | 52434552  | 53964    | 52380588  | 1%   | /home      |

The command result contains the following information:

- File system name
- File size (unit: KB)
- Used space
- Free space
- Capacity percentage of the filled file system and the mounting point

When you run the **df** command without any parameters, the free disk space in each mounted device is displayed.

When the free disk space is reduced to the bottom line, the system administrator must take immediate measures to locate the faulty file system.

## D.5.3 du Command

This topic describes the **du** command used for viewing the disk space used by a specific folder or file.

### Function

The **du** command is used to view the disk space used by a specific folder or file.

### Command Format

**du** *option folder or file*

### Option Description

- **-a** : to view the disk space used by each file
- **-s**: to view the used total disk space
- **-k**: to view the result (unit: KB)
- **-h**: print sizes in human readable format

### Example

- To view the disk space used by the files in the **/etc** folder, run the following command:

```
du -k /etc |more
4 /etc/X11/fs
4 /etc/X11/twm
84 /etc/X11/xdm/pixmaps
157 /etc/X11/xdm
721 /etc/X11/xkb/rules
52 /etc/X11/xkb/types
16 /etc/X11/xkb/semantics
8 /etc/X11/xkb/geometry/ibm_vndr
44 /etc/X11/xkb/geometry/digital_vndr
44 /etc/X11/xkb/geometry/sgi_vndr
285 /etc/X11/xkb/geometry
81 /etc/X11/xkb/compat
```

```

28 /etc/X11/xkb/symbols/sun_vndr
16 /etc/X11/xkb/symbols/fujitsu_vndr
84 /etc/X11/xkb/symbols/macintosh_vndr
8 /etc/X11/xkb/symbols/nec_vndr
32 /etc/X11/xkb/symbols/digital_vndr
4 /etc/X11/xkb/symbols/sony_vndr
12 /etc/X11/xkb/symbols/xfree68_vndr
4 /etc/X11/xkb/symbols/hp_vndr
4 /etc/X11/xkb/symbols/sgi_vndr
850 /etc/X11/xkb/symbols
40 /etc/X11/xkb/keymap/sun_vndr
8 /etc/X11/xkb/keymap/digital_vndr
93 /etc/X11/xkb/keymap/sgi_vndr
181 /etc/X11/xkb/keymap
16 /etc/X11/xkb/keycodes/digital_vndr
12 /etc/X11/xkb/keycodes/sgi_vndr
108 /etc/X11/xkb/keycodes
2345 /etc/X11/xkb
4 /etc/X11/xsm
4 /etc/X11/lbxproxy
16 /etc/X11/fvwm2
4 /etc/X11/xserver/C/print/ddx-config/raster
4 /etc/X11/xserver/C/print/ddx-config
12 /etc/X11/xserver/C/print/attributes
245 /etc/X11/xserver/C/print/models/PSdefault/fonts
--More-

```

- To view the disk space used by all file systems in the current folder and send the results to the sort command for sorting, run the following command:

```
du -s * |sort -rn|more
```

```

28672 opt
3757 X11
2522 cups
1282 boot splash
822 xscreensaver
808 sysconfig
661 services
661 init.d
473 postfix
428 apparmor
416 mono
389 joe
193 profile.d
165 ssl
165 apparmor.d
164 ssh
145 pam.d
145 lvm
112 fonts
109 xinetd.d
--More-

```

- To list the first ten file systems according to the file size, run the following command:

```
du -s * |sort -rn|head -10
```

```

28672 opt
3757 X11
2522 cups
1282 boot splash
822 xscreensaver
808 sysconfig
661 services
661 init.d
473 postfix
428 apparmor

```

## D.5.4 ps Command

This topic describes the `ps` command used for viewing the status of the processes currently running in the system.

### Function

The `ps` command is used to view the status of the processes currently running in the system..

### Command Format

`ps option`

### Option Description

- `-e` : to view the status of all the processes that are running in the system
- `-l` : to view the running processes in a long-form list
- `-u user` : to view the process status of a specific user
- `-f` : to view all the status information about the processes that are running in the system

### Example

- To view the status of all the running processes controlled by the login device (the terminal), run the following command:

```
ps
 PID TTY TIME CMD
 13726 pts/5 0:00 ksh
```

- To view the complete information about the active processes, run the following command:

```
ps -f
 UID PID PPID C STIME TTY TIME CMD
sybase 13726 13724 0 08:44:35 pts/5 0:00 -ksh
```

- To view the U2000 processes, run the following command:

```
ps -ef|grep imap
 root 22344 1 0 17:49:43 ? 0:03 imapsvcd -name devdoc_agent
-
sysagent DEFAULTSYSAGENT -port 31105 -agentid 0
 root 22374 1 0 17:49:48 ? 0:02 imapsvcd -name am_agent -
sysa
gent DEFAULTSYSAGENT -port 31131 -agentid 0
 root 22346 1 0 17:49:43 ? 0:01 imapsvcd -name em_agent -
sysa
gent DEFAULTSYSAGENT -port 31002 -agentid 0
 root 22342 1 0 17:49:43 ? 0:11 imapsvcd -name cmdc_agent -
sy
sagent DEFAULTSYSAGENT -port 31103 -agentid 0
 root 22355 1 0 17:49:45 ? 0:11 imapsvcd -name ifms_agent -
sy
sagent DEFAULTSYSAGENT -port 31011 -agentid 119
 root 22338 1 0 17:49:42 ? 0:02 imapsvcd -name 3gpp_agent -
sy
.....
```

 **NOTE**

- After you run the **ps** command without any parameters, the screen displays information about all running processes that are controlled by the login device (terminal).
- After you specify the **-f** parameter, more information is displayed. The information includes the user name (UID), process ID (PID), parent process ID (PPID), technical number that indicates the running time of the process (C), process start time (STIME), name of the terminal that activates the process (TTY), and the process name (CMD). If TTY displays ?, infer that this process is not associated with the terminal.
- To view all the processes related to specific characters, for example, the process related to the U2000, run the **grep** command with the **ps** command.

## D.5.5 kill Command

This topic describes the **kill** command used for terminating one or more processes.

### Function

The **kill** command is used to terminate a process.

### Command Format

**kill option processID**

### Option Description

- **-l** : lists the names of all the signals
- **-s signal**: sends a signal named signal to the processes

### Parameter Description

*processID*: the ID of the process to be terminated, that is, the process ID

### Example

- To list all the signal names, run the following command:  

```
kill -l
1) SIGHUP 2) SIGINT 3) SIGQUIT 4) SIGILL
5) SIGTRAP 6) SIGABRT 7) SIGEMT 8) SIGFPE
9) SIGKILL 10) SIGBUS 11) SIGSEGV 12) SIGSYS
13) SIGPIPE 14) SIGALRM 15) SIGTERM 16) SIGUSR1
17) SIGUSR2 18) SIGCHLD 19) SIGPWR 20) SIGWINCH
21) SIGURG 22) SIGIO 23) SIGSTOP 24) SIGTSTP
25) SIGCONT 26) SIGTTIN 27) SIGTTOU 28) SIGVTALRM
```
- To terminate the process with PID as 256, run the following command:  

```
kill -s KILL 256
```

 **NOTE**

- The previous signal names can be expressed by code.  
For example, **-1** for **HUP**, **-2** for **INT**, **-3** for **QUIT**, **-9** for **KILL**, **-15** for **TERM**. The signal **KILL** can be replaced with **-9**.  
This signal is the most frequently used one in the **kill** command, and thus it has the highest priority.  
The default signal **15** is used when no option is specified for the **kill** command. Run the following command to terminate the process with the PID as 256:  

```
kill -9 256
```
- Run the **ps** command to check the execution of the **kill** command by listing the PIDs of the terminated processes.
- The **kill** command may lead to a data loss. Run this command with care.

## D.5.6 who Command

This topic describes the **who** command used for reporting the login information about all the users in the current system.

### Function

The **who** command reports the login information about all the users in the current system.

### Command Format

**who** **Option**

### Option Description

- **-b** : display the system date and time of the last startup
- **-m**: display the related information about the users who run the command (the same as the command **who** with two parameters **am i**)

### Parameter Description

**am i**: display the login information about the users who run the command

### Example

- Display the login information about all the users in the current system:

```
who
root pts/3 Feb 4 10:08 (10.129.16.60)
sybase pts/5 Feb 4 08:45 (10.129.28.44)
root pts/6 Feb 4 11:25 (10.129.16.60)
```

- Display the login information about the users who run the command:

```
who am i
sybase pts/5 Feb 4 08:45 (10.129.28.44)

or:

who -m
sybase pts/5 Feb 4 08:45 (10.129.28.44)
```

## D.5.7 which Command

This topic describes the `which` command used for viewing the location where a command is run.

### Function

The `which` command is used to view the location where a command is run. The result may be an absolute path or alias of the command found in the user environment variant `PATH`.

### Command Format

**which** *command*

### Example

To view the position where the commands `pwd`, `who`, and `which` are run, run the following command:

```
which pwd who which
```

```
/usr/bin/pwd
/usr/bin/who
/usr/bin/which
```

#### NOTE

If the command to be located does not exist in the file, the following error messages are displayed after you run the `which` command:

```
which qqqq
no qqqq in /usr/bin /usr/ucb /etc
```

## D.5.8 hostname Command

This topic describes the `hostname` command used for viewing or setting the host name.

### Function

The `hostname` command is used to view or set the host name.

### Command Format

**hostname** *host name*

### Example

To view the host name, run the following command:

```
hostname
```

#### NOTE

If you run the `hostname` command without parameters, the host name of the equipment is displayed. If you run the `hostname` command with parameters, the host name is set. Only the super user can run the `hostname` command.

## D.5.9 uname Command

This topic describes the `uname` command used for viewing the information about the operating system.

### Function

The `uname` command is used to view the information about the operating system. If you run this command without parameters, only the name of the operating system is displayed. If you run this command with parameters, more details about the operating system are displayed.

### Format

`uname option`

### Option Description

The options of the `uname` command can be combined. Add the prefix `-` before the options. [Table D-17](#) lists some frequently used options.

**Table D-17** Description of the `uname` options

| Option                       | Description                                                                                               |
|------------------------------|-----------------------------------------------------------------------------------------------------------|
| <b>-a</b>                    | Views all the information.                                                                                |
| <b>-i</b>                    | Views hardware information.                                                                               |
| <b>-m</b>                    | Views the name of the equipment hardware. It is recommended that <b>-p</b> be used instead of <b>-m</b> . |
| <b>-n</b>                    | Views the name of the network equipment.                                                                  |
| <b>-p</b>                    | Views the ISA of the host or the type of the processor.                                                   |
| <b>-r</b>                    | Views the serial number of the operating system of the host.                                              |
| <b>-s</b>                    | Views the name of the operating system of the host (it is the default option).                            |
| <b>-v</b>                    | Views the version of the operating system of the host.                                                    |
| <b>-S</b> <i>system_name</i> | Sets the host name of the machine. <b>system_name</b> stands for the host name set by the user.           |

### Example

To view the name, version, and serial number of the operating system on the host, run the following command:

```
uname -svr
```

## D.5.10 ifconfig Command

This topic describes the ifconfig command used for viewing the IP address of the host.

### Function

The ifconfig command is used to view the IP address of the host.

### Command Format

**ifconfig option**

### Option Description

**-a:** to view all the address information

### Example

To view the IP address of the host, run the following command:

```
ifconfig -a
```

```
lo0: flags=849<UP,LOOPBACK,RUNNING,MULTICAST> mtu 8232 inet 127.0.0.1 netmask
 ff000000
hme0: flags=863<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST>mtu 1500 inet
 129.9.169.143 netmask ffff0000 broadcast 129.9.255.255
hme0:1: flags=863<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST> mtu 1500 inet
 129.6.253.136 netmask ffff0000 broadcast 129.6.255.255
```

#### NOTE

In the previous output, the IP address of the displayed host is 129.9.169.143, and the logical IP address is 129.6.253.136. In the Solaris or SUSE Linux system, a network adapter can bind several logical IP addresses, which realizes communications between different network segments.

## D.5.11 script Command

This topic describes the script command used for recording in a script file all the screen input and output that occur from the time when the script command is run to the time when the exit command is entered.

### Function



#### CAUTION

Close the script file before running the **exit** command to terminate the recording of the screen I/O. If you do not close the script file, the script file builds up and hinders the normal operation of the system.

---

Record in a script file all the screen input and output that occur from the time when the script command is run to the time when the exit command is entered. The script command is helpful for programming and debugging.



## Format

**script** *option file*

## Option Description

**-a**: appends the screen I/O content to a file. If you do not set this parameter, the screen I/O overwrites the content of the file.

## Parameter Description

*file*: the file used to save the screen I/O content. If you do not specify the file name, the screen I/O content is saved to the **typescript** file.

## Example

To save the screen I/O content in the default destination file **typescript**, run the following commands:

```
script

Script started, file is typescript

ps

 PID TTY TIME CMD
 775 pts/8 0:00 ksh

pwd

/export/home

date

Mon Feb 4 19:12:14 GMT 2002

exit

Script done, file is typescript
```

To view the content of the **typescript** file, run the following command:

```
cat typescript

Script started on Mon Feb 04 19:11:49 2002
$ ps
 PID TTY TIME CMD
 775 pts/8 0:00 ksh
$ pwd
/export/home
$ date
Mon Feb 4 19:12:14 GMT 2002
$ exit
exit
script done on Mon Feb 04 19:12:24 2002
```

## D.5.12 date Command

This topic describes the **date** command used for viewing the current date and time of the system.

## Function

The data command is used to view the current date and time of the system. The super user can run the date command to set the system date and time.

## Format

**date option +format**

## Option Description

- **-u**: to use the Greenwich mean time.
- **+format**: to specify the command output format.

**Table D-18** describes the format of the command output.

**Table D-18** Format of the command output

| Format    | Description                                         |
|-----------|-----------------------------------------------------|
| <b>%h</b> | Abbreviation of the month: from January to December |
| <b>%j</b> | A day in a year: from 001 to 366                    |
| <b>%n</b> | Switch to next line                                 |
| <b>%t</b> | The tab key                                         |
| <b>%y</b> | The last two digits of the year: from 00 to 99      |
| <b>%D</b> | Output format of the date: month/date/year          |
| <b>%H</b> | Hour: from 00 to 23                                 |
| <b>%M</b> | Minute: from 00 to 59                               |
| <b>%S</b> | Second: from 00 to 59                               |
| <b>%T</b> | Output format of time: hour:minute:second           |

## Example

- To view the current date and time of the system, run the following command:  
**date**  
Mon Feb 4 20:26:16 GMT 2002
- To view the current system date and time in the Greenwich Mean Time, run the following command:  
**date -u**  
Mon Feb 4 12:27:26 GMT 2002
- To view the current date of the system in the format of month/day/year, run the following command:  
**date +%D**  
02/04/02

## D.5.13 bc Command

This topic describes the `bc` command used for simple calculation.

### Function

The `bc` command is used to perform a simple calculation.

### Example

To multiply 4 by 5, run the following command:

```
bc
```

```
4*5
```

```
20
```

 **NOTE**

To get the result, run the `bc` command, and then press **Enter**. Type the formula `4*5`, and then press **Enter**. The result is displayed on the screen. Press **Ctrl+D** to exit from the `bc` program.

## D.5.14 prtconf Command

This topic describes the `prtconf` command used for checking the system configuration.

### Function

The `prtconf` command is used to check the system configuration.

### Format

**prtconf** *option device path*

### Instance

- Check all the configuration information about the system.

```
prtconf
```

```
System Configuration: Sun Microsystems sun4u
Memory size: 4096 Megabytes
System Peripherals (Software Nodes):
```

```
SUNW,Netra-240
 scsi_vhci, instance #0
 packages (driver not attached)
 SUNW,builtin-drivers (driver not attached)
 deblocker (driver not attached)
 disk-label (driver not attached)
 terminal-emulator (driver not attached)
 dropins (driver not attached)
 kbd-translator (driver not attached)
 obp-tftp (driver not attached)
 SUNW,i2c-ram-device (driver not attached)
 SUNW,fru-device (driver not attached)
 SUNW,asr (driver not attached)
 ufs-file-system (driver not attached)
 chosen (driver not attached)
 openprom (driver not attached)
 client-services (driver not attached)
```

```

options, instance #0
aliases (driver not attached)
memory (driver not attached)
virtual-memory (driver not attached)
SUNW,UltraSPARC-IIIf, instance #0 (driver not attached)
memory-controller, instance #0
SUNW,UltraSPARC-IIIf, instance #1 (driver not attached)
memory-controller, instance #1
pci, instance #0
 network, instance #0
 network, instance #1
pci, instance #1
 isa, instance #0
 flashprom (driver not attached)
 rtc (driver not attached)
 i2c, instance #0
 i2c-bridge (driver not attached)
 i2c-bridge (driver not attached)
 motherboard-fru-prom, instance #0 (driver not attached)
 chassis-fru-prom, instance #1 (driver not attached)
 alarm-fru-prom, instance #2 (driver not attached)
 power-supply-fru-prom, instance #3 (driver not attached)
 power-supply-fru-prom, instance #4 (driver not attached)
 dimm-spd, instance #5 (driver not attached)
 dimm-spd, instance #6 (driver not attached)
 dimm-spd, instance #7 (driver not attached)
 dimm-spd, instance #8 (driver not attached)
 rsrcrtc (driver not attached)
 nvram, instance #9 (driver not attached)
 idprom (driver not attached)
 gpio, instance #0 (driver not attached)
 gpio, instance #1 (driver not attached)
 gpio, instance #2 (driver not attached)
 gpio, instance #3 (driver not attached)
 gpio, instance #4 (driver not attached)
 gpio, instance #5 (driver not attached)
 power, instance #0
 serial, instance #0
 serial, instance #1 (driver not attached)
 rmc-comm, instance #0
 pmu, instance #0
 i2c, instance #0
 gpio, instance #0
 usb, instance #0
 ide, instance #0
 disk (driver not attached)
 cdrom (driver not attached)
 sd, instance #3
pci, instance #2
 scsi, instance #0
 disk (driver not attached)
 tape (driver not attached)
 sd, instance #0
 sd, instance #1 (driver not attached)
 sd, instance #2 (driver not attached)
 sd, instance #4 (driver not attached)
 sd, instance #5 (driver not attached)
 sd, instance #6 (driver not attached)
 sd, instance #7 (driver not attached)
 sd, instance #8 (driver not attached)
 sd, instance #9 (driver not attached)
 sd, instance #10 (driver not attached)
 sd, instance #11 (driver not attached)
 sd, instance #12 (driver not attached)
 sd, instance #13 (driver not attached)
 sd, instance #14 (driver not attached)
 sd, instance #15 (driver not attached)
 st, instance #1 (driver not attached)
 st, instance #2 (driver not attached)

```

```
st, instance #3 (driver not attached)
st, instance #4 (driver not attached)
st, instance #5 (driver not attached)
st, instance #6 (driver not attached)
ses, instance #1 (driver not attached)
ses, instance #2 (driver not attached)
ses, instance #3 (driver not attached)
ses, instance #4 (driver not attached)
ses, instance #5 (driver not attached)
ses, instance #6 (driver not attached)
ses, instance #7 (driver not attached)
ses, instance #8 (driver not attached)
ses, instance #9 (driver not attached)
ses, instance #10 (driver not attached)
ses, instance #11 (driver not attached)
ses, instance #12 (driver not attached)
ses, instance #13 (driver not attached)
ses, instance #14 (driver not attached)
ses, instance #15 (driver not attached)
scsi, instance #1
disk (driver not attached)
tape (driver not attached)
sd, instance #16 (driver not attached)
sd, instance #17 (driver not attached)
sd, instance #18 (driver not attached)
sd, instance #19 (driver not attached)
sd, instance #20 (driver not attached)
sd, instance #21 (driver not attached)
sd, instance #22 (driver not attached)
sd, instance #23 (driver not attached)
sd, instance #24 (driver not attached)
sd, instance #25 (driver not attached)
sd, instance #26 (driver not attached)
sd, instance #27 (driver not attached)
sd, instance #28 (driver not attached)
sd, instance #29 (driver not attached)
sd, instance #30 (driver not attached)
st, instance #8 (driver not attached)
st, instance #9 (driver not attached)
st, instance #10 (driver not attached)
st, instance #11 (driver not attached)
st, instance #12 (driver not attached)
st, instance #13 (driver not attached)
ses, instance #16 (driver not attached)
ses, instance #17 (driver not attached)
ses, instance #18 (driver not attached)
ses, instance #19 (driver not attached)
ses, instance #20 (driver not attached)
ses, instance #21 (driver not attached)
ses, instance #22 (driver not attached)
ses, instance #23 (driver not attached)
ses, instance #24 (driver not attached)
ses, instance #25 (driver not attached)
ses, instance #26 (driver not attached)
ses, instance #27 (driver not attached)
ses, instance #28 (driver not attached)
ses, instance #29 (driver not attached)
ses, instance #30 (driver not attached)
ses, instance #31 (driver not attached)
pci, instance #3
network, instance #2
network, instance #3
iscsi, instance #0
pseudo, instance #0
```

## D.5.15 prstat Command

This topic describes the prstat command used for viewing the CPU usage.

## Function

The CPU usage may be high when a large number of NE alarms are reported in a short period or when the performance data is high. This command is used to find out the cause of these alarms.

## Permitted Users

User root and other common users are authorized to run the **prstat** command.

## Example

```
prstat
```

The command result contains the CPU usage of each process.

# D.6 Commands for Network Communications in the Solaris or Linux System

This section describes the commands for network communication in the Solaris or Linux system. It also describes the functions of these commands and gives some examples.

### [D.6.1 ping Command](#)

This topic describes the ping command used for checking the connection of networks.

### [D.6.2 telnet Command](#)

This topic describes the telnet command used for logging in to the remote Solaris or Linux host from the local computer.

### [D.6.3 ftp Command](#)

This topic describes the ftp command used for transferring files between the local computer and the remote host.

### [D.6.4 finger Command](#)

This topic describes the finger command used for viewing the information about the online users who are using the Solaris or Linux system.

### [D.6.5 netstat Command](#)

This topic describes the netstat command used for displaying the current network status.

### [D.6.6 route Command](#)

This topic describes the route command used for changing the maintenance routing table.

## D.6.1 ping Command

This topic describes the ping command used for checking the connection of networks.

## Function

The ping command is used to check the physical connection of the network when the communication between a user computer and the hosts in the network is interrupted.

## Format

**ping** *IP address of a host*

## Example

Check the physical connection between the current host and the host whose IP address is 129.9.0.1.

```
ping 129.9.0.1
```

```
129.9.0.1 is alive
64 bytes from 129.9.0.1: icmp_seq=1 ttl=64 time=0.038 ms
64 bytes from 129.9.0.1: icmp_seq=2 ttl=64 time=0.021 ms
```

The Internet Control Message Protocol (ICMP) is used through the **ping** command to check the network connection. An ICMP echo request message is sent to a specific host to request an ICMP echo response message. If the response message is not received within a specified time, the `Host unreachable` message is displayed on the screen.

The `Host unreachable` message is displayed in the following cases:

- The specified host is invalid.
- The network cables are not correctly connected.
- The two communicating hosts do not support the same communication protocol.

To analyze the causes, run the **ping** command to connect to other hosts in the same network segment. If the **ping** command is successful, you can infer that the connection is functional. In this case, check the physical connection and the operational status of the specified host. If the **ping** command fails, check whether the physical network connection of the current host is secure or whether the TCP/IP protocol is set correctly only for Windows 95 users.

## D.6.2 telnet Command

This topic describes the telnet command used for logging in to the remote Solaris or Linux host from the local computer.

### Function

#### NOTE

Before running the **telnet** command, ensure that a local computer is connected to the remote Solaris or Linux host according to the TCP/IP protocol.

Telnet is the software used to log in to remote Solaris or Linux hosts through network connection. Telnet takes the local computer as a simulated terminal of the remote Solaris or Linux host and enables you to log in to the remote server from the local computer. After you log in to the remote Solaris or Linux host successfully through telnet, you become a remote simulated terminal user and you can use the local computer as a real Solaris or Linux terminal. In this case, the resources and functions available and the operating mode depend on the settings of the remote host and the access privileges of the login account.

### Command Format

```
telnet IP address or domain name port
```

### Parameter Description

- *IP address*: the IP address of a remote Solaris or Linux host
- *Domain*: the domain name of a remote Solaris or Linux host

- *port*: the port number of the listening port of the telnet service. If the port number is omitted, it indicates that the port with the number of 23 is connected to the telnet service by default.

## Example

Run the **telnet** command on a local computer and log in to a remote Solaris or Linux host. Assume that the IP address of the Solaris or Linux host is 129.9.169.143.

1. On the local computer, choose **Start > Run**.
2. Enter **telnet 129.9.169.143** and click **OK**.

### NOTE

The **telnet** command can also be used to test the listening status of a port of a host. For example, test whether port 22 of the host with the IP address of 129.9.169.143 is in listening status by running the following command:

**telnet 129.9.169.143 22**

You can determine whether the port is in listening status according to the displayed message.

3. The Telnet dialog box appears and prompts you to enter the Solaris or Linux user name and password.

login: **root**

Password: **root password**

### NOTE

Enter the password on the right of **Password**. The entered password is not displayed.

The subsequent steps are the same as those when you operate on the Solaris or Linux host.

## D.6.3 ftp Command

This topic describes the ftp command used for transferring files between the local computer and the remote host.

### Function

The ftp command is used to transfer files between the local computer and the remote host. You can transfer one or multiple files at a time between the remote Solaris or Linux system and the local computer.

### Format

**ftp** *IP address or domain*

### Parameter Description

- *IP address*: the IP address of the remote Solaris or Linux host
- *Domain name*: the domain name of the remote Solaris or Linux host

## Example

Run the **ftp** command on the local computer. Assume that the IP address of the remote Solaris or Linux host is 129.9.169.143.



Choose **Start > Run** on the local computer. In the displayed dialog box, enter **ftp 129.9.169.143** and click **OK**. When the ftp window is displayed, enter the Solaris or Linux user name and password.

User (129.9.169.143: (none) : ) **ftpuser**

Password: *password of ftpuser*  
230 Login successful.  
ftp>

 **NOTE**

Enter the password after Password: . The password is not displayed.

Enter the ftp command behind the prompt ftp>. [Table D-19](#) describes the ftp commands that are commonly used.

**Table D-19** Common ftp commands

| ftp Command                            | Description                                                                                                         |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| <b>!command</b>                        | Use a local command and return to ftp immediately.                                                                  |
| <b>? help command</b>                  | View the command help.                                                                                              |
| <b>ascii</b>                           | Transfer files in ASCII format (default).                                                                           |
| <b>binary</b>                          | Transfer files in binary format.                                                                                    |
| <b>cd folder</b>                       | Switch to the specified remote destination directory (the directory on the computer that provides the FTP service). |
| <b>close</b>                           | Break the remote connection.                                                                                        |
| <b>dir remote-directory local-file</b> | View the remote directory. If there is a local file, save the result to the local file.                             |
| <b>get file1 file2</b>                 | Copy the remote file1 to the local file2.                                                                           |
| <b>lcd folder</b>                      | Switch to the specified local destination directory (the directory on the computer that provides the FTP service).  |
| <b>ls r-folder l-file</b>              | Same as <b>dir</b> , but the display format is different.                                                           |
| <b>mget several files</b>              | Copy several remote files to the local computer.                                                                    |
| <b>open IP address or domain</b>       | Reestablish a connection.                                                                                           |
| <b>put file1 file2</b>                 | Copy the remote file1 to the local file2.                                                                           |
| <b>pwd</b>                             | List the folders of the current remote host.                                                                        |
| <b>quit bye</b>                        | Exit from the ftp.                                                                                                  |
| <b>status</b>                          | View the current ftp status.                                                                                        |

- Copy all the files in the path **C:\mydoc** on the local computer to the **/usr/local/tmp** folder on the remote host.  

```
ftp> binary
ftp> lcd c:\mydoc
ftp> cd /usr/local/tmp
ftp> mput *.*
```
- Copy the **.login** file in the **/usr/home/rms** folder on the remote host to the path **C:\mydoc** folder on the local computer.  

```
ftp> ascii
ftp> lcd c:\temp\from
ftp> cd /usr/home/rms
ftp> get .login
```
- Copy all files in the **/usr/home/rms** folder on the remote computer to the path **C:\temp\from** on the local computer in binary format.  

```
ftp> binary
ftp> lcd c:\temp\from
ftp> cd /usr/home/rms
ftp> mget *
```
- To exit ftp.  

```
ftp> quit
```



## CAUTION

The Telnet and FTP protocols belong to the TCP/IP family. They are the protocols at the application layer. They work in client/server mode. The telnet/ftp program running on the local computer is a telnet/ftp client program. The telnet/ftp program connects to the server program in the remote host through the TCP/IP protocol. Any system installed with the telnet/ftp server-side software can serve as a remote host. In addition to the default network protocol TCP/IP, the Solaris or Linux system supports the Telnet/FTP protocols. Because a Solaris or Linux host is installed with both the telnet/ftp server software and the client software, the Solaris or Linux host can serve as either a telnet/ftp server or a telnet/ftp client.

---

## D.6.4 finger Command

This topic describes the finger command used for viewing the information about the online users who are using the Solaris or Linux system.

### Function

The finger command is used to view the information about online users of the Solaris or Linux system.

## Command Format

**finger** *user name@host domain|IP address*

## Parameter Description

- *user name*: the user that has currently logged in to the local system.
- *host domain*: the Solaris or Linux host domain.
- *IP address*: the IP address of the Solaris or Linux host.

## Example

**Table D-20** lists some common examples of the finger command.

**Table D-20** Examples of the finger command

| Example                                | Description                                                             |
|----------------------------------------|-------------------------------------------------------------------------|
| # <b>finger</b>                        | View the information about all local users.                             |
| # <b>finger root</b>                   | View the information about user root.                                   |
| # <b>finger @omcsyb2</b>               | View the information about all users in the host omcsyb2.               |
| # <b>finger @omcsyb2.huawei.com.cn</b> | View the information about all users in the host omcsyb2.huawei.com.cn. |
| # <b>finger abc@omcsyb2</b>            | View the information about user abc in the host omcsyb2.                |
| # <b>finger abc@10.10.10.1</b>         | View the information about user abc in the host 10.10.10.1.             |

## D.6.5 netstat Command

This topic describes the netstat command used for displaying the current network status.

### Function

The **netstat** command is used to display the current network status. The **netstat** command is powerful but complex in format. This describes common applications of the **netstat** command.

## Command Format

**netstat** *options*

## Option Description

- For viewing all the sockets and routing tables (**netstat -anv**)
  - **-a**: views all socket information.

- **-n**: views the information by number. If you do not specify this parameter, the information is displayed by logical name.
- **-v**: views the information about sockets and routing tables of the additional information.
- For viewing the IP address of the network adapter (**netstat -i -I interface interval**)
  - **-i**: views the information about the network interface.
  - **-I interface**: specifies an interface, for example, **hme0:1**
  - **interval**: indicates a time interval.
- For viewing the routing table status (**netstat -r -anv**)
  - **-r**: views the information about the routing table.
  - **-anv**: refers to [For viewing all the sockets and routing tables](#).
- For viewing the broadcast information (**netstat -M -ns**)
  - **-M**: views broadcast routing tables.
  - **-n**: views the information by number. If you do not specify this parameter, the information is displayed by logical name.
  - **-s**: summarizes the status of each protocol.
- For viewing the DHCP status (**netstat -D -I interface**)
  - **-D**: views the DHCP information.

## Example

Use the command **netstat -rn** to view the information about the routing tables:

# **netstat -rn**

Routing Table:

| Destination | Gateway       | Flags | Ref | Use | Interface |
|-------------|---------------|-------|-----|-----|-----------|
| 10.105.28.0 | 10.105.28.202 | U     | 4   | 2   | hme0      |
| 10.0.0.0    | 10.105.31.254 | UG    | 0   | 0   |           |
| 224.0.0.0   | 10.105.28.202 | U     | 4   | 0   | hme0      |
| 127.0.0.1   | 127.0.0.1     | UH    | 0   | 896 | lo0       |

Kernel IP routing table

| Destination | Gateway     | Genmask         | Flags | MSS | Window | irrt | Iface |
|-------------|-------------|-----------------|-------|-----|--------|------|-------|
| 10.71.158.0 | 0.0.0.0     | 255.255.255.128 | U     | 0   | 0      | 0    | eth2  |
| 169.254.0.0 | 0.0.0.0     | 255.255.0.0     | U     | 0   | 0      | 0    | eth2  |
| 127.0.0.0   | 0.0.0.0     | 255.0.0.0       | U     | 0   | 0      | 0    | lo    |
| 0.0.0.0     | 10.71.158.1 | 0.0.0.0         | UG    | 0   | 0      | 0    | eth2  |

A router can be in any of the following five different flags: U, G, H, D, and M, as described in [Table D-21](#).

**Table D-21** Description of routing flags

| Flag | Description                                      |
|------|--------------------------------------------------|
| U    | U indicates that a route is currently available. |

| Flag | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| G    | G indicates that a route is destined for a gateway such as a router.<br><br>If this flag is not set, you can infer that the destination is connected directly. Flag G distinguishes between direct and indirect routes. Flag G is unnecessary for direct routes. The difference is that the packet sent through a direct route carries both the destination IP address and the link-layer address. In the packet sent through an indirect route, however, the IP address points to the destination and the link layer address points to the gateway (for example, the next router).                                                                        |
| H    | H indicates a route destined for a host. That is, the destination address is a complete host address.<br><br><b>NOTE</b> <ul style="list-style-type: none"><li>● If this flag is not set, you can infer that the route leads to a network and that the destination address is a network address: either a network number or a network. The part in the address for the host is 0.</li><li>● When you search the routing table for an IP address, the host address must exactly match the destination address.</li><li>● The network address, however, is required to match only the network number and subnet number of the destination address.</li></ul> |
| D    | D indicates that a route is created by a redirected packet.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| M    | M indicates that a route is modified by a redirected packet.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

The `Ref` (Reference count) column lists the number of routing progresses. The protocol for connection, such as TCP, requires a fixed route when a connection is established. If the telnet connection is established between the host `svr4` and the host `slip`, the `Ref` is 1. If another telnet connection is established, its value is changed to 2.

The next column (`Use`) displays the number of packets sent through a specified route. After you run the `ping` command as the unique user of this route, the program sends five groups and the number of packets is displayed as 5. The last column (`Interface`) indicates the name of the local interface.

The name of the loop-back interface is permanent set to `lo0`. Flag G is not set because the route is not destined for a gateway. Flag H indicates that the destination address, `127.0.0.1`, is a host address and not a network address. Because flag G is not set, the route here is a direct route and the gateway column shows the outgoing IP address.

Each host has one or multiple default routes. That is, if a particular route is not found in the table, the packet is sent to the router. In addition, the current host can access other systems through the Sun router (and the `slip` link) on the internet, based on the settings of the routing table. The flag UG refers to the gateway.

## D.6.6 route Command

This topic describes the `route` command used for changing the maintenance routing table.

### Function

The routing table relays IP address between network segments. The `route` command is used to modify and maintain the routing table.

## Format

**route -f** *command modifiers args*

**route -f** *add|change|delete|get -host|net destination gateway args*

**route -n** *monitor*

**route -n** *flush*

**route** *add|del -host | -net destination gw gateway args*

### NOTE

The meaning of "|" is the same as that of the word "or".

## Parameter Description

Options of the route command can be combined. [Table D-22](#) lists some common options.

**Table D-22** Description of the route commands

| Option       | Description                                                                                                                                                                                                                         |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -f           | Refresh routing tables for all gateways.                                                                                                                                                                                            |
| -n           | View the information in characters instead of symbols.                                                                                                                                                                              |
| -v           | View the additional information.                                                                                                                                                                                                    |
| -q           | Suspend all outputs.                                                                                                                                                                                                                |
| -commond     | Refer to the <b>add</b> , <b>change</b> , <b>flush</b> (clear the gateways in the routing table), <b>get</b> or <b>monitor</b> .<br><b>add del</b>                                                                                  |
| -net         | Set a route to a network segment.                                                                                                                                                                                                   |
| -host        | Set a route to a host.                                                                                                                                                                                                              |
| -destination | Destination network segment. For example, <i>10.0.0.0</i> stands for section 10, and <i>10.11.0.0</i> stands for section 10.11.<br>destination network segment ( <i>10.1.1.0/24</i> , <b>number of network/subnet mask digits</b> ) |
| -gateway     | Indicate the IP address of the gateway.                                                                                                                                                                                             |

## Example

- Obtain the routing information about network segment 10.

```
route -n get 10.0.0.0
 route to: 10.0.0.0
destination: 10.0.0.0
 mask: 255.0.0.0
 gateway: 10.105.31.254
 interface: hme0
 flags: <UP,GATEWAY,DONE,STATIC>
```

```
recvpipe sendpipe ssthresh rtt, msec rttvar hopcount mtu expire
0 0 0 0 0 0 0 1500
0
```

- Clear the gateways in the routing table.

```
route -n flush
```

```
10 10.105.31.254 done
```

```
netstat -rn
```

```
Routing Table:
Destination Gateway Flags Ref Use Interface

10.105.28.0 10.105.28.202 U 4 6 hme0
224.0.0.0 10.105.28.202 U 4 0 hme0
127.0.0.1 127.0.0.1 UH 0 1500 lo0
```

```
telnet 10.129.3.4
```

```
Trying 10.129.3.4...
```

```
telnet: Unable to connect to remote host: Network is unreachable
```

After the gateways in the routing table are cleared, the network segments beyond 10.105.28.202/34 are no longer accessible.

- Add a routing record.

Add the route to the network segment 129.9.0.0/16 with the gateway as 10.105.28.202.

```
route add 129.9.0.0/16 10.105.28.202
```

```
add net 129.9.0.0: gateway 10.105.28.202
```

```
netstat -rn
```

```
Routing Table:
Destination Gateway Flags Ref Use Interface

10.105.28.0 10.105.28.202 U 4 2 hme0
129.9.0.0 10.105.28.202 UG 0 0
10.0.0.0 10.105.31.254 UG 0 0
224.0.0.0 10.105.28.202 U 4 0 hme0
127.0.0.1 127.0.0.1 UH 0 313 lo0
```

#### NOTE

129.9.0.0 10.105.28.202 UG 0 0 is the newly-added routing record.

```
route add -net 129.9.0.0/16 gw 10.105.28.202
```

```
route
```

```
Kernel IP routing table
```

```
Destination Gateway Genmask Flags Metric Ref Use Iface
129.9.0.0 10.105.28.202 255.255.0.0 UG 0 0 0
```

#### NOTE

129.9.0.0 10.105.28.202 255.255.0.0 UG 0 0 0 is the added route.

- Modify the routing table.

```
route change 129.9.0.0 1.2.3.4
```

```
change net 129.9.0.0: gateway 1.2.3.4
```

```
netstat -rn
```

```
Routing Table:
Destination Gateway Flags Ref Use Interface

10.105.28.0 10.105.28.202 U 4 2 hme0
129.9.0.0 1.2.3.4 UG 0 0
10.0.0.0 10.105.31.254 UG 0 0
224.0.0.0 10.105.28.202 U 4 0 hme0
127.0.0.1 127.0.0.1 UH 0 445 lo0
```

 **NOTE**

129.9.0.0 1.2.3.4 UG 0 0 is the routing record of the modified gateway.

- Delete a routing record.

Delete the route to the network segment 129.9.0.0/16 with the gateway as 10.105.28.202.

# **route del -net 129.9.0.0/16 gw 10.105.28.202**

# **route delete -net 129.9.0.0/16 10.105.28.202**



# E Reference of Sybase Database Commands

---

This topic describes the common command reference of the Sybase database, including command functions and usage examples.

## [E.1 startserver Command](#)

This topic describes the **startserver** command used for starting the Sybase database.

## [E.2 showserver Command](#)

This topic describes the **showserver** command used to view the running status of the Sybase database.

## [E.3 isql Command](#)

This topic describes the **isql** command used for connecting to the Sybase database.

## [E.4 shutdown Command](#)

This topic describes the **shutdown** command used for shutting down the Sybase database.

## [E.5 sp\\_configure Command](#)

This topic describes the **sp\_configure** command used for viewing and setting the Sybase database parameters.

## E.1 startserver Command

This topic describes the **startserver** command used for starting the Sybase database.

### Function

The **startserver** command is used to start the Sybase database instance or corresponding backup instance.

### Syntax

**startserver -f parameter**

### Parameter Description

**Table E-1** describes the parameters.

**Table E-1** Condition List Description

| Parameter | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| parameter | <p>The parameter is used to specified Sybase database instance or corresponding backup instance.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"><li>Parameters are named in RUN_SYB_server or RUN_SYB_server_back format. SYB_server and SYB_server_back stand for the Sybase database instance and backup instance respectively.</li><li>The Sybase database instance name and backup instance name are specified when the Sybase database is created. You can view the <b>RUN*</b> file in <b>ASE-*/install</b> under the Sybase database installation path.</li></ul> <p>The asterisk (*) stands for a wild card.</p> |

### Examples

Assume that the Sybase database is installed in **/opt/sybase**, the database instance name is SYB\_server, the corresponding backup instance name is SYB\_server\_back.

In the command prompt window, run the following commands to start the Sybase database.

 **NOTE**

The asterisk (\*) is a wild card. Because the Sybase database has different versions, the asterisk (\*) is used to indicate a version. The ampersand (&) indicates the Sybase instance running on the OS daemon.

```
./opt/sybase/SYBASE.sh
```

```
cd /opt/sybase/ASE-*/install
```

```
./startserver -f ./RUN_SYB_server&
```

```
./startserver -f ./RUN_SYB_server_back&
```

A large amount of start information is displayed. See [E.2 showserver Command](#) to check whether the Sybase database is started successfully.

## E.2 showserver Command

This topic describes the **showserver** command used to view the running status of the Sybase database.

### Function

The **showserver** command is used to view the running status of the Sybase database.

### Syntax

```
showserver
```

### Parameter Description

None.

### Examples

Assume that the Sybase database is installed in **/opt/sybase**, the database instance name is SYB\_server, and backup database instance name is SYB\_server\_back.

In the command prompt window, run the following command to view the running status of the Sybase database.

#### NOTE

The asterisk (\*) is a wild card. Because the Sybase database has different versions, the asterisk (\*) is used to stands for a version.

```
cd /opt/sybase/ASE-*/install
```

```
./showserver
```

The information similar to the following is displayed. If **SYB\_server** and **SYB\_server\_back** are displayed, it indicates that both the Sybase database instance and the backup database instance run properly.

| UID                                               | PID | PPID | C | STIME    | TTY | TIME | CMD                           |
|---------------------------------------------------|-----|------|---|----------|-----|------|-------------------------------|
| root                                              | 615 | 613  | 2 | 14:57:49 | ?   | 2:57 | /opt/sybase/ASE-15_0/bin/data |
| server -sSYB_server -d/opt/sybase/data/master.dat |     |      |   |          |     |      |                               |
| root                                              | 739 | 737  | 0 | 14:58:50 | ?   | 0:00 | /opt/sybase/ASE-15_0/bin/back |
| upserver -SSYB_server_back -e/opt/sybase/ASE-15_0 |     |      |   |          |     |      |                               |

If the following information is displayed, it means that no Sybase database is started. See [E.1 startserver Command](#) to start the Sybase database.

| UID | PID | PPID | C | STIME | TTY | TIME | CMD |
|-----|-----|------|---|-------|-----|------|-----|
|-----|-----|------|---|-------|-----|------|-----|

## E.3 isql Command

This topic describes the **isql** command used for connecting to the Sybase database.

## Function

The **isql** command is used to connect to the Sybase database. You can run sql sentences in the **isql** command line or configure the Sybase database.

## Syntax

**isql** option 1 *parameter 1* option 2 *parameter 2*...

## Parameter Description

**Table E-2** describes the parameters.

**Table E-2** Condition List Description

| Option                                | Description                                                                                                      |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------|
| <b>-S</b> <i>sybase_instance_name</i> | <b>-S</b> is followed by the name ( <i>sybase_instance_name</i> ) of the Sybase database instance to connect to. |
| <b>-U</b> <i>sybase_user</i>          | <b>-U</b> is followed by the user name ( <i>sybase_user</i> ) of the Sybase database.                            |
| <b>-P</b> <i>password</i>             | <b>-P</b> is followed by the user ( <i>sybase_user</i> ) password ( <i>password</i> ) of the Sybase database.    |

## Examples

Assume that the Sybase database is installed in **/opt/sybase**, the database instance name is **SYB\_server**, and the password of the **sa** user is **password**.

In the command prompt window, run the following commands to connect to the Sybase database.

### NOTE

For an application developed based on the Sybase database, the environment variable of the Sybase database is usually run automatically when you set the environment variable of the application (such as U2000). In the condition that the environment variable of the application does not conflict with that of the Sybase database, use method one to connect to the Sybase database. Otherwise, use method two to avoid the conflict.

- Method one: Run the environment variable of the Sybase database first.  
# **./opt/sybase/SYBASE.sh**  
# **isql -SSYB\_server -Usa -Ppassword**
- Method two: Run the environment variable of the Sybase database in the path of the **isql** command.

### NOTE

The asterisk (\*) is a wild card. Because the Sybase database has different versions, the asterisk (\*) is used to stands for a version.

```
cd /opt/sybase/OCS-*/bin
./isql -SSYB_server -Usa -Ppassword
```

If connecting to the Sybase database succeeds, the following prompt of the **isql** command line is displayed:

```
1>
```

If connecting to the Sybase database fails, find out the cause according to the prompt.

## E.4 shutdown Command

This topic describes the **shutdown** command used for shutting down the Sybase database.

### Function

The **shutdown** command is used shut down the Sybase database instance or corresponding backup instance after you use the **isql** command to connect to the Sybase database.

### Syntax

**shutdown** *parameter*

### Parameter Description

[Table E-3](#) describes the parameters.

**Table E-3** Condition List Description

| Parameter         | Description                                                                                                      |
|-------------------|------------------------------------------------------------------------------------------------------------------|
| <i>SYB_BACKUP</i> | This parameter is used to shut down the the connected Sybase database instance or corresponding backup instance. |
| None.             | If the parameter is null, it means that the connected Sybase database instance is to be shut down.               |

### Examples

Assume that the Sybase database is installed in **/opt/sybase**, the database instance name is **Sybase\_server**, and the password of the **sa** user is **password**.

1. In the command prompt window, run the following command to connect to the Sybase database. For details about the **isql** command, see [E.3 isql Command](#).

 **NOTE**

The asterisk (\*) is a wild card. Because the Sybase database has different versions, the asterisk (\*) is used to stands for a version.

```
cd /opt/sybase/OCS-*/bin
```

```
./isql -SSYB_server -Usa -Ppassword
```

2. Shut down the backup instance of the Sybase database.

```
1> shutdown SYB_BACKUP
```

2> **go**

If the information similar to the following is displayed, it indicates that the backup instance of the Sybase database is shut down normally. Otherwise, find out the cause to a failure according to the prompt.

Backup Server: 3.48.1.1: The Backup Server will go down immediately.  
Terminating sessions.

3. Shut down the Sybase database instance.

1> **shutdown**

2> **go**

If the information similar to the following is displayed, it indicates that the Sybase database instance is to be shut down normally. Otherwise, find out the cause to a failure according to the prompt.

Server SHUTDOWN by request.  
ASE is terminating this process.

## E.5 sp\_configure Command

This topic describes the **sp\_configure** command used for viewing and setting the Sybase database parameters.

### Function

The **sp\_config** command is run in the ISQL CLI and used to view and set the Sybase database parameters.

### Syntax

**sp\_configure** *parameter parameter value*

### Parameter Description

[Table E-4](#) describes the parameters.

**Table E-4** Condition List Description

| Parameter                         | Description                                                                                                                                             |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| parameters of the Sybase database | Parameters of the Sybase database to be viewed or set. When you view and set the parameters, place a parameter name between single quotation marks ("). |

### Examples

Assume that the Sybase database is installed in **/opt/sybase**, the database instance name is Sybase\_server, and the password of the **sa** user is password. The task in this example is to set the **max memory** parameter of the Sybase database to **2048 MB**.

#### NOTE

For details about parameter settings, see the related documents of the Sybase database.

1. In the command prompt window, run the following command to connect to the Sybase database. For details about the **isql** command, see [E.3 isql Command](#).

 **NOTE**

The asterisk (\*) is a wild card. Because the Sybase database has different versions, the asterisk (\*) is used to stands for a version.

```
cd /opt/sybase/OCS-*/bin
```

```
./isql -SSYB_server -Usa -Ppassword
```

2. Query the value of **max memory**:

```
1> sp_configure 'max memory'
```

```
2> go
```

The parameter value similar to the following is displayed:

| Parameter Name | Default           | Memory Used | Config Value |
|----------------|-------------------|-------------|--------------|
| Run Value      | Unit              | Type        |              |
| -----          |                   |             |              |
| max memory     | 53248             | 1048576     | 524288       |
| 524288         | memory pages (2k) | dynamic     |              |

```
(1 row affected)
(return status = 0)
```

3. Set the value of **max memory**:

```
1> sp_configure 'max memory',2097152
```

```
2> go
```

 **NOTE**

- If the prompt contains **(1 row affected)** and **(return status = 0)**, it indicates that the setting is successful. In the case of a failure, find out the cause according to the prompt.
- In this sample, the memory unit is 2 KB, so the parameter value is **2097152** (2 KB), that is, 2048 MB x 1024 x 2.





# F Reference of Oracle Database Commands

---

This topic describes the common command reference of the Oracle database, including command functions and usage examples.

## [F.1 sqlplus Command](#)

This topic describes the **sqlplus** command used for access the Oracle database.

## [F.2 startup Command](#)

This topic describes the **startup** command used for starting the Oracle database.

## [F.3 shutdown Command](#)

This topic describes the **shutdown** command used for shutting down the Oracle database.

## [F.4 show Command](#)

This topic describes the **show** command used for viewing operational parameters of the Oracle database.

## [F.5 alter Command](#)

This topic describes the **alter** command used for changing operational parameters of the Oracle database.

## F.1 sqlplus Command

This topic describes the **sqlplus** command used for access the Oracle database.

### Function

The **sqlplus** command is used to connect to the Oracle database. You can run SQL statements in the SQL command line window or configure the Oracle database.

### Syntax

**sqlplus parameter**

### Parameter Description

**Table F-1** describes the option.

**Table F-1** Option

| Option    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| parameter | <p>Only parameters that are used to access the Oracle database are described here. They are classified into two types: <b>/ as sysdba</b> and <b>user/password</b>. For more parameter setting methods, see the related documents provided by the Oracle company.</p> <ul style="list-style-type: none"><li>● <b>/ as sysdba</b> indicates that the user connects the Oracle database as <b>sysdba</b>. The <b>sysdba</b> user has the permissions to start and stop the Oracle database. This connection mode is applicable only to the Oracle user.</li><li>● <b>dbuser/password</b> indicates that the database user connects the Oracle database as <b>dbuser</b>. <b>password</b> is the password of the <b>dbuser</b> user. In this mode, the <b>dbuser</b> user performs operations according to the permissions assigned.</li></ul> |

### Example

Assume that the **root** user already logs in to the SUSE Linux OS. The OS user name of the Oracle database is **oracle**.

In the command prompt window, run the related command to connect to the Oracle database.

- Method 1: Switch to the **oracle** user. Connect the Oracle database as **sysdba**.  
# **su - oracle**

```
$ sqlplus / as sysdba
```

If the following information is displayed, it indicates that the Oracle database is connected successfully. In the case of a failure, find out the cause according to the prompt.

```
SQL>
```

- Method 2: Log in to the SUSE Linux OS as the **root** user. Connect the Oracle database as the **system** user. Assume that the password of the **system** user is **testpwd**.

```
$ sqlplus system/testpwd
```

If the following information is displayed, it indicates that the Oracle database is connected successfully. In the case of a failure, find out the cause according to the prompt.

```
SQL>
```

## F.2 startup Command

This topic describes the **startup** command used for starting the Oracle database.

### Function

In the SQL command line window, the **startup** command is used to start the Oracle database.

### Syntax

**startup parameter**

### Parameter Description

**Table F-2** describes the parameters.

**Table F-2** Parameters

| Parameter | Description                                                                                                                                                                |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| null      | The database is started normally. After the <b>startup</b> command is run, the instances are started, then the database is installed, and finally the database is started. |
| force     | The database is started forcibly. When the database cannot be closed normally, the <b>startup force</b> command is used to close and then start the database.              |
| nomount   | Only the instances are started.                                                                                                                                            |
| mount     | The database is installed after the instances are started.                                                                                                                 |

### Example

Assume that the **oracle** user, who has the permission to manage the Oracle database, already logs in to SUSE Linux.

In the command prompt window, after you run the following command to connect to the Oracle database, run the **startup** command to start the Oracle database.

```
$ sqlplus / as sysdba
```

#### NOTE

For details on how to use the **sqlplus** command, see [F.1 sqlplus Command](#).

```
> 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.

## F.3 shutdown Command

This topic describes the **shutdown** command used for shutting down the Oracle database.

### Function

In the SQL command line window, the **shutdown** command is used to shut down the Oracle database.

### Syntax

**shutdown** *parameter*

### Parameter Description

[Table F-3](#) describes the parameters.

**Table F-3** Parameters

| Parameter               | Description                                                                                                      |
|-------------------------|------------------------------------------------------------------------------------------------------------------|
| normal                  | To close the database, dismount the database, and close the instances after all users are disconnected.          |
| immediate (recommended) | To roll back all user transactions, and then close the database, dismount the database, and close the instances. |

| Parameter     | Description                                                                                                                                                                                                                                                     |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| transactional | To close the database, dismount the database, and close the instances when all user transactions end.                                                                                                                                                           |
| abort         | <p>To terminate the instances immediately. Ongoing user transactions are restored at next start.</p> <p><b>NOTE</b></p> <p>The <b>abort</b> parameter is used when the database cannot be closed normally. The use of this parameter may lead to data loss.</p> |

## Example

Assume that the **oracle** user, who has the permission to manage the Oracle database, already logs in to SUSE Linux.

In the command prompt window, run the following command to connect to the Oracle database, and then run the **shutdown** command to shut down the Oracle database.

```
$ sqlplus / as sysdba
```



### NOTE

For details on how to use the **sqlplus** command, see [F.1 sqlplus Command](#).

```
> shutdown immediate
```

The following is a sample display:

```
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.

## F.4 show Command

This topic describes the **show** command used for viewing operational parameters of the Oracle database.

### Function

In the SQL command line window, the **show** command is used to view operational parameters of the Oracle database.

### Syntax

```
show parameter parameter
```

## Parameter Description

**Table F-4** describes the parameters.

**Table F-4** Parameters

| Parameter | Description                                                                                       |
|-----------|---------------------------------------------------------------------------------------------------|
| null      | Lists all operational parameters of the Oracle database with three columns: name, type and value. |
| parameter | Displays the value of the specified <b>parameter</b> .                                            |

### Example 1

Assume that the **oracle** user, who has the permission to manage the Oracle database, already logs in to SUSE Linux.

This example describes how to view all operational parameters of the Oracle database.

In the command prompt window, run the following command to connect to the Oracle database, and then run the **show** command to view all operational parameters of the Oracle database.

```
$ sqlplus / as sysdba
```

#### NOTE

For details on how to use the **sqlplus** command, see [F.1 sqlplus Command](#).

> **show parameter**

The following is a sample display that contains part of contents:

```
...
NAME TYPE VALUE

undo_management string AUTO
undo_retention integer 900
undo_tablespace string UNDOTBS1
use_indirect_data_buffers boolean FALSE
user_dump_dest string /opt/oracle/oradb/home/admin/i
 mapdb/udump
utl_file_dir string
workarea_size_policy string AUTO
```

### Example 2

Assume that the **oracle** user, who has the permission to manage the Oracle database, already logs in to SUSE Linux.

This example describes how to view the value of **processes**.

In the command prompt window, run the following command to connect to the Oracle database, and then run the **show** command to view operational parameters of the Oracle database.

```
$ sqlplus / as sysdba
```

#### NOTE

For details on how to use the **sqlplus** command, see [F.1 sqlplus Command](#).

> **show parameter** *processes*

The information of all the parameters containing **processes** is displayed:

| NAME                      | TYPE    | VALUE |
|---------------------------|---------|-------|
| aq_tm_processes           | integer | 0     |
| db_writer_processes       | integer | 1     |
| gcs_server_processes      | integer | 0     |
| job_queue_processes       | integer | 10    |
| log_archive_max_processes | integer | 2     |
| processes                 | integer | 150   |

## F.5 alter Command

This topic describes the **alter** command used for changing operational parameters of the Oracle database.

### Function

In the SQL command line window, the **alter** command is used to change operational parameters of the Oracle database.

### Syntax

**alter option 1 parameter 1 option 2 parameter 2...**

### Parameter Description

[Table F-5](#) describes the options.

**Table F-5** Option list

| Option     | Description                                                                                                                                                                                                                                                                                                                                                                                |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| user       | Indicates that you can set the information about the user of the Oracle database. For example, you can set the user password.<br><b>NOTE</b><br>The example in this topic describes only how to change the password of an Oracle user. For more parameter settings, see the related documents provided by the Oracle company.                                                              |
| system set | Indicates that you can set the system parameters of the Oracle database.<br><b>NOTE</b><br>The example in this topic describes only how to change the system parameter of the Oracle database. Take parameter values according to actual situations. The example is for your reference only. For more parameter setting methods, see the related documents provided by the Oracle company. |

### Example 1

Assume that the **oracle** user, who has the permission to manage the Oracle database, already logs in to SUSE Linux.

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

```
$ sqlplus / as sysdba
```

 **NOTE**

For details on how to use the **sqlplus** command, see [F.1 sqlplus Command](#).

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.

## Example 2

Assume that the **oracle** user, who has the permission to manage the Oracle database, already logs in to SUSE Linux.

Initialize the operational parameter **processes**. Set the number of concurrent processes that connects to the Oracle database to **1024**.

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

```
$ sqlplus / as sysdba
```

 **NOTE**

For details on how to use the **sqlplus** command, see [F.1 sqlplus Command](#).

Run the following command to change the operational parameter of the Oracle database:

```
> alter system set processes=1024 scope=spfile;
```

**processes** is the operational parameter to be changed. **scope=spfile** indicates that **processes** is the initialized parameter of the database. To view the current value of **processes**, see [F.4 show Command](#).

If **User altered** is displayed, it indicates that modification is successful; otherwise, find out the cause for failure according to the prompt.



# G Common Commands for HA System (Veritas Hot Standby)

---

The common commands and their functions for the HA system (Veritas Hot Standby) are described.

## [G.1 Overview of Commands](#)

The software for Veritas includes VxVM, VVR, VCS, and GCO. The common commands are classified into status query commands and maintenance commands. The software for the high availability (HA) system (Sun Cluster) includes VxVM and Sun Cluster. The common commands are classified into status query commands and maintenance commands.

## [G.2 Status Query Commands](#)

You can use the status query commands to check the statuses of the volume, RLink, RVG, disks, disk groups, and HA system. The commands are usually used for routine patrol. In this way, you can proceed with the next operation according to the current status.

## [G.3 Maintenance Command](#)

When the HA system becomes abnormal, you can run the following command to repair the fault.

## G.1 Overview of Commands

The software for Veritas includes VxVM, VVR, VCS, and GCO. The common commands are classified into status query commands and maintenance commands. The software for the high availability (HA) system (Sun Cluster) includes VxVM and Sun Cluster. The common commands are classified into status query commands and maintenance commands.

### Commands

**Table G-1** Common commands

| Command                        | Description                                                                      |
|--------------------------------|----------------------------------------------------------------------------------|
| <a href="#">G.2.1 vxprint</a>  | Displays the VxVM configuration information.                                     |
| <a href="#">G.2.2 vxdisk</a>   | Displays the disk information.                                                   |
| <a href="#">G.2.3 vxdg</a>     | Displays the disk group information.                                             |
| <a href="#">G.2.4 vradm</a>    | Displays the configuration information and related commands of data replication. |
| <a href="#">G.2.5 hastatus</a> | Displays the current status information of VCS.                                  |
| <a href="#">G.3.1 hagr</a>     | Displays related commands of VCS resource groups.                                |
| <a href="#">G.3.2 hstop</a>    | Shuts down the VCS server.                                                       |
| <a href="#">G.3.3 hgui</a>     | Starts the VCS graphical user interface.                                         |

### Generic Naming Rules of Veritas Commands

- The commands of VxVM usually start with "vx".
- The commands of VVR usually start with "vr".
- The commands of VCS usually start with "ha".

### Generic Formats of Veritas Commands

- Format of query commands of VxVM: command list
- Format of VCS commands (hares and hagr): command -action, resource/resource group -sys host name

 **NOTE**

The actions often include online, offline, and clear.

### Query methods of Veritas Command Help

- command -H

- `man` command

## Directories of Saving Veritas Commands

- `/opt/VRTS/bin`
- `/usr/bin`
- `/usr/sbin`

## G.2 Status Query Commands

You can use the status query commands to check the statuses of the volume, RLink, RVG, disks, disk groups, and HA system. The commands are usually used for routine patrol. In this way, you can proceed with the next operation according to the current status.

### [G.2.1 vxprint](#)

You can check the statuses of the volume, RLink, and RVG.

### [G.2.2 vxdisk](#)

You can check whether the disks managed by Veritas are normal.

### [G.2.3 vxdg](#)

You can check whether the disk groups managed by Veritas are normal.

### [G.2.4 vradmin](#)

You can query the replication status.

### [G.2.5 hastatus](#)

You can query the VCS status.

## G.2.1 vxprint

You can check the statuses of the volume, RLink, and RVG.

## Application Scenarios

- Check the statuses of the volume, RLink, and RVG.
- Query the status during routine patrol and fault maintenance.

## Command Formats

- View the volume status: **`vxprint -v`**.
- View the RVG status:
  - **`vxprint -V`**
  - **`vxprint -l datarvg`**
- View the RLink status:
  - **`vxprint -P`**
  - **`vxprint -l datarlk`**

## Screen Output Format

| TY | NAME | ASSOC | KSTATE | LENGTH | PLOFFS | STATE | TUTILO | PUTILO |
|----|------|-------|--------|--------|--------|-------|--------|--------|
|----|------|-------|--------|--------|--------|-------|--------|--------|

**Table G-2** Screen output format description of vxprint

| Screen Output Format | Description                                                                                                                                                                                                                                                                                                                             |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TY                   | Type. In general, "dg" indicates the disk group, "dm" indicates the disk, "v" indicates the volume, "rl" indicates the RLink, and "rv" indicates RVG. "pl" and "sd" can be neglected.                                                                                                                                                   |
| NAME                 | Name. It indicates names of the volume, RVG, and RLink.                                                                                                                                                                                                                                                                                 |
| ASSOC                | Association. For the volume, if it is attached to an RVG, the RVG name is displayed; otherwise, "gen" is displayed. For the RLink, if it is attached to an RVG, the RVG name is displayed; otherwise, "-" is displayed. For an srl_vol volume, if it is attached to an RVG, the RVG name is displayed; otherwise, "fsgen" is displayed. |
| KSTATE               | Normally, it is ENABLED for the volume, CONNECT for the RLink, and ENABLED for the RVG.                                                                                                                                                                                                                                                 |
| STATE                | Normally, it is ACTIVE for the volume, RLink, and RVG.                                                                                                                                                                                                                                                                                  |

**Table G-3** Screen output description of vxprint -l datarlk

| Field Name | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Disk group | The disk group to which RLINK belongs.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Rlink      | RLINK name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| info       | Some information about RLINK. <b>timeout</b> indicates timeout time, and <b>packet_size</b> indicates packet length.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| state      | The state of RLINK. Normally, it is ACTIVE, synchronous state is off, latencyprot state is off and srlprot state is autodcm.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| assoc      | Association information of RLINK. <ul style="list-style-type: none"> <li>● rvg refers to the RVG to which this RLINK belongs</li> <li>● remote_host refers to remote host name</li> <li>● IP_addr refers to the IP address of the remote host</li> <li>● port refers to port No. of the remote host</li> <li>● remote_dg refers to remote disk group</li> <li>● remote_dg_dgid refers to remote disk group ID</li> <li>● remote_rvg_version refers to remote host's RVG version No.</li> <li>● remote_rlink refers to the name of remote host's RLINK</li> <li>● remote_rlink_rid refers to remote host's RLINK ID</li> <li>● local_host refers to local host's IP address</li> <li>● port refers to port No. of local host</li> </ul> |
| protocol   | Data synchronization protocol.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

| Field Name | Description                                                                                                              |
|------------|--------------------------------------------------------------------------------------------------------------------------|
| flags      | The flag for RLINK, which should be <b>write enabled attached consistent connected asynchronous</b> in the normal state. |

**Table G-4** Screen output description of **vxprint -l datarvg**

| Field Name | Description                                                                                                                                                                                         |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Disk group | The disk group to which this RVG belongs.                                                                                                                                                           |
| Rvg        | RVG name.                                                                                                                                                                                           |
| info       | The information about RVG.                                                                                                                                                                          |
| state      | The state of RVG. Normally, it should be <b>ACTIVE</b> and kernel should be <b>ENABLED</b> .                                                                                                        |
| assoc      | The association information of RVG.<br>datavols refers to data disk volumes contained in RVG, srl refers to the SRLog disk volume contained in RVG and rlinks refers to the Rlink contained in RVG. |
| att        | The Rlink activated by RVG.                                                                                                                                                                         |
| flags      | The flag information of RVG, which should be <b>closed primary enabled attached</b> normally.                                                                                                       |
| device     | The device information of RVG, containing device ID and trail.                                                                                                                                      |
| perms      | The authority information of RVG.                                                                                                                                                                   |

## G.2.2 vxdisk

You can check whether the disks managed by Veritas are normal.

### Application Scenarios

- Check whether the disks managed by Veritas are normal.
- Check the disks during routine maintenance.

### Command Formats

```
vxdisk list
```

### Screen Output Format

|        |      |      |       |        |
|--------|------|------|-------|--------|
| DEVICE | TYPE | DISK | GROUP | STATUS |
|--------|------|------|-------|--------|

**Table G-5** Screen output format description of vxdisk

| Screen Output Format | Description                                                            |
|----------------------|------------------------------------------------------------------------|
| DEVICE               | Equipment number. It is usually "c*t*d*", which indicates a hard disk. |
| TYPE                 | Type. It is usually "auto:sliced".                                     |
| DISK                 | Disk name.                                                             |
| GROUP                | Disk group name.                                                       |
| STATUS               | Normally, it is online.                                                |

## G.2.3 vx dg

You can check whether the disk groups managed by Veritas are normal.

### Application Scenarios

- Check whether the disk groups managed by Veritas are normal.
- Check the disk groups during routine maintenance.

### Command Formats

```
vx dg list
```

### Screen Output Format

|      |       |    |
|------|-------|----|
| NAME | STATE | ID |
|------|-------|----|

**Table G-6** Screen output format description of vx dg

| Screen Output Format | Description                                                                                                       |
|----------------------|-------------------------------------------------------------------------------------------------------------------|
| NAME                 | Disk group name. It is datadg in the case of two hard disks, and rootdg in the case of at least three hard disks. |
| STATE                | Enabled.                                                                                                          |
| ID                   | Disk group ID, which can be neglected.                                                                            |

## G.2.4 vradmin

You can query the replication status.

### Application Scenarios

- Query the replication status.

- Query the status during routine patrol and fault maintenance. In this way, you can proceed with the next operation according to the current status.

## Command Formats

- `# vradmin printrvg RVG name`
- `# vradmin -g datadg repstatus RVG name`

## Screen Output Format

The screen output of **vradmin printrvg datarvg** is as follows:

```
Replicated Data Set: datarvg
Primary:
 HostName: 129.9.1.1 <localhost>
 RvgName: datarvg
 DgName: datadg
Secondary:
 HostName: 129.9.1.2
 RvgName: datarvg
 DgName: datadg
```

**Table G-7** Screen output format description

| Screen Output Format                | Description                                        | Example                          |
|-------------------------------------|----------------------------------------------------|----------------------------------|
| Replicated Data Set                 | RVG name.                                          | It is datarvg in this example.   |
| Primary                             | Active site, which is the data replication source. | -                                |
| HostName: IP address<br><localhost> | IP address of the local site.                      | It is 129.9.1.1 in this example. |
| RvgName                             | RVG name.                                          | It is datarvg in this example.   |
| DgName                              | Disk group that the RVG belongs to.                | It is datadg in this example.    |
| Secondary                           | Standby site, which is the data replication sink.  | -                                |
| HostName: IP address                | IP address of the remote site.                     | It is 129.9.1.2 in this example. |
| RvgName                             | RVG name.                                          | It is datarvg in this example.   |
| DgName                              | Disk group that the RVG belongs to.                | It is datadg in this example.    |

The screen output of **vradmin -g datadg repstatus datarvg** is as follows:

```
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: consistent, up-to-date
Replication status: replicating (connected)
Current mode: asynchronous
Logging to: SRL
Timestamp Information: behind by 0h 0m 0s

```

**Table G-8** Screen output format description

| Screen Output Format | Description                                          | Example                                |
|----------------------|------------------------------------------------------|----------------------------------------|
| Replicated Data Set  | RVG name.                                            | It is datarvg in this example.         |
| Primary              | Active site.                                         | -                                      |
| Host name            | IP address of the active site.                       | It is 129.9.1.1 in this example.       |
| RVG name             | RVG name of the active site.                         | It is datarvg in this example.         |
| DG name              | Disk group that the RVG belongs to.                  | It is datadg in this example.          |
| RVG state            | RVG status. Normally, the status is enabled for I/O. | it is enabled for I/O in this example. |
| Data volumes         | Disk volumes to be replicated.                       | It is 1 in this example.               |
| SRL name             | SRL name.                                            | It is srl_vol in this example.         |
| SRL size             | SRL size, which is usually 1G.                       | It is 1G in this example.              |
| Total secondaries    | Standby site count, which is usually 1.              | It is 1 in this example.               |
| Secondary            | Standby site.                                        | -                                      |
| Host name            | IP address of the standby site.                      | It is 129.9.1.1 in this example.       |
| RVG name             | RVG name of the standby site.                        | It is datarvg in this example.         |
| DG name              | Disk group that the RVG belongs to.                  | It is datadg in this example.          |



| Screen Output Format  | Description                                                                                                                                                                                                                                             | Example                                       |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|
| Data status           | Data status. <ul style="list-style-type: none"><li>● If the active site is synchronous with the standby site, the status is consistent, up-to-date.</li><li>● Otherwise, the status is inconsistent (the number of bytes to be synchronized).</li></ul> | It is consistent, up-to-date in this example. |
| Replication status    | Replication status. Normally, the status is replicating (connected).                                                                                                                                                                                    | It is replicating(connected) in this example. |
| Current mode          | Replication mode, which is usually asynchronous.                                                                                                                                                                                                        | It is asynchronous in this example.           |
| Logging to            | Buffer area, which is usually SRL. In the case of SRL overflow, it is DCM.                                                                                                                                                                              | It is SRL in this example.                    |
| Timestamp Information | Time stamp. If the data is consistent between the active and standby sites, it is N/A. Otherwise, the time for synchronization is specified.                                                                                                            | It is N/A in this example.                    |

## G.2.5 hastatus

You can query the VCS status.

### Application Scenarios

- Query the VCS status for the Veritas hot standby system.
- Query the status during routine patrol and fault maintenance. In this way, you can proceed with the next operation according to the current status.

### Command Examples

- `# hastatus -sum`  
View the status of each service group in the VCS.
- `# hastatus`  
View the status of each resource in the VCS.

### Screen Output Format

The screen output of the **hastatus -sum** command is as follows:

**Table G-9** Screen output format description

| Screen Output Format                                | Description                                                                                    |
|-----------------------------------------------------|------------------------------------------------------------------------------------------------|
| A primary RUNNING 0                                 | The VCS running status of the current node. Normally, it is RUNNING.                           |
| B AppService Primary Y N ONLINE                     | The name of the application group of the primary node is AppService, and the status is ONLINE. |
| B ClusterService Primary Y N ONLINE                 | The name of the heartbeat group is ClusterService, and the status is ONLINE.                   |
| B VVRService Primary Y N ONLINE                     | The name of the data replication group is VVRService, and the status is ONLINE.                |
| L Icmp SecondaryCluster ALIVE                       | The heartbeat status between the primary and secondary nodes. Normally, it is ALIVE.           |
| M SecondaryCluster RUNNING                          | The VCS running status of the remote node. Normally, it is RUNNING.                            |
| N secondaryCluster:secondary RUNNING 0              | The running status of the secondary node. Normally, it is RUNNING.                             |
| O AppService SecondaryCluster:Secondary Y N OFFLINE | The application group of the secondary node. The status is OFFLINE.                            |

The screen output of the **hastatus** command is as follows:

 **NOTE**

To terminate the **hastatus** command, press the shortcut keys **Ctrl+C**.

**Table G-10** Screen output format description

| Screen Output Format                    | Description                                                                                                                                         |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| SecondaryCluster RUNNING                | The running status of the remote node. Normally, it is RUNNING.                                                                                     |
| HB:Icmp SecondaryCluster ALIVE          | The heartbeat status of the remote node. Normally, it is ALIVE.                                                                                     |
| SecondaryCluster:Secondary RUNNING      | The server running status of the remote site. Normally, it is RUNNING.                                                                              |
| AppService localclus:Primary ONLINE     | The running status of the local application group. Normally, the status on the active site is ONLINE and the status on the standby site is OFFLINE. |
| ClusterService localclus:Primary ONLINE | The running status of the local heartbeat group. Normally, it is ONLINE.                                                                            |

| Screen Output Format                          | Description                                                                                                                                                                                                                                      |
|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VVRService localclus:Primary ONLINE           | The running status of the local data replication group. Normally, it is ONLINE.                                                                                                                                                                  |
| AppService SecondaryCluster:Secondary OFFLINE | The running status of the remote application group. Normally, the status on the active site is ONLINE and the status on the standby site is OFFLINE.                                                                                             |
| EMSApp SecondaryCluster:Secondary OFFLINE     | The running status of a single local resource. Normally, the application group status of the active site is ONLINE, the application group status of the standby site is OFFLINE, and the status of resources in other resource groups is ONLINE. |

## G.3 Maintenance Command

When the HA system becomes abnormal, you can run the following command to repair the fault.

### [G.3.1 hagrp](#)

You can control the VCS resource groups.

### [G.3.2 hastop](#)

This section describes how to forcibly shut down the VCS server in the Veritas hot standby.

### [G.3.3 hagui](#)

This section describes how to start the VCS graphical user interface (GUI) in the Veritas hot standby.

## G.3.1 hagrp

You can control the VCS resource groups.

### Application Scenarios

Control the VCS resource groups.

### Command Formats

- `# hagrp -online resource group name -sys host name`
- `# hagrp -offline resource group name -sys host name`
- `# hagrp -freeze resource group name -sys host name`
- `# hagrp -unfreeze resource group name -sys host name`
- `# hagrp -clear resource group name -sys host name`

### Examples

- `# hagrp -online AppService -sys Primary`  
Start the U2000 server on the primary site.

 **NOTE**

Prerequisites:

- All the groups that the resource group depends on are online.
- The resource group is not frozen.

Operation result: The U2000 server is started.

If you perform the online operation the first time, the **-force** parameter is required. For example:  
**hagrp -online -force AppService -sys Primary**.

- **# hagrp -offline AppService -sys Primary**  
Shut down the U2000 server on the primary site.

 **NOTE**

Prerequisites:

- All the groups that depend on the resource group are offline.
- The resource group is not frozen.

Operation result: The U2000 server is shut down.

- **# hagrp -freeze AppService -sys Primary**  
Freeze the AppService group on the primary site.

 **NOTE**

Prerequisites: None

Operation result: The resource group is locked. The VCS no longer monitors this resource group. That is, the VCS function is disabled.

- **# hagrp -unfreeze AppService -sys Primary**  
Unfreeze the AppService group on the primary site.

 **NOTE**

Prerequisites: None

Operation result: The resource group is unlocked. The VCS function is enabled.

- **# hagrp -clear AppService -sys Primary**  
Clear faults of the AppService group on the primary site.

 **NOTE**

Prerequisites: The status of a resource group is **FAULT**. In this case, a resource is usually faulty. For example, a core dump of the U2000 process occurs.

Operation result: The error tag of the VCS is cleared. In this way, the online operation can be performed.

## G.3.2 hastop

This section describes how to forcibly shut down the VCS server in the Veritas hot standby.

### Application Scenarios

Forcibly shut down the VCS server. The VCS server cannot be normally shut down by running the `/etc/rc3.d/S99vcs` script.

### Command Formats

```
hastop -all -force
```

### Examples

```
hastop -all -force
```

Forcibly shut down the VCS server.

 **NOTE**

Prerequisites: None

Operation result: The VCS server is forcibly shut down. The status of VCS resources is not offline.

## G.3.3 hagui

This section describes how to start the VCS graphical user interface (GUI) in the Veritas hot standby.

### Application Scenarios

Start the VCS GUI.

### Command Formats

```
hagui
```

### Examples

```
hagui
Start the VCS GUI.
```



# H Common Maintenance Tools

---

This topic describes the maintenance tools that are commonly used in the U2000.

**Table H-1** show the maintenance tools that are commonly used in the U2000.

**Table H-1** Common maintenance tools in the U2000

| Tool                 | Functions                                                                                                                        |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------|
| QuickStep            | Collects the fault information about the U2000 and performs routine inspection.                                                  |
| NMS Maintenance Tool | Deploys the U2000, manages the database, backs up and restores the database, initializes the database, and maintains the system. |
| SetSolaris           | Reinforces the security of the NMS in the Solaris OS.                                                                            |





---

# I 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         |