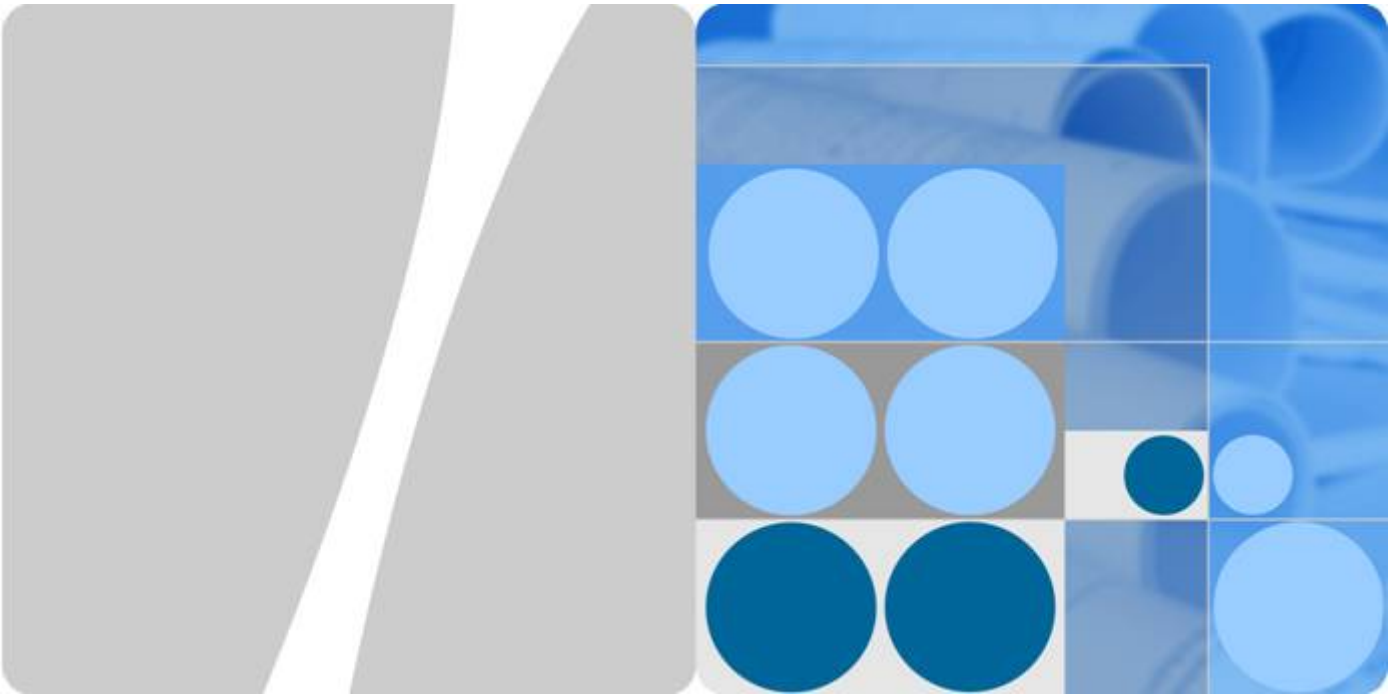


iManager U2000 Unified Network Management System

V200R014C60

Routine Maintenance

Issue 04

Date 2015-11-20

HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2015. 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

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 a 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

Copyright © Huawei Technologies Co., Ltd.

About This Document

Related Version

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

Product Name	Version
iManager U2000	V200R014C60

Intended Audience

This document describes the suggestions for secure running, the method of obtaining the technical support for the iManager SecowayU2000, and how to perform routine maintenance on a daily, weekly, monthly, or quarterly basis.

Through routine maintenance, you can detect and rectify the potential faults to ensure secure, stable, and reliable running of the U2000.

The intended audience of this document is system maintenance engineers.

Symbol Conventions

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

Symbol	Description
	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
	Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.

Copyright © Huawei Technologies Co., Ltd.

Symbol	Description
	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
	Calls attention to important information, best practices and tips. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

Command Conventions

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

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

GUI Conventions

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

Convention	Description
Boldface	Buttons, menus, parameters, tabs, window, and dialog titles are in **boldface**. For example, click **OK**.

Copyright © Huawei Technologies Co., Ltd.

Convention	Description
>	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 04 (2015-11-20) Based on Product Version V200R014C60

The fourth commercial release has the following updates:

Fixed some bugs.

Changes in Issue 03 (2015-08-30) Based on Product Version V200R014C60

The third commercial release has the following updates:

Fixed some bugs.

Changes in Issue 02 (2015-02-28) Based on Product Version V200R014C60

The second commercial release has the following updates:

Fixed some bugs.

Changes in Issue 01 (2014-11-30) Based on Product Version V200R014C60

Initial release.

Copyright © Huawei Technologies Co., Ltd.

Contents

About This Document ii

1 Security Instructions (Routine Maintenance) 1

2 Maintenance Item List 14

3 Obtaining Technical Support 19

4 Daily Maintenance 20

4.1 Viewing Current Alarms 22
4.2 Querying OSS Logs 23
4.3 Checking the Resource Usage of the U2000 Server 26
4.4 Checking the Status of Network Communications Between the U2000 and NEs 27
4.5 Checking the Running Status of the Processes and Services of the U2000 29
4.6 Checking the HA System Resource Status 33
4.7 Checking the Status of Data Replication Between the Primary and Secondary Sites in the Veritas High Availability System 36
4.8 Backing Up the U2000 Data 43
4.9 Monitoring the Status of the HA System 44

5 Weekly Maintenance 46

5.1 Checking the Disk Space of the U2000 Server 48
5.2 Checking the Logs of the OS 48
5.3 Checking the Logs of the SQL Server Database 50
5.4 Checking the Logs of the Sybase Database 50
5.5 Checking Operation Logs Associated with Project Deployment 51
5.6 Checking the Running Status of Anti-Virus Software 52
5.7 Checking the Database Status 53
5.8 Checking the Backing Up the U2000 Data 53

6 Monthly Maintenance 55

6.1 Checking User Configurations 56
6.2 Checking the DCN Bandwidth Between the Primary and Secondary Sites in a High Availability System 56
6.3 Backing Up System Files 57
6.4 Viewing Alarm Statistics 58
6.5 Checking the Server Time of the U2000 58
6.6 Changing the Password of the Current User 59

Copyright © Huawei Technologies Co., Ltd.

6.7 Checking U2000 Directories..... 60
6.8 Releasing the Disk Space of the U2000 Server..... 61
7 Quarterly Maintenance.....63
7.1 Checking the Disk Status of the U2000 Server..... 64
7.2 Checking the Equipment Room Environment..... 66
7.3 Checking the Power Supply of the U2000 Server..... 66
7.4 Checking Hardware and Peripherals of the U2000 Server..... 68
7.5 Check whether the U2000 license is expired.....69
7.6 Checking Maintenance Information..... 70
A Glossary and Abbreviations.....71

Copyright © Huawei Technologies Co., Ltd.

1 Security Instructions (Routine Maintenance)

This topic describes the suggestions on running security. To ensure normal running of the U2000, you must comply with the precautions for hardware and software operations.

Precautions for Hardware Operations

Pay attention to the following items during hardware operations:

- Configuring an independent uninterruptible power supply (UPS) for the U2000 server is recommended. This can avoid some serious problems such as hardware damage, system restoration failure, and data loss caused by abnormal power failure. If the independent UPS cannot be configured for the U2000 server, properly shut down the U2000 application and then the database, and then the OS, before the administrator cuts the power upon a power cut notification.
- You must properly shut down the U2000 server in any case. Do not run U2000 server or hardware on Solaris and SUSE Linux. Otherwise, the system will fail to be restored.
- Checking the network communication status on a daily basis according to routine maintenance items is recommended to avoid network communication interruption result in lost data or effect on system.
- Removing network cables from the server is prohibited if the U2000 is running. If unwanted network cables need to be removed, remove them after stopping U2000 services. Otherwise, the U2000 service will be affected.

  NOTE

  On Solaris and SUSE Linux, removing unwanted network cables may lead to intermittent network interruption.
- You must keep the equipment room clean, dustproof and moistureproof.

Precautions for Software Operations

Read carefully the following precautions for software operations for better U2000 O&M.

Copyright © Huawei Technologies Co., Ltd.

NOTICE

During U2000 O&M, any violation against the following precautions leads to service risks or system collapse. Read the precautions carefully and perform operation in strict compliance with them.

Table 1-1 Precautions on software operation

Item	Precautions	Risks	Remarks
OS	Do not install the OS that is incompatible with the U2000 version. For example, the OS is unauthorized, pirated, or incompatible with the U2000 version.	This operation may result in incompatibility between the OS and U2000 and consequently a failure to start the U2000 process.	For the mapping OS, see Chapter **Software Configuration Planning for the NMS Server** in *U2000 Planning Guide*.
	Do not install the system patch after OS installation is configured without confirmation by Huawei engineers. For example, do not install the third-party vulnerability patch and upgrade package.	● This operation may affect U2000 operation. ● This operation may result in system collapse.	● In normal cases, to install the system patch, you need to obtain the OS patch package from Huawei official website. ● If the patch package obtained from Huawei official website does not meet the requirement, contact Huawei engineers.

Copyright © Huawei Technologies Co., Ltd.

Item	Precautions	Risks	Remarks
	Do not add, delete, or modify the U2000 configuration file or permissions as the **root** or non-NMS user.	This operation may result in system failure.	-
	Do not enable insecure services that are irrelevant to the OS. For example, the Telnet and FTP services of the OS and the mail service.	This operation may bring risks of attacks.	Using the SSH and SFTP services is recommended because the SSH and SFTP services are more secure.
	Do not install the unwanted unauthenticated third-party application on the running U2000 server. For example, game software.	● A lot of system resources are consumed, which may lead to slow operation on the U2000. ● This operation may lead to security threats from virus attacks.	-
	Do not install unauthenticated antivirus software such as 360 antivirus software on the U2000 server.	This operation may cause exceptions such as U2000 file isolation or insufficient memory on the U2000.	Installing the OfficeScan is recommended.
	Do not use the OS hardening tools that are not provided the U2000.	This operation may result in system failure.	Use the OS hardening tools provided by the U2000.

Copyright © Huawei Technologies Co., Ltd.

Item	Precautions	Risks	Remarks
	Do not configure the U2000 server as the DNS server.	If the connection between the OS and DNS fails or is at a slow speed, the U2000 restart fails.	-
	Do not manually change the IP address and host name of OS.	This operation may lead to a failure to start U2000 processes.	If the IP address and host name of OS need to be changed, use the U2000 MSuite tool to change it. Ensure that the U2000 processes have been stopped before making such a change.
	Do not use the **reboot** or **init 6** command to restart the Solaris OS, and do not use **Stop+A** to switch to the **ok** prompt on the running U2000 server.	This operation may result in system failure.	-
	Do not use the switching partition **swap** as a normal partition.	This operation increases the usage of the switching partition **swap** and affects the U2000 operation speed.	-
	Do not leak the password. The permissions on passwords are classified based on the user level and can be assigned only to the maintenance owner.	This operation may lead to beyond authority operations.	-

Copyright © Huawei Technologies Co., Ltd.

Item	Precautions	Risks	Remarks
	Periodically change the OS password.	● After security hardening, you need to specify a validity period for the password. If you do not change the password in time, it will expire, causing a failure to log in to the OS. ● The password that has not been changed for a long time is less secure.	-
	Regularly check the size of the **/var/adm/pacct** file, the accounting file of the Solaris OS. If the size of the **/var/adm/pacct** file exceeds 2 GB, dump the data and then clean up the file.	This operation may slow down the system operation or event results in a primary/ secondary switchover.	-
Database	Do not install the database that is incompatible with the U2000 version. For example, the database is unauthorized, pirated, or incompatible with the U2000 version.	This operation may cause incompatibility between the database and the U2000 version and consequently a failure to start the U2000.	For the mapping OS, see Chapter **Software Configuration Planning for the NMS Server** in *U2000 Planning Guide*.

Copyright © Huawei Technologies Co., Ltd.

Item	Precautions	Risks	Remarks
	Do not manually log in to the database and perform operations on the database, such as adding, deleting, modifying, and viewing the database. For example, do not use T-SQL to change the U2000 database data or manually modify the **interfaces** file of the Sybase database.	This operation results in a data inconsistency between the U2000 and NEs. Accessing the database among different sets of U2000 results in a database disorder.	-
	Do not use the commands carried by the database to change the passwords of the **sa** and **dbuser** users.	This operation results in a failure to start U2000 processes.	If the passwords of the **sa** and **dbuser** users need to be changed, use the U2000 MSuite to change them.
	Do not leak the password. The permissions on passwords are classified based on the user level and can be assigned only to the maintenance owner. The administrator password can be managed only by the maintenance owner.	This operation may lead to beyond authority operations.	-

Copyright © Huawei Technologies Co., Ltd.

Item	Precautions	Risks	Remarks
	Periodically change the database password.	● After security hardening, you need to specify a validity period for the password. If you do not change the password in time, it will expire, causing a failure to log in to the database. ● The database password that has not been changed for a long time is less secure.	If the passwords of the **sa** and **dbuser** users need to be changed, use the U2000 MSuite to change them.
	Regularly back up the U2000 database. This minimizes damages if an exception occurs on the system.	If you do not back up the U2000 database, U2000 data may be lost upon system exceptions.	-
High availability system (Veritas)	Do not perform large-data-volume operations during full synchronization between the primary and secondary sites, such as searching for circuits and protection subnets and querying alarms on the entire network.	This operation may affect the performance of the entire U2000 high availability system.	-

Copyright © Huawei Technologies Co., Ltd.

Item	Precautions	Risks	Remarks
	In normal cases, the U2000 is running only on the primary site, and the secondary site works as a backup.	If the U2000 is running on both the primary and secondary sites, a major abnormality may occur. For example, this operation may lead to that the system enters the dual host status.	-
U2000	Do not browse web pages on the U2000 server. Do not configure unnecessary share directories. Pay attention to the permissions of a share directory.	● A lot of system resources are consumed, which may lead to slow operation on the U2000. ● This operation may bring risks of attacks.	-
	Do not connect another PC or laptop to the network where the U2000 server resides unless allowed.	Various issues may occur, such as IP address conflict and virus infection.	-

Copyright © Huawei Technologies Co., Ltd.

Item	Precautions	Risks	Remarks
	Do not use multiple sets of U2000 to manage an NE or use the U2000 and a third-party OSS together to manage an NE. For example, do not use MIBs to interconnect NEs when MIBs are being used by the U2000 to manage NEs. In addition, do not use the TR-069 server and U2000 together to manage ONT NEs.	● This operation results in discrete services, data inconsistency, and device CPU load growth. ● After one set of the U2000 is used to apply configurations to a router, other sets of the U2000 may fail to incrementally synchronize the configurations. In this situation, the data on the U2000s is inconsistent with the NE data. If operations are performed using these U2000s, configuration conflicts may occur, which interrupts services.	In scenarios where multiple sets of the U2000 are used in upgrading, contact the Huawei Technologies Co., Ltd. local representative office or customer service center.

Copyright © Huawei Technologies Co., Ltd.

Item	Precautions	Risks	Remarks
	Do not use both the U2000 and commands to manage the live network.	This operation results in a data inconsistency between the U2000 and NEs, and there is risk of deleting NE data.	-
	Do not modify the XML file of the ONT on the U2000 server.	This operation results in an inconsistency of the ONT XML file between the U2000 and NEs.	-
	Do not modify the system time during U2000 running.	This operation may cause time inconsistency between the U2000 and NEs and failures of some functions.	● To modify the system time of the server, exit the U2000 server and restart it after the modification. ● To modify the system time of the client, exit the U2000 client and restart it after the modification.
	Do not leak the password. The permissions on passwords are classified based on the user level and can be assigned only to the maintenance owner. The administrator password can be managed only by the maintenance owner.	This operation may lead to beyond authority operations.	-

Copyright © Huawei Technologies Co., Ltd.

Item	Precautions	Risks	Remarks
	Periodically change the NMS user password.	● After security hardening, you need to specify a validity period for the password. If you do not change the password in time, it will expire, causing a failure to log in to the U2000. ● The NMS user password that has not been changed for a long time is less secure.	-
	Refer to *Routine Maintenance* to regularly check and test the U2000 and record the results.	-	Troubleshoot faults in time. For the faults fail to be rectified, contact the Huawei Technologies Co., Ltd. local representative office or customer service center.

Copyright © Huawei Technologies Co., Ltd.

Item	Precautions	Risks	Remarks
	Use the UEasy tool to regularly perform health check on the U2000.	-	On Solaris or SUSE Linux, the UEasy tool is stored in the **$IMAP_ROOT/tools/UEasy** directory. On Windows, the UEasy tool is stored in the **%IMAP_ROOT%\tools\UEasy** directory. For details about how to use the UEasy tool, see the **readme_en.txt** file contained in the save path.
	After the DC is used to upgrade or degrade transport NEs, you must use the U2000 to upload the data about the involved transport NEs to the U2000 database.	This operation results in a failure to distribute services to transport NEs during transport NE configuration.	-
	Ensure data consistency between the U2000 and NEs.	If data is inconsistent between the U2000 and NEs, it may lead to misjudgment or misoperation.	-

Copyright © Huawei Technologies Co., Ltd.

Item	Precautions	Risks	Remarks
	The U2000 displays a warning message when a risky operation is to be performed. For example, a message is displayed indicating that services will be interrupted when data is to be downloaded from the U2000 to an NE.	-	-

Copyright © Huawei Technologies Co., Ltd.

2 Maintenance Item List

This topic describes the table listing the maintenance items on the basis of the maintenance period. According to the maintenance period, routine maintenance can be classified into daily maintenance, weekly maintenance, monthly maintenance, and quarterly maintenance. Refer to the table during the maintenance of the U2000.

NOTE

The routine maintenance item list varies according to the system implementation scheme.

- Single-Server System (Windows): To view items in the routine maintenance item list, see **Table 2-1**.
- Single-Server System (SUSE Linux): To view items in the routine maintenance item list, see **Table 2-2**.
- Single-Server System (Solaris): To view items in the routine maintenance item list, see **Table 2-3**.
- High Availability System (Solaris, SUSE Linux): To view items in the routine maintenance item list, see **Table 2-4**.

Table 2-1 List of maintenance items for a Single-Server System (Windows)

Maintenance Period	Routine Maintenance Task
Daily	**4.1 Viewing Current Alarms**
	4.2 Querying OSS Logs
	4.3 Checking the Resource Usage of the U2000 Server
	4.4 Checking the Status of Network Communications Between the U2000 and NEs
	4.5 Checking the Running Status of the Processes and Services of the U2000
	4.8 Backing Up the U2000 Data
Weekly	**7.1 Checking the Disk Status of the U2000 Server**
	5.1 Checking the Disk Space of the U2000 Server
	5.2 Checking the Logs of the OS
	5.3 Checking the Logs of the SQL Server Database

Copyright © Huawei Technologies Co., Ltd.

Maintenance Period	Routine Maintenance Task
	5.6 Checking the Running Status of Anti-Virus Software
	5.7 Checking the Database Status
	5.8 Checking the Backing Up the U2000 Data
Monthly	6.1 Checking User Configurations
	6.3 Backing Up System Files
	6.4 Viewing Alarm Statistics
	6.5 Checking the Server Time of the U2000
	6.6 Changing the Password of the Current User
	6.8 Releasing the Disk Space of the U2000 Server
Quarterly	7.2 Checking the Equipment Room Environment
	7.3 Checking the Power Supply of the U2000 Server
	7.4 Checking Hardware and Peripherals of the U2000 Server

Table 2-2 List of maintenance items for a Single-Server System (SUSE Linux)

Maintenance Period	Routine Maintenance Task
Daily	4.1 Viewing Current Alarms
	4.2 Querying OSS Logs
	4.3 Checking the Resource Usage of the U2000 Server
	4.4 Checking the Status of Network Communications Between the U2000 and NEs
	4.5 Checking the Running Status of the Processes and Services of the U2000
	4.8 Backing Up the U2000 Data
Weekly	7.1 Checking the Disk Status of the U2000 Server
	5.1 Checking the Disk Space of the U2000 Server
	5.2 Checking the Logs of the OS
	5.4 Checking the Logs of the Sybase Database
	5.6 Checking the Running Status of Anti-Virus Software
	5.7 Checking the Database Status

Copyright © Huawei Technologies Co., Ltd.

Maintenance Period	Routine Maintenance Task
	5.8 Checking the Backing Up the U2000 Data
Monthly	**6.1 Checking User Configurations**
	6.3 Backing Up System Files
	6.4 Viewing Alarm Statistics
	6.5 Checking the Server Time of the U2000
	6.6 Changing the Password of the Current User
	6.8 Releasing the Disk Space of the U2000 Server
Quarterly	**7.2 Checking the Equipment Room Environment**
	7.3 Checking the Power Supply of the U2000 Server
	7.4 Checking Hardware and Peripherals of the U2000 Server

Table 2-3 List of maintenance items for a Single-Server System (Solaris)

Maintenance Period	Routine Maintenance Task
Daily	**4.1 Viewing Current Alarms**
	4.2 Querying OSS Logs
	4.3 Checking the Resource Usage of the U2000 Server
	4.4 Checking the Status of Network Communications Between the U2000 and NEs
	4.5 Checking the Running Status of the Processes and Services of the U2000
	4.8 Backing Up the U2000 Data
Weekly	**7.1 Checking the Disk Status of the U2000 Server**
	5.1 Checking the Disk Space of the U2000 Server
	5.2 Checking the Logs of the OS
	5.4 Checking the Logs of the Sybase Database
	5.6 Checking the Running Status of Anti-Virus Software
	5.7 Checking the Database Status
	5.8 Checking the Backing Up the U2000 Data
Monthly	**6.1 Checking User Configurations**

Copyright © Huawei Technologies Co., Ltd.

Maintenance Period	Routine Maintenance Task
	6.3 Backing Up System Files
	6.4 Viewing Alarm Statistics
	6.5 Checking the Server Time of the U2000
	6.6 Changing the Password of the Current User
	6.8 Releasing the Disk Space of the U2000 Server
Quarterly	7.2 Checking the Equipment Room Environment
	7.3 Checking the Power Supply of the U2000 Server
	7.4 Checking Hardware and Peripherals of the U2000 Server

Table 2-4 List of maintenance items for a High Availability System (Solaris, SUSE Linux)

Maintenance Period	Routine Maintenance Task
Daily	4.1 Viewing Current Alarms
	4.2 Querying OSS Logs
	4.3 Checking the Resource Usage of the U2000 Server
	4.4 Checking the Status of Network Communications Between the U2000 and NEs
	4.5 Checking the Running Status of the Processes and Services of the U2000
	4.7 Checking the Status of Data Replication Between the Primary and Secondary Sites in the Veritas High Availability System
	4.8 Backing Up the U2000 Data
	4.9 Monitoring the Status of the HA System
Weekly	7.1 Checking the Disk Status of the U2000 Server
	5.1 Checking the Disk Space of the U2000 Server
	5.2 Checking the Logs of the OS
	5.4 Checking the Logs of the Sybase Database
	5.6 Checking the Running Status of Anti-Virus Software
	5.7 Checking the Database Status
	5.8 Checking the Backing Up the U2000 Data
Monthly	6.1 Checking User Configurations

Copyright © Huawei Technologies Co., Ltd.

Maintenance Period	Routine Maintenance Task
	6.3 Backing Up System Files
	6.4 Viewing Alarm Statistics
	6.5 Checking the Server Time of the U2000
	6.6 Changing the Password of the Current User
	6.8 Releasing the Disk Space of the U2000 Server
Quarterly	**7.2 Checking the Equipment Room Environment**
	7.3 Checking the Power Supply of the U2000 Server
	7.4 Checking Hardware and Peripherals of the U2000 Server

Copyright © Huawei Technologies Co., Ltd.

3 Obtaining Technical Support

This topic describes how to obtain technical support in the case of any problems encountered during routine maintenance.

During routine maintenance of the U2000, if there is any problem that is uncertain or hard to solve, or if you cannot find the solution to a problem from this manual, contact the customer service center of Huawei or send an email to **support@huawei.com**. Go to **http://support.huawei.com/carrier** to obtain the latest technical materials of Huawei.

NOTE

- Before seeking technical support, collect the relevant information.
- Only Huawei technical support engineers have the right to obtain some documents. Therefore, if these documents are required, contact Huawei technical support engineers.

Copyright © Huawei Technologies Co., Ltd.

4 Daily Maintenance

About This Chapter

This topic describes how to perform daily maintenance. Daily maintenance allows you to collect the information about the running status and trend of the U2000 in real time, which improves the efficiency of handling emergencies.

4.1 Viewing Current Alarms
This topic describes how to view current alarms. This function allows you to know the running status of the live network. During network maintenance, you must acknowledge the alarm information and take proper measures on time.

4.2 Querying OSS Logs
By querying OSS logs, you can understand the U2000 operating status, system security status, or specific user operation information.

4.3 Checking the Resource Usage of the U2000 Server
This topic describes how to check the resource usage of the U2000 server. If the CPU usage, memory usage, disk usage, or database usage exceeds the normal value, the system runs slowly. Checking the current running status of the U2000 server periodically is recommended to find and solve problems as soon as possible and ensure efficient running of the system.

4.4 Checking the Status of Network Communications Between the U2000 and NEs
This topic describes how to check the status of network communications between the U2000 server and the managed NEs.

4.5 Checking the Running Status of the Processes and Services of the U2000
This topic describes how to check the running status of the processes and services of the U2000 periodically to ensure the normal running of the U2000.

4.6 Checking the HA System Resource Status
If an HA system resource is in the **Faulted** state, the **Faulted** label must be removed immediately; otherwise, the switchover of the primary and secondary sites will be abnormal. This topic describes how to check the HA system resource status and remove the **Faulted** label.

4.7 Checking the Status of Data Replication Between the Primary and Secondary Sites in the Veritas High Availability System
This topic describes how to check the status of data replication between the primary and secondary sites in the Veritas high availability system.

Copyright © Huawei Technologies Co., Ltd.

4.8 Backing Up the U2000 Data
This topic describes how to back up the U2000 data. You can back up the U2000 data to a local or remote server. In this way, the data can be securely and quickly restored when a fault occurs.

4.9 Monitoring the Status of the HA System
This topic describes how to check the OS, Veritas monitor, Veritas data volume, Veritas replication, and U2000 status on the primary and secondary sites and whether to perform an active/standby switchover based on the check results.

Copyright © Huawei Technologies Co., Ltd.

4.1 Viewing Current Alarms

This topic describes how to view current alarms. This function allows you to know the running status of the live network. During network maintenance, you must acknowledge the alarm information and take proper measures on time.

Procedure

Step 1 Log in to a U2000 client.

Step 2 Choose **Fault** > **Browse Current Alarm** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarm** > **Browse Current Alarm** from the main menu (application style).

Step 3 On the **Filter** tab page, set filter criteria and click **OK**. The tab page for viewing current alarms is displayed.

NOTE

If you have already set the startup template for viewing current alarms, the **Filter** dialog box will not be displayed, but the alarms that meet the startup template criteria will be directly displayed.

Step 4 Select an alarm. Details about the alarm and the handling suggestions are displayed in the bottom pane.

Step 5 **Optional:** Right-click an alarm in the query result area. Then, perform the following steps as required:

- Choose **Memo** from the shortcut menu to set remarks for the alarm.
- Choose **Acknowledge** from the shortcut menu to acknowledge the alarm.

  NOTE

  - If the selected alarm is an unacknowledged and uncleared alarm, it changes to an acknowledged but uncleared alarm after confirmation.
  - If the selected alarm is an unacknowledged but cleared alarm, the alarm changes to a historical alarm after confirmation.
- Choose **Query Opposite Port Alarms** from the shortcut menu to query the alarms of the opposite port that is connected by the optical fiber.
- Choose **Mask** from the shortcut menu to mask the alarm.

NOTE

The shortcut menu operation varies according to alarms.

Step 6 **Optional:** Select one or more uncleared alarms, right-click, and then choose **Clear** from the shortcut menu. In the dialog box that is displayed, click **Yes**.

The service status restores after the fault is rectified.

Step 7 **Optional:** Select the **Display latest alarms** check box to view the reported alarms in real time.

Step 8 **Optional:** Click the buttons in the lower pane to perform the following steps:

- Click **Template** to new, open, save, or delete an alarm filtering template.
- Click **Filter** to set filter criteria.

Copyright © Huawei Technologies Co., Ltd.

- Click **Synchronize** to synchronize current alarms.
- If an alarm reported from the equipment is changed, a message is displayed indicating a new alarm. Click **Refresh** to refresh current alarms.
- Click **Acknowledge** to acknowledge current alarms.
- Click **Clear** to clear current alarms.

Step 9 **Optional:** On a Veritas high availability system, log in to the VCS client and check whether the resource group has a fault tag. If the resource group has a fault tag, select the resource node corresponding to the fault tag (for example, AppService), right-click, and then choose **Clear Fault** > ***host name*** from the shortcut menu to clear the fault tag.

----End

Troubleshooting

Select the alarm to be handled, and then clear the alarm according to the **Handling Suggestion** in the table at the bottom of the window.

4.2 Querying OSS Logs

By querying OSS logs, you can understand the U2000 operating status, system security status, or specific user operation information.

Context

- Query results are generated based on the existing data in the database. If the database is empty, no query result is displayed.
- Different users have different log query rights. For details, see **Table 4-1**.

Table 4-1 Log query rights

Log Type	Operation Rights
Operation logs	● Users in the **Administrators** group or users who have the **Query All Operation Logs** permission can query operation logs of all users. ● Users in the **SMManagers** group who have the **Query Operation Logs** permission can query operation logs of all users. ● Common users who do not belong to the **Administrators** or **SMManagers** group and who have the **Query Operation Logs** permission can query only their own operation logs.
System logs	● Users who have the **Query System Logs** permission can query system logs.

Copyright © Huawei Technologies Co., Ltd.

Log Type	Operation Rights
Security logs	● Users in the **SMManagers** group can query security logs of all users. ● Users who have the **Query All Security Logs** permission can query security logs of all users. ● Users in a group of the **Subdomain Security Administrator Group** type can view their own and their managed users' security logs. ● Users who have the **Query Security Logs** permission can query their own security logs.

Procedure

Step 1 Choose a menu portal.

- Querying operation logs: Choose **Administration** > **Log Management** > **Query Operation Logs** from the main menu (traditional style); alternatively, double-click **Security Management** in **Application Center** and choose **Log Management** > **Query Operation Logs** from the main menu (application style) from from the main menu.
- Querying system logs: Choose **Administration** > **Log Management** > **Query System Logs** from the main menu (traditional style); alternatively, double-click **Security Management** in **Application Center** and choose **Log Management** > **Query System Logs** from the main menu (application style) from from the main menu.
- Querying security logs: Choose **Administration** > **Log Management** > **Query Security Logs** from the main menu (traditional style); alternatively, double-click **Security Management** in **Application Center** and choose **Log Management** > **Query Security Logs** from the main menu (application style) from from the main menu.

Step 2 In the **Filter** dialog box, set filter criteria and click **OK**.

Step 3 Right-click OSS logs in the query result window and choose the following operations from the shortcut menu:

Operation	Method
Details	Right-click a log in the window and choose **Details** from the shortcut menu, or double-click the log. **NOTE** The **Log Details** dialog box displays log information, such as the operation time, risk level, or operation result.

Copyright © Huawei Technologies Co., Ltd.

Operation	Method
Save All Records	1. Right-click a log in the window and choose **Save All Records** from the shortcut menu. 2. In the **Save** dialog box, select the path to save all the records, and click **Save**. **NOTE** ● Log records can be saved as a file in **.txt**, **.html**, **.csv**, **.pdf**, **.xls** or **.xlsx** format. When a user saves a log file in **.xls** or **.xlsx** format, a cell can support a maximum of 32,767 characters. ● For .txt files, code formats **ISO-8859-1** and **UTF-8** are supported. The default encoding format is **ISO-8859-1**. You are advised to use the default encoding format if the saved file does not need to support multiple languages; otherwise, **UTF-8** is recommended. ● The **Progress** dialog box is displayed if numerous log records exist. You can click **Background** in the **Progress** dialog box or press **Enter** to perform other operations on the background.
Save Selected Records	1. Select one or more logs in the query window, right-click, and choose **Save Selected Records** from the shortcut menu. 2. In the **Save** dialog box, select the path to save the records and click **Save**. **NOTE** ● Log records can be saved as a file in **.txt**, **.html**, **.csv**, **.pdf**, **.xls** or **.xlsx** format. When a user saves a log file in **.xls** or **.xlsx** format, a cell can support a maximum of 32,767 characters. ● For .txt files, code formats **ISO-8859-1** and **UTF-8** are supported. The default encoding format is **ISO-8859-1**. You are advised to use the default encoding format if the saved file does not need to support multiple languages; otherwise, **UTF-8** is recommended. ● The **Progress** dialog box is displayed if numerous log records exist. You can click **Background** in the **Progress** dialog box or press **Enter** to perform other operations on the background.
Save Specified Records	1. Right-click a log in the window and choose **Save Specified Records** from the shortcut menu. 2. In the **Save Specified Records** dialog box, set the start and end log records and the name of the file to be saved, and click **OK**. **NOTE** ● In the **Save Specified Records** dialog box, click on the right of **File name**. In the **Save** dialog box, select the path for saving the records. Log records can be saved as a file in **.txt**, **.html**, **.csv**, **.pdf**, **.xls** or **.xlsx** format. When a user saves a log file in **.xls** or **.xlsx** format, a cell can support a maximum of 32,767 characters. ● For .txt files, code formats **ISO-8859-1** and **UTF-8** are supported. The default encoding format is **ISO-8859-1**. You are advised to use the default encoding format if the saved file does not need to support multiple languages; otherwise, **UTF-8** is recommended. ● The **Progress** dialog box is displayed if numerous log records exist. You can click **Background** in the **Progress** dialog box or press **Enter** to perform other operations on the background.

Copyright © Huawei Technologies Co., Ltd.

Operation	Method
Print All Records	1. Right-click a log in the window and choose **Print All Records** from the shortcut menu. 2. In the **Print** dialog box, set the print parameters and click **Print**.
Print Selected Records	1. Select one or more logs in the query window, right-click, and choose **Print Selected Records** from the shortcut menu. 2. In the **Print** dialog box, set the print parameters and click **Print**.
Print Specified Records	1. Right-click a log in the window and choose **Print Specified Records** from the shortcut menu. 2. In the **Print Specified Records** dialog box, set the start and end log records and click **OK**. 3. In the **Print** dialog box, set the print parameters and click **Print**.
Find	Enter a keyword in **Find what** in the **Find** dialog box for search. **NOTE** ● Match case: determines whether the case of search contents matches the case of the keyword. By default, the cases do not match. ● Match entire cell contents: If you want the search contents to partially match the cell contents, clear **Match entire cell contents**. If you want the search contents to exactly match the cell contents, select **Match entire cell contents**. By default, **Match entire cell contents** is cleared.

----End

4.3 Checking the Resource Usage of the U2000 Server

This topic describes how to check the resource usage of the U2000 server. If the CPU usage, memory usage, disk usage, or database usage exceeds the normal value, the system runs slowly. Checking the current running status of the U2000 server periodically is recommended to find and solve problems as soon as possible and ensure efficient running of the system.

Context

If the CPU usage, memory usage, disk usage, or database usage of the server exceeds a preset threshold, the sysmonitor server sends an alarm to the U2000 server. Meanwhile, the related record in the sysmonitor client turns red.

Procedure

Step 1 Double-click the related shortcut icon on the desktop to start the U2000 System Monitor client.

Step 2 Click the **Server Monitor** tab and view information such as the CPU usage, total physical memory, and free physical memory of the server.

Step 3 Click the **Hard Disk Monitor** tab and view the disk usage.

Step 4 Click the **Database Monitor** tab and view the data space usage and the log space usage.

----End

Copyright © Huawei Technologies Co., Ltd.

Reference Standards

Check Item	Standard
CPU usage rate	Lower than 85%
Memory usage rate	Lower than 95%
Disk usage rate	Lower than 80%
Data usage rate	Lower than 85%
Log usage rate	Lower than 80%

Troubleshooting

If the hardware configuration of the server does not meet the performance requirement for the ever increasing number of managed equipment, upgrade the hardware configuration or replace the server with a new one.

4.4 Checking the Status of Network Communications Between the U2000 and NEs

This topic describes how to check the status of network communications between the U2000 server and the managed NEs.

Context

In addition to the following network connectivity ping test, the availability of service ports and protocols needs to be checked. For details, see the section "U2000 Port List" in *U2000 Administrator Guide*.

Procedure

Step 1 Log in to a U2000 client.

Step 2 View the icons of equipment nodes in the navigation tree.

----End

Reference Standard

In the device tree, if the icon of an NE node is not in gray, the communication status of the NE is normal.

NOTE

You can choose **File** > **Preferences** to customize icon colors. The icon color described in this document is the default setting of the system.

Copyright © Huawei Technologies Co., Ltd.

Troubleshooting

- For datacomm and access devices:
  - If the icon of a device node is gray, it indicates that the device is offline. In this case, do as follows:
    i. Right-click a device node and choose **Tool** > **Ping** from the shortcut menu to ping the device.

    NOTE

    If the ping fails, check whether the physical link of the network is abnormal.

    ii. Right-click a device node and choose **Refresh Status** from the shortcut menu.

    If the icon of the device node still fails to turn green, contact Huawei technical support engineers.
  - If the icon of a device node is not green, it indicates that a fault occurs on the device. In this case, contact the maintenance personnel of the equipment room immediately to check the device.
- For transport equipment: If the communication between the U2000 and an NE is abnormal, the icon of this NE is grayed out in the user interface of the U2000. If the communication between the U2000 and a GNE is abnormal, the NE_COMMU_BREAK alarm is also reported, indicating that the NE communication is interrupted. Locate and clear the fault in the following methods according to the actual situation:
  - If only a non-GNE is unreachable to the U2000, check the settings of the NE, and the ECC route between this NE and the GNE. Perform the check in the sequence below:
    i. Check whether the ECC route between the NE and the GNE is normal. For example, you can view the ECC route status in the NE ECC Link Management user interface of the NE Explorer.
    ii. Check whether the configurations such as the NE ID and extended ID are correct. These configurations on the U2000 must be consistent with those on the equipment.
    iii. On the U2000, check whether the user name and password of the user that logs in to the NE are correct.
  - If many NEs are unreachable to the U2000, check the settings of the corresponding GNE, and the network connectivity between the U2000 and the GNE. Perform the check in the sequence below:
    i. Check the network connectivity between the U2000 and the GNE. For example, you can run the ping command to check the packet loss ratio and the network connectivity between the U2000 and the GNE.
    ii. Check whether the communication parameters (for example, IP address, subnet mask, and gateway IP address) of the U2000 and GNE are correct. If not, modify the parameters.
    iii. Check whether the configurations such as the GNE ID and extended ID are correct. These configurations on the U2000 must be consistent with those on the equipment.
    iv. On the U2000, check whether the user name and password of the user that logs in to the GNE are correct.

Copyright © Huawei Technologies Co., Ltd.

4.5 Checking the Running Status of the Processes and Services of the U2000

This topic describes how to check the running status of the processes and services of the U2000 periodically to ensure the normal running of the U2000.

Procedure

- Perform the following steps in a Single-Server System (Windows), Single-Server System (SUSE Linux) and Single-Server System (Solaris):

  Check the process status in U2000 System Monitor client.

  a. Log in to the U2000 System Monitor client.

  b. Click the **Process Monitor** tab and view the running statuses of all processes on the U2000 server and of the **Database Server Process**.

  NOTE

  On Solaris or SUSE Linux, you can also run the following command to check whether the U2000 processes are started:

  Log in to the operating system of the server as the **ossuser** user.

  $ **cd /opt/oss/server/platform/bin**

  $ **svc_adm -cmd status**

  After you run the preceding commands, the started processes and the not running processes are displayed.

- Perform the following steps in a High Availability System:
  - On the primary site, query the status of all the services and service groups of the U2000 by using the VCS browser.

    i. Run the following command to log in to the graphical user interface (GUI) of the VCS Cluster Explorer:

    # **hagui &**

    ii. In the **Cluster Monitor** window, click **Click here to log in**.

    iii. In the login dialog box, enter the user name and password for logging in to the VCS. Then, click **OK**.

    NOTE

    The default VCS user name is **admin** and the default password is **Changeme_123**. To ensure system security, change the default password in time. If the default password has been changed, enter the new password. For details, see **FAQs** > **Veritas HA System** > **System Settings** > **How to Change the admin User Password for Logging In to the VCS Client** in the *U2000 Administrator Guide*.

    iv. Access the **Cluster Explorer** window. For the service groups including ClusterService, AppService, and VVRService, click the **Status** tab respectively to view the status.
  - Query the status of all services and service groups by using commands on the primary site.

    i. Run the following command to view the status of all service groups in the VCS:

    # **hastatus -sum**

Copyright © Huawei Technologies Co., Ltd.

The following information is displayed:

```
-- SYSTEM STATE
-- System              State            Frozen

A  Pri_master          RUNNING          0

-- GROUP STATE
-- Group           System              Probed    AutoDisabled
State

B  AppService      Pri_master          Y         N
ONLINE
B  ClusterService  Pri_master          Y         N
ONLINE
B  VVRService      Pri_master          Y         N
ONLINE

-- WAN HEARTBEAT STATE
-- Heartbeat       To                  State

L  Icmp             Sec_masterCluster  ALIVE

-- REMOTE CLUSTER STATE
-- Cluster         State

M  Sec_masterCluster RUNNING

-- REMOTE SYSTEM STATE
-- cluster:system State Frozen

N  Sec_masterCluster:Sec_master  RUNNING          0

-- REMOTE GROUP STATE
-- Group            cluster:system    Probed    AutoDisabled
State

O  AppService       Sec_masterCluster:Sec_master  Y     N
OFFLINE
```

ii. Run the following command to view the status of all services in the VCS:

 # hastatus

The following information is displayed:

```
group           resource             cluster:system
message
--------------- -------------------- --------------------
--------------------
                                     Sec_masterCluster
RUNNING
HB:Icmp                              Sec_masterCluster
ALIVE
                                     localclus:Pri_master
RUNNING
                                     Sec_masterCluster:Sec_master
RUNNING

-------------------------------------------------------------------------
----
AppService                           localclus:Pri_master
ONLINE
ClusterService                       localclus:Pri_master
ONLINE
VVRService                           localclus:Pri_master
ONLINE
AppService                           Sec_masterCluster:Sec_master
OFFLINE

-------------------------------------------------------------------------
----
```


Copyright © Huawei Technologies Co., Ltd.

```
                NMSServer           localclus:Pri_master
ONLINE
                datarvg_primary     localclus:Pri_master
ONLINE
                DatabaseServer      localclus:Pri_master
ONLINE
                BackupServer        localclus:Pri_master
ONLINE
                wac                 localclus:Pri_master
ONLINE

-------------------------------------------------------------------
----
                webip               localclus:Pri_master
ONLINE
                csgnic              localclus:Pri_master
ONLINE
                VCSweb              localclus:Pri_master
ONLINE
                VVRServiceNIC       localclus:Pri_master
ONLINE
                datarvg             localclus:Pri_master
ONLINE

-------------------------------------------------------------------
----
                VCShm               localclus:Pri_master
ONLINE
                NMSServer           Sec_masterCluster:Sec_master
OFFLINE
                datarvg_primary     Sec_masterCluster:Sec_master
OFFLINE
                DatabaseServer      Sec_masterCluster:Sec_master
OFFLINE
                BackupServer        Sec_masterCluster:Sec_master
OFFLINE
```

NOTE

- If NBIs are enabled, the command output contains the information about NBIs, such as CorbaApp and SNMPApp.
- If the IPMP protection scheme is used, the command output does not contain information about the webip, csgnic, and VVRServiceNIC resources.
- If the IPMP feature is enabled, the name of the **Cluster** service group is the same as the host name of the computer.
- To stop running commands, press the shortcut keys **Ctrl+C**.

----End

Reference Standard

- In the Single-Server System (Windows), Single-Server System (SUSE Linux) and Single-Server System (Solaris), all processes status in U2000 System Monitor client are running and no process has been restarted repeatedly.
- In a High Availability System:
  - If you use the VCS Cluster Explorer and all service groups and services meet the standards in the following table, the service groups and services of the high availability System run properly.

Copyright © Huawei Technologies Co., Ltd.

Table 4-2 Standard status of services and service groups in VCS Cluster Explorer

Resource Group Name	Check Item	Reference Standard
AppService Group	Group Status on Member Systems	The service group on the active site is in the **Online** state.
	Resource Status	Each service is in the **Online on Pri_master** state.
	Remote cluster	The system members are in the **Offline** state.
ClusterServic e Group	Group Status on Member Systems	Each service on the primary site is in the **Online** state.
	Resource Status	Each service is in the **Online on Pri_master** state.
VVRService Group	Group Status on Member Systems	Each service on the active site is in the **Online** state.
	Resource Status	Each service is in the **Online on Pri_master** state.

- If you use command lines to query the status of service groups and services that meet the standards in the following table, the service groups and services of the high availability system run properly.

Table 4-3 Standard status of services and service groups by using command lines

Command	Check Item	Reference Standard
hastatus -sum	SYSTEM STATE	**System** is displayed as **RUNNING** on the primary and secondary sites.
	GROUP STATE	All groups on the primary site, including ClusterService, AppService, and VVRService, are in the **ONLINE** state.
hastatus	resource	All services on the primary site are in the **ONLINE** state.

Troubleshooting

- Do as follows in the Single-Server System (Windows), Single-Server System (SUSE Linux) and Single-Server System (Solaris):
  - If a process is not in the **RUNNING** state, use **System Monitor client** to restart the process.
  - Check the settings of the process startup mode and set a proper startup mode for the selected process.

Copyright © Huawei Technologies Co., Ltd.

NOTE

The available starting modes of a process are as follows:

- Automatic: The process automatically restarts after it exits abnormally.
- Manual: The process does not automatically restart after it exits abnormally. In this case, you must manually start it.
- Disabled: Do not start processes. The system cannot automatically restart the process. You cannot manually start it either. To start the process, you must change the startup mode to automatic start or manual start by using the System Monitor client.

  - If the process cannot be started, log in to the server to rectify the fault.

- Do as follows in the High Availability System:

  If there is an abnormal process on the master server of the primary site, the system automatically restarts the process. If the restart fails for three times, perform active/standby switchover to ensure the normal running of the entire U2000.

  Contact the local office or customer service center of Huawei according to the warranty.

4.6 Checking the HA System Resource Status

If an HA system resource is in the **Faulted** state, the **Faulted** label must be removed immediately; otherwise, the switchover of the primary and secondary sites will be abnormal. This topic describes how to check the HA system resource status and remove the **Faulted** label.

Context

The cause of a faulty resource may be a U2000 or database process abnormality.

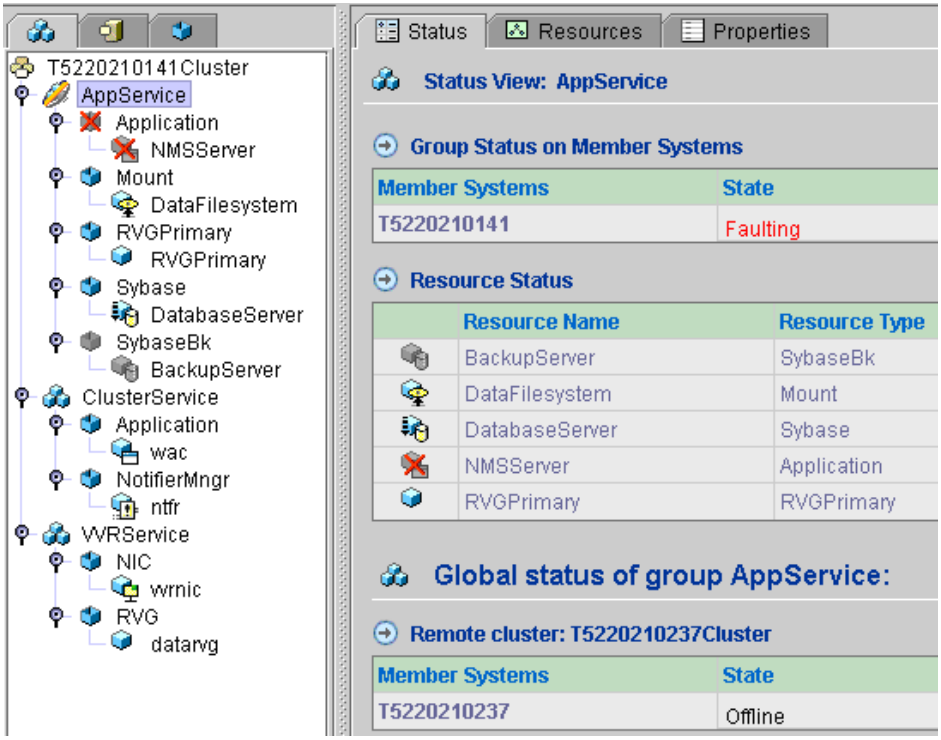
Procedure

Step 1 Log in to the VCS client.

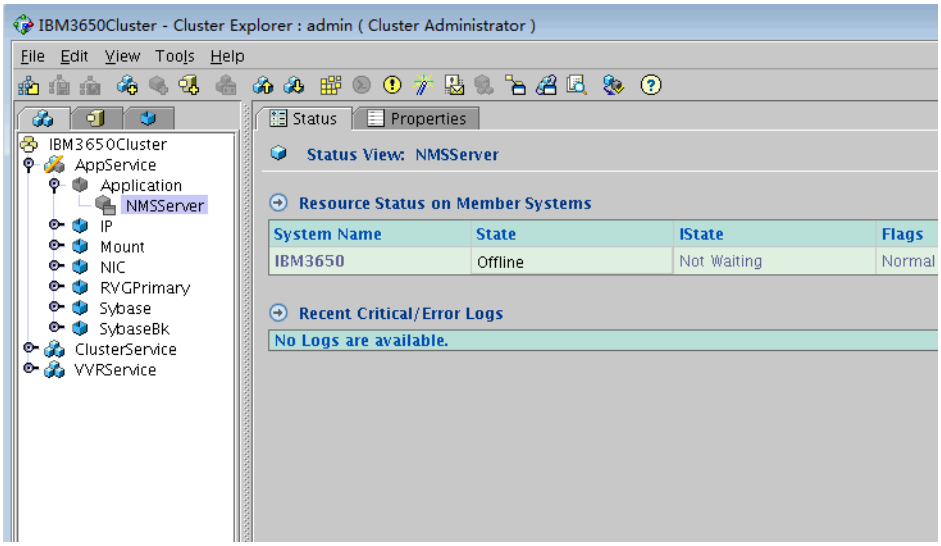
Step 2 Check whether any HA system resource is in the **Faulted** state. If a red cross is displayed for a resource, the resource is in the **Faulted** state.

- High Availability System (Solaris):

Copyright © Huawei Technologies Co., Ltd.



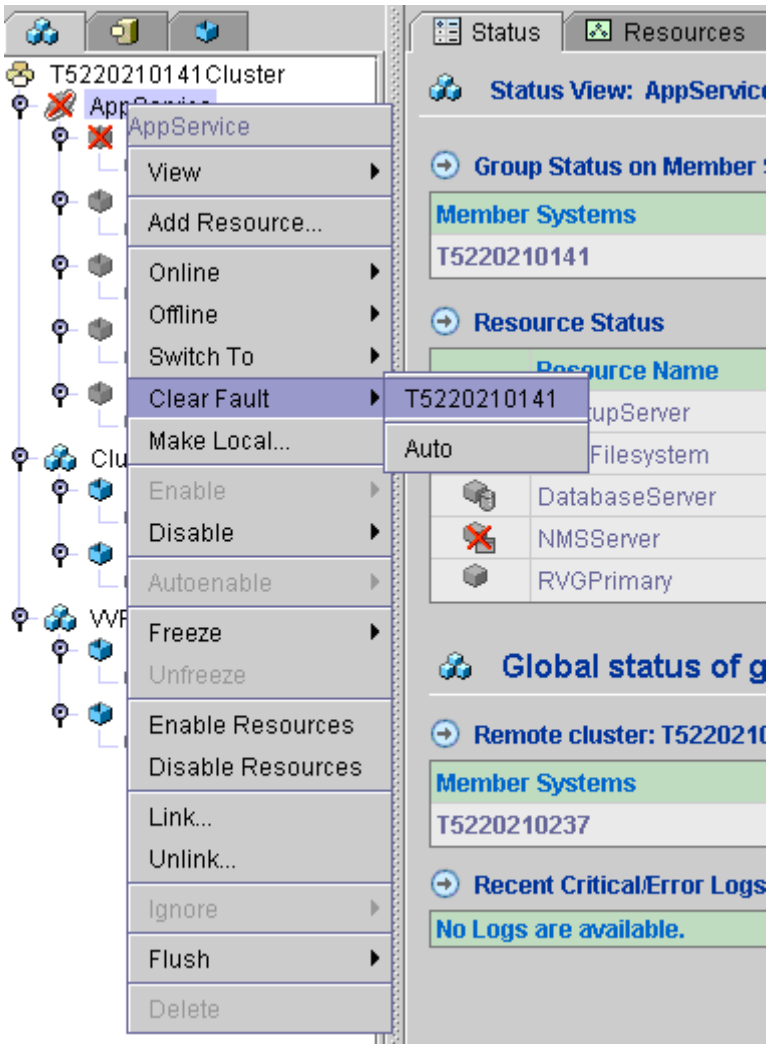
- High Availability System (SUSE Linux):



Step 3 Right-click the name of the resource in the **Faulted** state and choose **Clear Fault** > ***site name*** from the shortcut menu to clear fault.

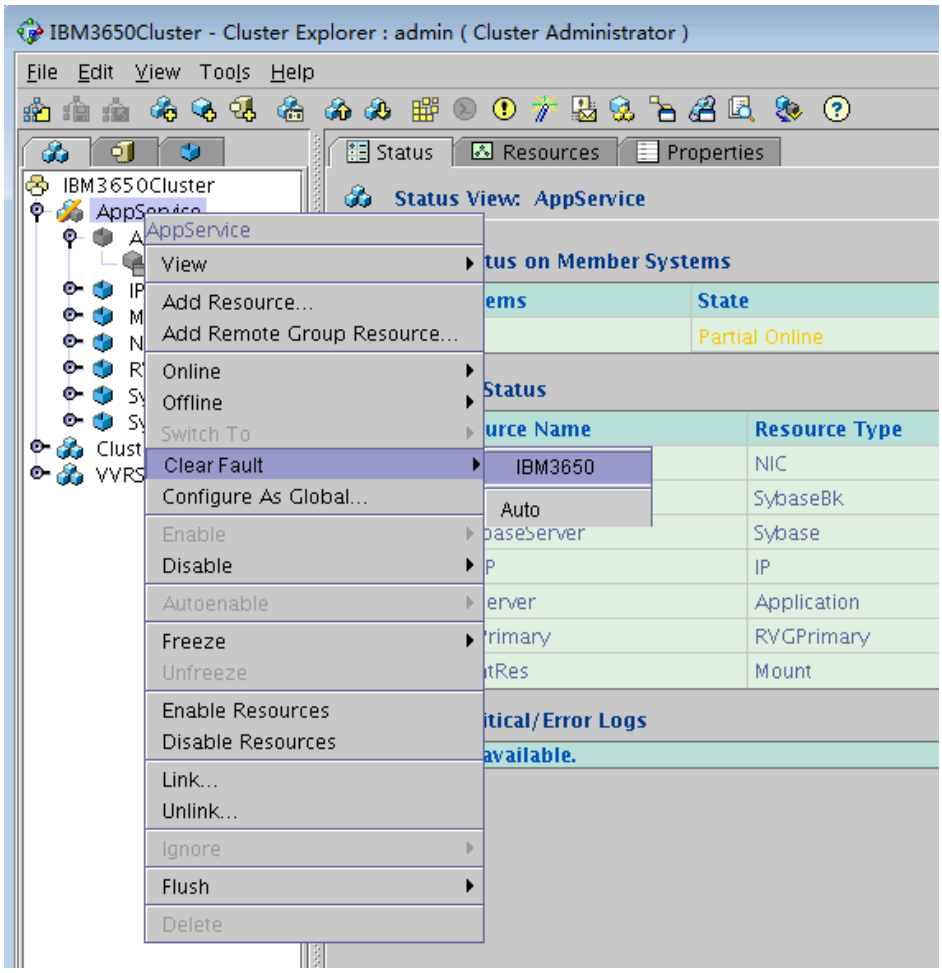
- High Availability System (Solaris):

Copyright © Huawei Technologies Co., Ltd.



- High Availability System (SUSE Linux):

Copyright © Huawei Technologies Co., Ltd.



----End

Follow-up Procedure

In the case of the active site, restart the HA system after removing a **Faulted** label. To restart the HA system, right-click **AppService** and choose **Online** > ***site name*** from the shortcut menu.

4.7 Checking the Status of Data Replication Between the Primary and Secondary Sites in the Veritas High Availability System

This topic describes how to check the status of data replication between the primary and secondary sites in the Veritas high availability system.

Procedure

- On Solaris:
  a. Log in to the OS as the ossuser user.
  b. Open a CLI. Then, run the following commands to switch to the **root** user:

     $ **su - root**

Copyright © Huawei Technologies Co., Ltd.

`Password:` *password_of_user_root*

c. Run the following command to view the disk usage on the primary and secondary sites:

 # df -h

The following information is displayed:

```
Filesystem             kbytes      used      avail         capacity
Mounted on
/dev/vx/dsk/bootdg/rootvol
                       12G   3.8G   7.9G    33%    /
/devices                0K     0K     0K     0%    /devices
ctfs                    0K     0K     0K     0%    /system/contract
proc                    0K     0K     0K     0%    /proc
mnttab                  0K     0K     0K     0%    /etc/mnttab
swap                  9.1G   1.8M   9.1G     1%    /etc/svc/volatile
objfs                   0K     0K     0K     0%    /system/object
sharefs                 0K     0K     0K     0%    /etc/dfs/sharetab
/platform/sun4u-us3/lib/libc_psr/libc_psr_hwcap1.so.1
                       12G   3.8G   7.9G    33%    /platform/sun4u-
us3/lib/libc
_psr.so.1
/platform/sun4u-us3/lib/sparcv9/libc_psr/libc_psr_hwcap1.so.1
                       12G   3.8G   7.9G    33%    /platform/sun4u-
us3/lib/spar
cv9/libc_psr.so.1
fd                      0K     0K     0K     0%    /dev/fd
/dev/vx/dsk/bootdg/var
                      7.9G   1.4G   6.4G    19%    /var
swap                  9.1G   104K   9.1G     1%    /tmp
swap                  9.1G    40K   9.1G     1%    /var/run
swap                  9.1G     0K   9.1G     0%    /dev/vx/dmp
swap                  9.1G     0K   9.1G     0%    /dev/vx/rdmp
/dev/vx/dsk/bootdg/opt
                       64G   7.4G    56G    12%    /opt
/dev/vx/dsk/bootdg/home
                     1002M   1.0M   941M     1%    /export/home
/dev/odm                0K     0K     0K     0%    /dev/odm
/dev/vx/dsk/datadg/lv_nms_data
                       39G    40M    39G     1%    /opt/sybase/data
```

d. Run the following commands on the primary and secondary sites:

vxdisk list

In the case of two hard disks, a message similar to the following will be displayed:

```
DEVICE       TYPE            DISK         GROUP        STATUS
c1t0d0s2     auto:sliced     rootdisk     datadg       online
c1t1d0s2     auto:sliced     rootmirror   datadg       online
```

In the case of four hard disks, a message similar to the following will be displayed:

```
DEVICE       TYPE            DISK         GROUP        STATUS
c1t0d0s2     auto:slice     rootdisk      rootdg        online
c1t1d0s2     auto:slice     rootmirror      rootdg        online
c1t2d0s2     auto:slice     datadisk      datadg        online
c1t3d0s2     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.

e. Run the following commands on both the primary and secondary sites:

vxdg list

A message similar to the following will be displayed:

Copyright © Huawei Technologies Co., Ltd.

```
NAME         STATE           ID
datadg       enabled  997585324.1237.Primary
```

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.

f. Run the following commands to check whether the disk volume status is normal, according to the disk volume information:

vxprint -v

A message similar to the following will be displayed:

```
Disk group: rootdg

TY NAME         ASSOC        KSTATE   LENGTH   PLOFFS   STATE    TUTIL0
PUTIL0
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    TUTIL0
PUTIL0
v  lv_nms_data  datarvg      ENABLED  83886080 -        ACTIVE   -
-
v  srl_vol      datarvg      ENABLED  2097152  SRL      ACTIVE   -
-
```

NOTE

The displayed information varies with the data of the 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.

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**.

g. Run the following command to view the mounting status of the U2000 file system and the Sybase file system.

df -k

A message similar to the following will be displayed:

Copyright © Huawei Technologies Co., Ltd.

```
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/oss
```

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.

h. Run the following commands to check the status of data replication between the primary and secondary sites on the primary site:

vradmin -g *datadg* **repstatus** *datarvg*

A message similar to the following will be displayed:

```
Replicated Data Set: datarvg
Primary:
  Host name:                    10.168.1.10
  RVG name:                     datarvg
  DG name:                      datadg
  RVG state:                    enabled for I/O
  Data volumes:                 1
  VSets:                        0
  SRL name:                     srl_vol
  SRL size:                     1.00 G
  Total secondaries:            1

Secondary:
  Host name:                    10.168.1.11
  RVG name:                     datarvg
  DG name:                      datadg
  Data status:                  consistent, up-to-date
  Replication status:           replicating (connected)
  Current mode:                 asynchronous
  Logging to:                   SRL
  Timestamp Information:        behind by 0h 0m 0s
```

i. Run the following command to check the process of data replication between the primary and secondary sites on the primary site:

vxrlink -g *datadg* **-i 5 status** *datarlk*

Copyright © Huawei Technologies Co., Ltd.

A message similar to the following will be displayed:

```
......
VxVM VVR vxrlink INFO V-5-1-4467 Rlink datarlk is up to date
VxVM VVR vxrlink INFO V-5-1-4467 Rlink datarlk is up to date
VxVM VVR vxrlink INFO V-5-1-4467 Rlink datarlk is up to date
......
```

NOTE

To stop running the command, press the shortcut keys **Ctrl+C**.

- On SUSE Linux:
  a. Log in to the OS as the ossuser user.
  b. Open a CLI. Then, run the following commands to switch to the **root** user:

     $ **su - root**

     Password: *password_of_user_root*

  c. Run the following commands on the primary and secondary sites:

     # df -h

     A message similar to the following will be displayed:

```
Filesystem              kbytes      used      avail         capacity
Mounted on
/dev/sda1               50G  556M   47G   2% /
udev                   7.9G  192K  7.9G   1% /dev
/dev/sda8               20G  174M   19G   1% /export/home
/dev/sda7              119G   25G   88G  23% /opt
/dev/sda5               20G  2.2G   17G  12% /usr
/dev/sda6               20G  315M   19G   2% /var
tmpfs                  8.0G   68K  8.0G   1% /dev/shm
tmpfs                  4.0K     0  4.0K   0% /dev/vx
/dev/vx/dsk/datadg/lvdata
                        99G   32G   62G  34% /opt/sybase/data
```

  d. Run the following commands on the primary and secondary sites:

     # **vxdisk list**

     In the case of two hard disks, a message similar to the following will be displayed:

```
DEVICE       TYPE            DISK         GROUP        STATUS
sda          auto:none       -            -            online invalid
sdb          auto:sliced     disk02       datadg       online
sdc          auto:sliced     disk03       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.

  e. Run the following commands on both the primary and secondary sites:

     # **vxdg list**

     A message similar to the following will be displayed:

```
NAME         STATE           ID
datadg       enabled              1338278125.7.linux
```

     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.

Copyright © Huawei Technologies Co., Ltd.

- 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.

f. Run the following commands to check whether the disk volume status is normal, according to the disk volume information:

vxprint -v

A message similar to the following will be displayed:

```
Disk group: datadg

TY NAME         ASSOC        KSTATE   LENGTH    PLOFFS   STATE    TUTIL0
PUTIL0
v  lv_backup    fsgen        ENABLED  838860800 -        ACTIVE   -
-
v  lvdata       datarvg      ENABLED  213909504 -        ACTIVE   -
-
v  srl          datarvg      ENABLED  213909504 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.

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

g. Run the following command to view the mounting status of the U2000 file system and the Sybase file system.

df -k

A message similar to the following will be displayed:

```
Filesystem           1K-blocks      Used Available Use% Mounted on
/dev/sda1             51613016    569104  48422108   2% /
udev                   8205808       192   8205616   1% /dev
/dev/sda8             20641788    177428  19415720   1% /export/home
/dev/sda7            123860756  25997568  91571336  23% /opt
/dev/sda5             20641788   2234024  17359124  12% /usr
/dev/sda6             20641788    321824  19271324   2% /var
tmpfs                  8388608        68   8388540   1% /dev/shm
tmpfs                        4         0         4   0% /dev/vx
/dev/vx/dsk/datadg/lvdata
                     103212320  33101452  64867988  34% /opt/sybase/data
```

If the file system information is displayed as preceding, it indicates that the mounting status of the U2000 file system and the Sybase file system is normal.

h. Run the following commands to check the status of data replication between the primary and secondary sites on the primary site:

vradmin -g *datadg* **repstatus** *datarvg*

Copyright © Huawei Technologies Co., Ltd.

A message similar to the following will be displayed:

```
Replicated Data Set: datarvg
Primary:
  Host name:                    10.168.1.79
  RVG name:                     datarvg
  DG name:                      datadg
  RVG state:                    enabled for I/O
  Data volumes:                 1
  VSets:                        0
  SRL name:                     srl
  SRL size:                     102.00 G
  Total secondaries:            1

Secondary:
  Host name:                    10.168.1.128
  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
```

i. On the primary site, run the following command to check the process of data replication between the primary and secondary sites on the primary site:

vxrlink -g *datadg* **-i 5 status** *datarlk*

A message similar to the following will be displayed:

```
......
VxVM VVR vxrlink INFO V-5-1-4467 Rlink datarlk is up to date
VxVM VVR vxrlink INFO V-5-1-4467 Rlink datarlk is up to date
VxVM VVR vxrlink INFO V-5-1-4467 Rlink datarlk is up to date
......
```

NOTE

- To stop running the command, press the shortcut keys **Ctrl+C**.
- This command can be run only at the primary site.

----End

Reference Standard

The data replication status is normal in the scenario where the **Table 4-4** standard is complied with.

Table 4-4 Standard data replication status

Command	Item	Standard
vradmin -g *datadg* **repstatus** *datarvg*	Data status	**Data status** is in the **consistent, up-to-date** state.
	Replication status	**Replication status** is in the **replicating (connected)** state.
vxrlink -g *datadg* **-i 5 status** *datarlk*	Output information	The output information is **Rlink datarlk is up to date**.

Copyright © Huawei Technologies Co., Ltd.

Troubleshooting

If the data replication status is abnormal, run the **vxrlink -g** *datadg* **-i 5 status** *datarlk* command and observe the output replication process, and then repair the data replication function according to the actual condition.

- If the terminal displays that the required data remains the same (that is, the number of bytes following **AUTOSYNC** in the screen remains the same), data replication between the primary and secondary sites is abnormal. In this case, check the communication status between the primary and secondary sites such as the bandwidth, stability, and firewall settings, and repair the data replication function in time.
- If the terminal displays that the amount of the required data becomes smaller (that is, the number of bytes following **AUTOSYNC** becomes smaller), the system is synchronizing and restoring data. After **Rlink datarlk is up to date** is displayed in the screen, wait for a period of time (about 30 minutes). During this period of time, if **Rlink datarlk is up to date** is displayed in the screen continuously, data replication between the primary and secondary sites is normal. Otherwise, check the network stability between the primary and secondary sites such as the bandwidth and packet loss, and repair the data replication function in time.

If the fault persists, contact the local Huawei representatives in a timely manner or customer service center to obtain technical support based on the actual maintenance situation.

4.8 Backing Up the U2000 Data

This topic describes how to back up the U2000 data. You can back up the U2000 data to a local or remote server. In this way, the data can be securely and quickly restored when a fault occurs.

Context

- Two modes for backing up the U2000 data are available: immediate backup and timing backup. To reduce the workload for daily maintenance, it is recommended that you adopt the timing backup mode to back up the U2000 data periodically.
- It is recommended that you check the timing backup status weekly and make sure that the timing backup is enabled.
- It is recommended that you clear the data backup files periodically. This prevents the insufficiency of the disk space caused by a large number of backup files.

Procedure

Step 1 Back up the U2000 data on schedule.

For details, see the related contents of automatically backing up U2000 data to the local or remote server in chapter **Backing Up and Restoring the U2000 Database** of the *U2000 Administrator Guide*.

Step 2 Check the periodic backup status to determine whether the periodic backup function of the database is normal.

----End

Copyright © Huawei Technologies Co., Ltd.

Reference Standard

The data backup is normal and the backup file exists in the specified directory.

Troubleshooting

If the database backup fails, do as follows to locate and clear the fault:

- Check whether the database is started. If not, start the database manually.
- Check the disk space of the partition associated with the backup directory.

If the problem persists, contact the local office or customer service center of Huawei according to the warranty.

4.9 Monitoring the Status of the HA System

This topic describes how to check the OS, Veritas monitor, Veritas data volume, Veritas replication, and U2000 status on the primary and secondary sites and whether to perform an active/standby switchover based on the check results.

Prerequisites

The HA system is running properly. The primary and secondary sites are connected.

Context

Data replication status can only be checked on the MSuite of the primary site.

Procedure

Step 1 Log in to the MSuite client.

Step 2 Choose **Deploy** > **Monitor HA Status** from the main menu. The **Monitor the Status** dialog box is displayed.

Step 3 **Optional:** Click **View** to view the historical records of the primary and secondary sites.

NOTE

The status of each HA system indicator is displayed. You can click **detail info** to view details or restoration suggestions.

Step 4 Click **check now** to view the current information about the primary and secondary sites.

NOTE

- It takes three to five minutes to check the HA system status.
- After the check, you can view the check results, details, and suggestions in the **HA Status** dialog box.
- The check results are saved as **.xml** files in **/opt/oss/engr/engineering/ha_review/result**. The name of the latest check result file contains the word **new**. For example, *ha_review_result_20150421165146.xml*. In this example, *20150421165146* indicates the time when the HA system status is checked). You can run the following commands to check the file information:

  ```
  # cd /opt/oss/engr/engineering/ha_review/result
  # cat ha_review_result_20150421165146.xml
  ```

Step 5 **Optional:** Click **Switch to Secondary** to switch to the secondary site, if the queried result of the primary site is abnormal.

Copyright © Huawei Technologies Co., Ltd.

NOTE

- You are advised to perform an active/standby switchover when the primary and secondary sites are running properly.
- When the HA system status is abnormal, you can click **Yes** in the **Prompt** dialog box to forcibly perform an active/standby switchover.

----End

Copyright © Huawei Technologies Co., Ltd.

5 Weekly Maintenance

About This Chapter

This topic describes how to perform weekly maintenance. Weekly maintenance allows you to find defects such as function failure or performance degradation during the running of the U2000 in a timely manner. This helps you to take proper measures to handle the problem as soon as possible and eliminate potential risks and avoid accidents.

5.1 Checking the Disk Space of the U2000 Server
This topic describes how to check the disk space of the U2000 server. If the disk space usage exceeds 80%, the running efficiency of the U2000 may be affected, or the server may not be started. Therefore, you must periodically check the disk space and clear the space in a timely manner.

5.2 Checking the Logs of the OS
This topic describes how to check the running status of the OS by the related log information.

5.3 Checking the Logs of the SQL Server Database
This topic describes how to check the logs of SQL server database.

5.4 Checking the Logs of the Sybase Database
This topic describes how to check the logs of the Sybase database.

5.5 Checking Operation Logs Associated with Project Deployment
This topic describes how to check operation logs associated with project deployment, excluding query operations, to determine whether the environment is normal. The operation logs include the U2000 installation, upgrade, patch installation, and MSuite deployment.

5.6 Checking the Running Status of Anti-Virus Software
This topic describes how to check the running status of antivirus software. You must install OS patches in time, upgrade the antivirus software, and search for viruses to prevent the server and computer from affecting network viruses and to ensure the normal running of the U2000.

5.7 Checking the Database Status
This topic describes how to check the database status. If the database capacity exceeds the standard value, the U2000 cannot be used. Therefore, you must check the database status periodically to ensure the normal running of the U2000.

5.8 Checking the Backing Up the U2000 Data

Copyright © Huawei Technologies Co., Ltd.

This topic describes how to back up the U2000 data. You can back up the U2000 data to a local or remote server. In this way, the data can be securely and quickly restored when a fault occurs.

Copyright © Huawei Technologies Co., Ltd.

5.1 Checking the Disk Space of the U2000 Server

This topic describes how to check the disk space of the U2000 server. If the disk space usage exceeds 80%, the running efficiency of the U2000 may be affected, or the server may not be started. Therefore, you must periodically check the disk space and clear the space in a timely manner.

Context

NOTE

If the U2000 uses a high availability system, you must check the disk space of the U2000 server on both the primary and secondary sites.

Procedure

- Perform the following steps on Windows:

  View the disk space of the server on the U2000 System Monitor client or in the **My Computer** window. The information to be viewed includes the disk space usage of the OS, SQL server, and U2000.

- Perform the following steps in a Single-Server System (SUSE Linux), Single-Server System (Solaris) and High Availability System:

  You can view the disk space of the server on the U2000 System Monitor client or by using command lines. The following describes how to view the disk space by running commands:

  a. Log in to the OS as the ossuser user.

  b. Open a CLI. Then, run the following commands to switch to the **root** user:

     `$` **su**

     `Password:` *password_of_user_root*

  c. Run the following command to view the disk space usage on the server:

     `#` **df -h**

----End

Reference Standard

Generally, the space usage of each disk should be less than 80%.

Troubleshooting

If the disk space exceeds the standard value, you must clear the space in time. For details, see **6.8 Releasing the Disk Space of the U2000 Server**.

5.2 Checking the Logs of the OS

This topic describes how to check the running status of the OS by the related log information.

Copyright © Huawei Technologies Co., Ltd.

Procedure

- Perform the following steps on Windows:
  a. Choose **Start** > **Control Panel** > **Administrative Tools** > **Event Viewer**.
  b. In the window that is displayed, view the log and event information and check whether the information about the abnormal events that affect system running exists.

     NOTE

     For the method of using the Event Browser, refer to the OS Help or the user manuals.
- Perform the following steps in a Single-Server System (SUSE Linux), Single-Server System (Solaris) and High Availability System:
  a. Log in to the operating system as the ossuser user.
  b. Open a CLI. Then, run the following commands to switch to the **root** user:

     $ **su**

     Password: *password_of_user_root*
  c. Run the following command to navigate to the path where the log file is saved:
     - In a : # **cd /var/log**
     - In a Single-Server System (Solaris) or High Availability System: # **cd /var/adm**
  d. Run the following command to quickly search for error information:

     # **grep error messages***

     # **grep warn messages***

     # **grep panic messages***

     If there is no error information, no information is displayed in the command output.

     If there is error information, all error information contained in the file is displayed in the command output.

     NOTE

     On Solaris, you can also run the **fmadm** command to view hardware diagnosis information. Run the following command:

     # **fmadm faulty**

----End

Reference Standard

- On Windows:

  The **Error** information is not displayed in **Event Viewer**.
- In a Single-Server System (SUSE Linux), Single-Server System (Solaris) and High Availability System:

  The **error** information is not contained in the log file of the OS.

  NOTE

  Run the following command to view all OS log files, namely, files whose names start with **messages** (including error logs and non-error logs):

  # **more messages***

Copyright © Huawei Technologies Co., Ltd.

Troubleshooting

If a fault occurs, rectify it according to the error information contained in the log file. If the problem still persists, contact technical support engineers of Huawei.

5.3 Checking the Logs of the SQL Server Database

This topic describes how to check the logs of SQL server database.

Procedure

SQL Server 2008

Check the database running log files in **C:\MSDATA\MSSQL10.MSSQLSERVER\MSSQL\Log**.

Reference Standard

The log file does not contain error information that affects service operation.

Troubleshooting

Fix the system according to the error information contained in the log files. If the problem still persists, contact technical support engineers of Huawei.

5.4 Checking the Logs of the Sybase Database

This topic describes how to check the logs of the Sybase database.

Procedure

Step 1 Log in to the OS as the ossuser user.

Step 2 Open a CLI. Then, run the following commands to switch to the **root** user:

$ **su**

Password: *password_of_user_root*

Step 3 Run the following command to switch to the path where the log files reside:

cd /opt/sybase/ASE*/install

Step 4 Run the following commands to view the logs of the database:

more DBSVR.log

more DBSVR_back.log

----End

Reference Standard

No error information is contained in the file.

Copyright © Huawei Technologies Co., Ltd.

NOTE

Run the following command to quickly search for error information:

grep error DBSVR.log

grep error DBSVR_back.log

If there is no error information, no information is displayed in the command output.

If there is error information, all error information contained in the file is displayed in the command output.

Troubleshooting

Fix the system according to the error information contained in the log files. If the problem still persists, contact technical support engineers of Huawei.

5.5 Checking Operation Logs Associated with Project Deployment

This topic describes how to check operation logs associated with project deployment, excluding query operations, to determine whether the environment is normal. The operation logs include the U2000 installation, upgrade, patch installation, and MSuite deployment.

Procedure

- Perform the following steps on Single-Server System (Windows):
  a. Choose **Start** > **Control Panel** > **Administrative Tools** > **Event Viewer**.
  b. In the window that is displayed, click **application program** to check whether abnormal operation logs associated with project deployment affect system operation.

     NOTE

     For the method of using the Event Browser, refer to the OS Help or the user manuals.
- Perform the following steps in a Single-Server System (SUSE Linux) and High Availability System (SUSE Linux):
  a. Log in to the operating system as the ossuser user.
  b. Open a CLI. Then, run the following commands to switch to the **root** user:

     $ **su**

     `Password:` *password_of_user_root*
  c. Run the following command to check operation logs associated with project deployment, excluding query operations:

     # **vi /var/log/localmessages**
- In a Single-Server System (Solaris) and High Availability System (Solaris):
  a. Log in to the operating system as the ossuser user.
  b. Open a CLI. Then, run the following commands to switch to the **root** user:

     $ **su**

     `Password:` *password_of_user_root*
  c. Run the following command to check operation logs associated with project deployment, excluding query operations:

Copyright © Huawei Technologies Co., Ltd.

vi /var/adm/localmessages

----End

Reference Standard

- In a Single-Server System (Windows):

  The **Error** information is not displayed in **Event Viewer**.
- In a Single-Server System (SUSE Linux), Single-Server System (Solaris) and High Availability System:

  The **error** information is not contained in the log file of the **localmessages** file.

Troubleshooting

If a fault occurs, rectify it according to the error information contained in the log file. If the problem still persists, contact technical support engineers of Huawei.

5.6 Checking the Running Status of Anti-Virus Software

This topic describes how to check the running status of antivirus software. You must install OS patches in time, upgrade the antivirus software, and search for viruses to prevent the server and computer from affecting network viruses and to ensure the normal running of the U2000.

Procedure

1. Install OS patches in time.
2. Upgrade antivirus software and upgrades the virus patterns.

   Upgrade antivirus software in time.

   To ensure the stability and security of the NMS system services, it is recommended that you manually update the virus patterns every week. The procedure is as follows:
   - Select a special operation and maintenance terminal (installed with the anti-virus software). This terminal is installed with two network adapters, one for connection with the intranet and the other for connection with Internet.
   - Disconnect the operation and maintenance terminal with the intranet and connect it to the Internet to obtain the latest virus patterns from the Trend website.
   - Disconnect the terminal from Internet, connect it to the intranet, and then upload the latest virus patterns to the OfficeScan server.
   - Double-click the virus patterns on the OfficeScan server to upgrade them. Then, the server automatically upgrades the global OfficeScan client according to the setting.
3. Periodically search for viruses.

   a. Log in to the Web console of the OfficeScan.

   b. Choose **Networked Computers** > **Client Management** > **Settings** > **Privileges and Other Settings**.

   c. In the displayed **Privileges and Other Settings** dialog box, click the **Privileges** tab and select **Configure Real-time Scan settings**, click **Apply to All Clients** to start the real-time scan function on all clients.

Copyright © Huawei Technologies Co., Ltd.

Reference Standard

No virus is found.

Troubleshooting

If any virus is found, clear it at once. If the problem still persists, contact technical support engineers of Huawei.

5.7 Checking the Database Status

This topic describes how to check the database status. If the database capacity exceeds the standard value, the U2000 cannot be used. Therefore, you must check the database status periodically to ensure the normal running of the U2000.

Context

When the database utilization of the system exceeds the preset alarm threshold, the sysmonitor server sends an alarm to the U2000 server. Meanwhile, the related record in the sysmonitor client turns red.

Procedure

Step 1 Log in to the U2000 System Monitor client.

Step 2 Click the **Database Monitor** tab. Details about all manageable databases are displayed in a list.

Step 3 Select a database in the list, right-click, and choose **Refresh** from the shortcut menu to refresh all information about the selected database.

----End

Reference Standard

The databases are running properly. The ratio of the used data space to the total data space for each database is less than 85%.

Troubleshooting

If the log space of a database exceeds the standard value, dump the logs and clear the space in time. For details, see the associated contents in chapter **Backing Up and Restoring the U2000 Database** of the *U2000 Administrator Guide*.

5.8 Checking the Backing Up the U2000 Data

This topic describes how to back up the U2000 data. You can back up the U2000 data to a local or remote server. In this way, the data can be securely and quickly restored when a fault occurs.

Copyright © Huawei Technologies Co., Ltd.

Context

- Two modes for backing up the U2000 data are available: immediate backup and timing backup. To reduce the workload for daily maintenance, it is recommended that you adopt the timing backup mode to back up the U2000 data periodically.
- It is recommended that you check the timing backup status weekly and make sure that the timing backup is enabled.
- It is recommended that you clear the data backup files periodically. This prevents the insufficiency of the disk space caused by a large number of backup files.
- Regularly move the to-be-backed up database data to a third-party storage medium so that the database data can still be accessed even when the hard disk is damaged.

Procedure

Step 1 Back up the U2000 data on schedule.

For details, see the related contents of automatically backing up U2000 data to the local or remote server in chapter **Backing Up and Restoring the U2000 Database** of the *U2000 Administrator Guide*.

Step 2 Check the periodic backup status to determine whether the periodic backup function of the database is normal.

----End

Reference Standard

The data backup is normal and the backup file exists in the specified directory.

Troubleshooting

If the database backup fails, do as follows to locate and clear the fault:

- Check whether the database is started. If not, start the database manually.
- Check the disk space of the partition associated with the backup directory.

If the problem persists, contact the local office or customer service center of Huawei according to the warranty.

Copyright © Huawei Technologies Co., Ltd.

6 Monthly Maintenance

About This Chapter

This topic describes how to perform monthly maintenance. Monthly maintenance keeps the U2000 health in a good state for a long time, which ensures secure, stable and reliable running of the system.

6.1 Checking User Configurations
This topic describes how to check user configurations and authority configuration of the U2000.

6.2 Checking the DCN Bandwidth Between the Primary and Secondary Sites in a High Availability System
In a high availability system, if the DCN bandwidth between the primary and secondary sites is insufficient or unstable, various issues may occur. You need to use a network bandwidth check tool to regularly check the bandwidth between the primary and secondary sites.

6.3 Backing Up System Files
This topic describes how to regularly back up system files to restore system data in case of system breakdown.

6.4 Viewing Alarm Statistics
This topic describes how to collect and view statistics about alarms generated within the latest month.

6.5 Checking the Server Time of the U2000
This topic describes how to check whether the server time of the U2000 is correct.

6.6 Changing the Password of the Current User
This topic describes how to change the password of your account. It is recommended that you change the password periodically to improve the password security of your account.

6.7 Checking U2000 Directories
The directories automatically generated after the U2000 server software is installed cannot be deleted at random. Regularly check whether contents in all the U2000 directories are complete.

6.8 Releasing the Disk Space of the U2000 Server
This topic describes how to clear the disk space of the U2000 server to save resources.

Copyright © Huawei Technologies Co., Ltd.

6.1 Checking User Configurations

This topic describes how to check user configurations and authority configuration of the U2000.

Procedure

Step 1 Log in to the U2000 as the **admin** user.

Step 2 Choose **Administration** > **NMS Security** > **NMS User Management** from the main menu.

Step 3 In the **NMS User Management** window, choose **Users** from the navigation tree and then select a user node to view user configurations in the right pane.

----End

Reference Standard

No irrelevant user exists. The operation rights have been set properly. The password validity has been set.

Troubleshooting

- Assign user rights strictly according to the user group and operation set. Divide users with the same rights to a group, and avoid assigning rights to a single user. This reduces impacts on the U2000 performance.
- Delete users who no longer use equipment in time. Assign rights to users who maintain new equipment.
- Changing the password within a maximum of three months is recommended.

6.2 Checking the DCN Bandwidth Between the Primary and Secondary Sites in a High Availability System

In a high availability system, if the DCN bandwidth between the primary and secondary sites is insufficient or unstable, various issues may occur. You need to use a network bandwidth check tool to regularly check the bandwidth between the primary and secondary sites.

Procedure

Step 1 Select a commonly used network bandwidth check tool, such as IxChariot, to check the bandwidth between the primary and secondary sites on a regular basis.

Step 2 Ensure that the DCN bandwidth between the primary and secondary sites meets the planning requirement. For details about planning requirements, see **Network Parameter Planning for the NM Server** > **Bandwidth Planning** in *U2000 Planning Guide*.

----End

Copyright © Huawei Technologies Co., Ltd.

6.3 Backing Up System Files

This topic describes how to regularly back up system files to restore system data in case of system breakdown.

Procedure

- Perform the following steps to back up system files in a Single-Server System (Windows):

  NOTE

  Before the back up system files, make sure the system does not use file backup directory.

  a. Log in to the Windows OS as a user with the administrator rights.

  b. Back up the entire U2000 program directory, such as **D:\oss** and **D:\oss\engr**.

  c. Back up the entire SQL Server database program directory, including the database running files in the SQL Server installation directory and the sqlserver dynamic link library (DLL) files in the **C:\WINDOWS\system32** path.

  d. Back up the registry files.

  Click **Start** > **Run** and enter **regedit**. In the window that is displayed, choose **File** > **Export**.

- Perform the following steps to back up system files in a Single-Server System (Solaris) and High Availability System (Solaris):

  a. Log in to the OS as the **ossuser** user.

  b. Open a CLI. Then, run the following commands to switch to user **root**:

  > **su**

  `Password:` *password_of_user_root*

  c. Run the following commands to compress and save OS files to a directory with sufficient space (for example, /opt) and manually move them to a special storage device for backup:

  cd /opt

  tar cvf *backup1.tar* **/opt/oss/engr**

  tar cvf *backup2.tar* **/opt/oss**

  tar cvf *backup3.tar* **/opt/sybase**

  NOTE

  - Here, *backup1.tar*, *backup2.tar*, and *backup3.tar* are the names of compressed files. You can modify the names as required.
  - The size of compressed files increases along with the volume of data on the live network. Backing up data based on site conditions is recommended.
  - To ensure data security, dump the compressed files to another disk.

- Perform the following steps to back up system files in a Single-Server System (SUSE Linux) and High Availability System (SUSE Linux):

  a. Log in to the OS as the **ossuser**.

  b. Open a CLI. Then, run the following commands to switch to the **root** user:

  > **su**

Copyright © Huawei Technologies Co., Ltd.

`Password:` *password_of_user_root*

c. Run the following commands to compress and save OS files to a directory with sufficient space (for example, /opt) and manually move them to a special storage device for backup:

cd /opt

tar cvf *backup1.tar* **/opt/oss/engr**

tar cvf *backup2.tar* **/opt/oss**

tar cvf *backup3.tar* **/opt/sybase**

NOTE

- Here, *backup1.tar*, *backup2.tar*, and *backup3.tar* are the names of compressed files. You can modify the names as required.
- The size of compressed files increases along with the volume of data on the live network. Backing up data based on site conditions is recommended.
- To ensure data security, dump the compressed files to another disk.

----End

6.4 Viewing Alarm Statistics

This topic describes how to collect and view statistics about alarms generated within the latest month.

Procedure

Step 1 Log in to a U2000 client.

Step 2 Choose **Fault** > **Query Alarm Log Statistics** from the main menu (traditional style); alternatively, double-click **Fault Management** in **Application Center** and choose **Browse Alarm** > **Alarm Log Statistics** from the main menu (application style).

Step 3 In the **Statistic Filter** dialog box, set **Statistic Row** to **By month**. In the **Occurrence Time Segment** area on the **Basic Setting** tab page, set the associated parameters, and then click **OK**.

The alarm statistics are displayed in the **Query Alarm Log Statistics** window.

Step 4 Click the buttons at the bottom of the **Query Alarm Log Statistics** window to perform the associated operations. Details are as follows:

- Click **Template** to new, open, or save an alarm statistical template.
- Click **Statistic Filter** to set the statistical condition.
- Click **Refresh** to collect statistics on alarms again based on the current statistical condition.
- Click **Save As** to save the statistical result as a file.
- Click **Print** to print the statistical result in a specified medium.

----End

6.5 Checking the Server Time of the U2000

This topic describes how to check whether the server time of the U2000 is correct.

Copyright © Huawei Technologies Co., Ltd.

Procedure

- Perform the following steps on Windows:
  a. Open the **Control Panel** window. Then, double-click the **Data/Time** icon.
  b. In the dialog box that is displayed, click the **Data&Time** tab, and then check the system time.
- Perform the following steps in a Single-Server System (SUSE Linux), Single-Server System (Solaris) and High Availability System:
  a. Log in to the OS as the ossuser user.
  b. Open a CLI. Then, run the following commands to switch to the **root** user:

     `$ su`

     `Password:` *password_of_user_root*
  c. Run the following command to view the current server time:

     `#` **date**

----End

Reference Standard

The server time is correct.

Troubleshooting

1. Correct the server time. For details, see section **Setting the System Time and Time Zone** in the administrator guide.
2. Check the running status of the NTP service. If the NTP service is abnormal, reconfigure the NTP service. For details, see the chapter **Configuring System NTP Solutions** of the commissioning guide.

6.6 Changing the Password of the Current User

This topic describes how to change the password of your account. It is recommended that you change the password periodically to improve the password security of your account.

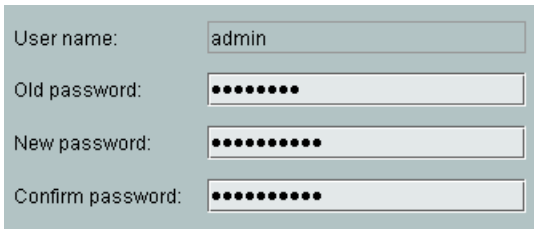
Context

- The new password must comply with the password policy. For details on how to set the password policy, see Setting Password Policies.
- The password of the admin user cannot be restored after being changed. Therefore, keep the password of the admin user secure.

Procedure

Step 1 Choose **File** > **Change Password** from the main menu (traditional style); alternatively, double-click **Security Management** in **Application Center** and choose **OSS Security** > **Change Password** from the main menu (application style).

Copyright © Huawei Technologies Co., Ltd.



Step 2 In the **Change Password** dialog box, set the new password for the current user and click **OK**.

Step 3 In the **Confirm** dialog box, click **Yes**.

----End

6.7 Checking U2000 Directories

The directories automatically generated after the U2000 server software is installed cannot be deleted at random. Regularly check whether contents in all the U2000 directories are complete.

Context

After the U2000 server software is installed, the U2000 directories will be generated automatically. Do not delete these directories at random; otherwise, the U2000 server software cannot be used properly.

Procedure

- Windows OS
  a. Log in to the operating system as the **administrator** user.
  b. Double-click **Computer** and check whether contents in the U2000 directories generated after the U2000 is installed are available.
     - D:\oss
     - D:\oss\engr
     - D:\oss\OSSJRE
- Solaris OS
  a. Log in to the OS as the **root** user.
  b. Use the **cd** and **ls** commands to check whether contents in the U2000 directories generated after the U2000 is installed are complete.
     - /opt/oss/engr
     - /opt/oss
     - /opt/sybase
     - /opt/install/OSSICMR
     - /opt/oss/OSSJRE
     - /etc/ICMR
     - /var/ICMR

     The following uses the **/opt/oss** directory as an example. Run the following commands to check whether the contents in the **/opt/oss** directory are complete:

Copyright © Huawei Technologies Co., Ltd.

cd /opt

ls

Check whether the command output contains the **oss**. If so, contents in the **/opt/oss** are complete.

- SUSE Linux OS
  a. Log in to the OS as the **root** user.
  b. Use the **cd** and **ls** commands to check whether contents in the U2000 directories generated after the U2000 is installed are complete.
     - /opt/oss/engr
     - /opt/oss
     - /opt/sybase
     - /opt/install/OSSICMR
     - /opt/oss/OSSJRE
     - /etc/ICMR
     - /var/ICMR

     The following uses the **/opt/oss** directory as an example. Run the following commands to check whether the contents in the **/opt/oss** directory are complete:

     # **cd /opt**

     # **ls**

     Check whether the command output contains the **oss**. If so, contents in the **/opt/oss** are complete.

----End

6.8 Releasing the Disk Space of the U2000 Server

This topic describes how to clear the disk space of the U2000 server to save resources.

Prerequisites

NOTICE

Make sure all files to be deleted are useless. Do not delete files generated in the recent three days.

Procedure

- Perform the following steps on Windows:
  a. Log in to the Windows OS as a user with the administrator rights.
  b. Delete the useless and outdated alarm log files that are automatically dumped. The default directory is **%IMAP_ROOT%\dump**.

Copyright © Huawei Technologies Co., Ltd.

NOTE

You can compare the creation time and the modification time of a file with the current system time. If a file was created a long time ago and has not been used for a long time, it can be concluded that the file is outdated.

c. Delete the useless and outdated abnormal event log files that are automatically dumped. The default directory is **%IMAP_ROOT%\dump**.

d. Delete useless and outdated performance dump files. The default directory is **%IMAP_ROOT%\var\dump**.

e. Delete the useless and outdated database backup files. The default directory is **%IMAP_ROOT%**.

f. Delete the outdated and useless running log files. The default directory is **%IMAP_ROOT%\log**.

g. Delete other outdated and unnecessary files, such as the program installation files and patch installation files of earlier versions.

- Do as follows in the Single-Server System (SUSE Linux), Single-Server System (Solaris) and High Availability System:

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

b. Delete the useless and outdated alarm log files that are automatically dumped. The default directory is **$IMAP_ROOT$/dump**.

c. Delete useless and outdated performance dump files. The default directory is **$IMAP_ROOT$/dump**.

d. Delete the useless and outdated abnormal event log files that are automatically dumped. The default directory is **$IMAP_ROOT$/var/dump**.

e. Delete the useless and outdated database backup files. The default directory is **$IMAP_ROOT$/var/backup**.

f. Delete the outdated and unnecessary running log files. The default directory is **$IMAP_ROOT$/log**.

g. Delete other outdated and unnecessary files, such as the application installation files and patch installation files of earlier versions.

----End

Copyright © Huawei Technologies Co., Ltd.

7 Quarterly Maintenance

About This Chapter

This topic describes how to perform quarterly maintenance. Quarterly maintenance keeps the equipment room environment of the U2000 in good condition, which ensures the reliability of power supply and related hardware.

7.1 Checking the Disk Status of the U2000 Server
This topic describes how to check the disk status of the U2000 server. If the disk status is abnormal, the data may be lost and the U2000 cannot be properly used. Therefore, you must check the disk status periodically. If any disk fault occurs, clear the fault or replace the disk in time.

7.2 Checking the Equipment Room Environment
This topic describes how to check the environment of the equipment room.

7.3 Checking the Power Supply of the U2000 Server
This topic describes how to check whether the power supply of the U2000 server is normal.

7.4 Checking Hardware and Peripherals of the U2000 Server
This topic describes how to check the status of hardware and peripherals of the U2000 server.

7.5 Check whether the U2000 license is expired
If the U2000 license expires, usage of U2000 functions will be affected. Applying for a new license from Huawei before the U2000 license expires is recommended.

7.6 Checking Maintenance Information
Pay attention to the maintenance information about the third-party software and hardware and the U2000, especially the milestone dates in the product lifecycle. The maintenance information ensures normal usage of services and applications.

Copyright © Huawei Technologies Co., Ltd.

7.1 Checking the Disk Status of the U2000 Server

This topic describes how to check the disk status of the U2000 server. If the disk status is abnormal, the data may be lost and the U2000 cannot be properly used. Therefore, you must check the disk status periodically. If any disk fault occurs, clear the fault or replace the disk in time.

Procedure

- Perform the following steps in a Single-Server System (Solaris):
  a. Log in to the OS as the ossuser user.
  b. Open a CLI. Then, run the following commands to switch to the **root** user:

     $ **su**

     Password: *password_of_user_root*
  c. Run the following commands to view the physical status of the disk on the current server:

     # **iostat -E**

     The following information is displayed:

```
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
```

     NOTE

     On a Single-Server System (Solaris), after you run the **iostat -E** command, if the **Hard Errors** of the disk is **0**, the physical status of the disk is normal.
- Perform the following steps in a Single-Server System (SUSE Linux):
  a. Log in to the OS as the ossuser user.
  b. Open a CLI. Then, run the following commands to switch to the **root** user:

     $ **su**

     Password: *password_of_user_root*
  c. Run the following commands to view the physical status of the disk on the current server:

     # **iostat -k**

     The following information is displayed:

```
Linux 2.6.16.60-0.85.1-smp (linux)      01/30/12

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           0.01    0.00    0.01    0.00    0.00   99.97

Device:            tps    kB_read/s    kB_wrtn/s    kB_read    kB_wrtn
sda               0.86         3.86        67.23     327919    5716356
sdb               0.00         0.09         0.00       7486        188
```

     NOTE

     On a Single-Server System (SUSE Linux), after you run the **iostat -k** command, the disk capacity is displayed in the Device column in the command output. If a disk volume becomes faulty, Device information cannot be displayed.

Copyright © Huawei Technologies Co., Ltd.

- Perform the following steps in a High Availability System:
  a. Log in to the OS as the ossuser user.
  b. Open a CLI. Then, run the following commands to switch to the **root** user:

     $ **su**

     Password: *password_of_user_root*

  c. Run the following commands on the master server of the primary and secondary sites:

     # **vxdisk list**

     The following information is displayed:

     ```
     DEVICE TYPE DISK GROUP STATUS
     c1t0d0s2 auto:sliced rootdisk datadg online
     c1t1d0s2 auto:sliced rootmirror 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. The displayed number of columns is consistent with the number of disks.
     - On a High Availability System, after you run the **vxdisk list** command, the disk is in the **online** state.
- Perform the following steps in a Single-Server System (Windows):

  NOTE

  Ensure that the disk is not used by the system before the check is performed. The U2000 and other processes using this disk must be stopped.

  a. In the **My Computer** window, select a disk, right-click, and then choose **Attribute** from the shortcut menu.
  b. In the dialog box that is displayed, click the **Tools** tab.
  c. In the **Check Error** area, click **Start Check**.
  d. In the dialog box that is displayed, select **Automatically fix file system errors** items and click **Start**. Then, check the disk status as prompted.

     NOTE

     On a Single-Server System (Windows), the associated message is displayed after the disk check is complete.

----End

Reference Standard

If the following standards are met, the disk status is normal:

- On a Single-Server System (Windows), the associated message is displayed after the disk check is complete.
- On a Single-Server System (Solaris), after you run the **iostat -E** command, if the **Hard Errors** of the disk is **0**, the physical status of the disk is normal.
- On a Single-Server System (SUSE Linux), after you run the **iostat -k** command, the disk capacity is displayed in the Device column in the command output. If a disk volume becomes faulty, Device information cannot be displayed.
- On a High Availability System, after you run the **vxdisk list** command, the disk is in the **online** state.

Copyright © Huawei Technologies Co., Ltd.

Troubleshooting

If a disk does not function properly, contact the equipment supplier to repair or replace the disk in a timely manner.

7.2 Checking the Equipment Room Environment

This topic describes how to check the environment of the equipment room.

Procedure

Step 1 Check the temperature, humidity, and dust-proof conditions of the equipment room.

Step 2 Check the power supply system, air filter, fire alarm system, and lightning proof system.

----End

Reference Standard

Item	Index
Temperature	Range: 15°C-35°C
Humidity	Range: 40%-65%
Dust condition	Clear and spotless
Power supply	The power supply is normal, which ensures the normal running of the equipment in the equipment room.
Air filter	The air filter is clean and the cabinet is in good ventilation condition.
Fire alarm system	The fire alarm system works properly and can effectively sense fire accidents.
Lightning proof system	The lightning proof system works properly and can effectively prevent the lightning stroke.

Troubleshooting

1. Adjust the temperature and humidity properly. Make sure that the doors and windows are airtight.
2. Remove the air filter from the cabinet, remove the dusts on the air filter with the vacuum cleaner, and then place the air filter in the cabinet.
3. Repair the power supply system, fire alarm system, and lightning proof system to ensure that the equipment in the equipment room works properly and securely.

7.3 Checking the Power Supply of the U2000 Server

This topic describes how to check whether the power supply of the U2000 server is normal.

Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The U2000 server must be powered on.

Procedure

Step 1 Check whether the power indicators of the server and monitor are normal.

Step 2 If the server is configured with devices such as disk array and storage device, check the power indicators of these devices.

Step 3 Check the external power of the system, configuring an independent uninterrupted power supply (UPS) for the U2000 server is recommended. This can avoid some serious problems such as hardware damage, system restoration failure, and data loss caused by abnormal power failure.

Step 4 View the power supply failure information in system logs. Confirm that the power supply of the server is normal.

- On Solaris:

  Run the following commands to view information about the power supply faults in the logs recorded in recent days:

  # **more /var/adm/messages | grep PSU**

  # **prtdiag -v**

  Information similar to the following is displayed:

  ```
  Jun 23 16:53:40 U2000Server rmclomv: [ID 632913 kern.error] Input power
  unavailable for PSU @ PS1.
  ```

  If **error** or **WARN** is contained in the command output, the power supply is in the abnormal state.

  NOTE

  The preceding method can be used to check the power supply information about the V series servers (such as the V240 server). The method for M series servers (such as the M4000 and M5000 servers) is different from that for the V series servers. For details, see the document delivered with the server.

- On SUSE Linux:

  Run the following commands to view information about the power supply faults in the logs recorded in recent days:

  # **more /var/log/messages | grep PSU**

  # **more /var/log/warn | grep PSU**

  Information similar to the following is displayed:

  ```
  Jun 23 16:53:40 U2000Server rmclomv: [ID 632913 kern.error] Input power
  unavailable for PSU @ PS1.
  ```

  If **error** or **WARN** is contained in the command output, the power supply is in the abnormal state.

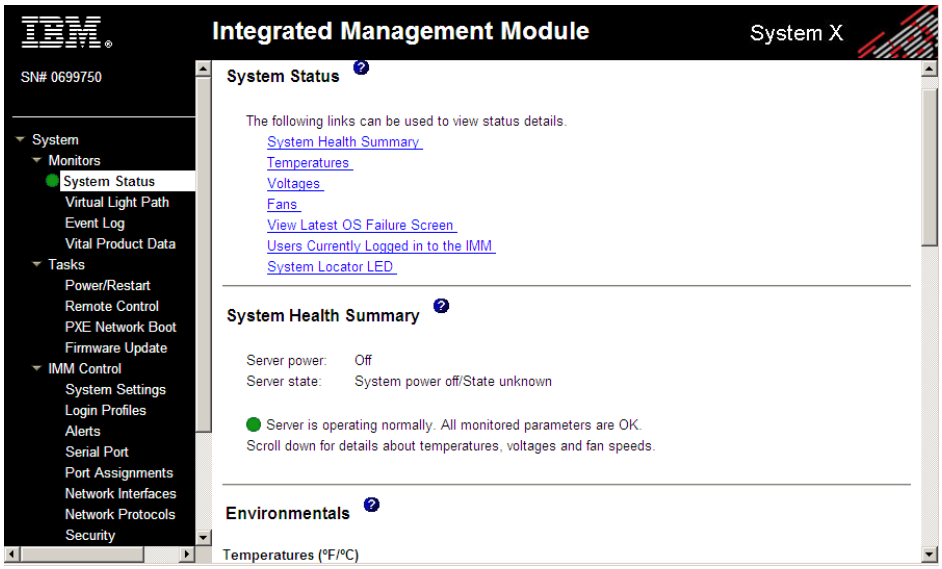
- On Windows:

  a. Enter the default IMM IP address on the Internet Explorer of the PC to access the IMM Web management page.

  b. Click **Continue** to access the **Integrated Management Module** web page.

Copyright © Huawei Technologies Co., Ltd.

Figure 7-1 Integrated Management Module web page



NOTE

You do not need to set **Inactive session timeout value**. Keep the default value **no timeout**.

c. Choose **System Status** from the navigation tree. The information such as the power supply status, temperature, and fan is displayed. Determine whether the system is running properly by comparing the reference value and current value of **View Thresholds**.

----End

Reference Standard

In normal cases, all the power indicators of the server peripherals turn green and all fault indicators are off.

Troubleshooting

If a fault about the external power of the system occurs, the system does not record the related information. In this case, you must detect the external power supply and circuits in other methods. For details, refer to the delivery manual of the server. If you encounter complicated problems, contact the manufacturer to repair or replace the server.

7.4 Checking Hardware and Peripherals of the U2000 Server

This topic describes how to check the status of hardware and peripherals of the U2000 server.

Prerequisites

The U2000 server is powered on.

Copyright © Huawei Technologies Co., Ltd.

Procedure

Step 1 Refer to the delivery manual of the server according to the server model to check the hardware of the server. For example, hard disk, power, and fan.

Step 2 If a disk array is used, refer to the related manual of the disk array according to the disk array model to check the hardware of the server.

NOTICE

Check the battery charge of the disk array on a regular basis and ensure that the batter is fully charged.

Step 3 Check whether the CD/DVD-ROM runs properly.

----End

Reference Standard

In normal cases, the server and peripherals run properly and all indicators work properly. For example, if the hard disk drive indicator is steady on, the drive is being used.

Troubleshooting

Refer to the delivery manual according to the models of the server and peripherals to locate faults. If you encounter complicated problems, contact the manufacturer to repair or replace the server.

7.5 Check whether the U2000 license is expired

If the U2000 license expires, usage of U2000 functions will be affected. Applying for a new license from Huawei before the U2000 license expires is recommended.

Prerequisites

The U2000 client can be logged in to properly.

Context

There are different types U2000 licenses, such as the commissioning license, temporary license for commercial use, and permanent license for commercial use. Only permanent licenses for commercial use can be permanently used in the product lifecycle. The validity periods for other types of licenses are limited and vary according to the license type.

The U2000 license status may be abnormal in the following conditions and the U2000 functions may become abnormal:

- The number of load items exceeds the license threshold.
- The license is expired.
- The ESN is incorrect.

Copyright © Huawei Technologies Co., Ltd.

Regularly perform the following operations to check whether the U2000 license status is normal and apply for a new U2000 license file from Huawei in time:

Procedure

Step 1 Log in to the U2000 Client.

Step 2 Choose **Help** > **License Management** > **License Information**.

Step 3 In the **License Information** dialog box that is displayed to view the condition of the license.

Focus on whether the number of loaded items exceeds the U2000 license threshold and whether the U2000 license validity period is expired.

----End

Reference Standards

Check whether the U2000 license is expired. If the U2000 license is expired, apply for a new U2000 license from Huawei to ensure normal usage of U2000 functions.

For details about how to apply for a U2000 license, see *U2000 Administrator Guide*.

7.6 Checking Maintenance Information

Pay attention to the maintenance information about the third-party software and hardware and the U2000, especially the milestone dates in the product lifecycle. The maintenance information ensures normal usage of services and applications.

Procedure

- Check the milestone dates for third-party software and hardware, for example, EOFS and EOS.

  NOTE

  For third-party software and hardware maintenance information, go to the official website of the vendor or dial up the after-sales phone number for help.

- Check the milestone time points for the U2000 software lifecycle, for example, EOFS and EOS.

  EOFS: deadline for Huawei to provide customer software versions with patch development services. During the period from EOFS to EOS, Huawei does not develop patches for any new online problems and still supports uploading of released patches.

  EOS: deadline for stopping locating version problems. From the EOS date on, Huawei does not provide any services (including hot line phone services) for the product. During one year from the EOS date on, you can visit http://support.huawei.com to query or download FAQs related to the product and known issue cases.

----End

Result

Upgrading software and hardware to the latest version is recommended. You can communicate with the manufacturer about the software and hardware versions to be replaced.

Copyright © Huawei Technologies Co., Ltd.

A Glossary and Abbreviations

A

access control list	A list of entities, together with their access rights, which are authorized to have access to a resource.
access control right	The level of right granted to a user for his access to certain items.
ACL	See **access control list**
advanced telecom application environment	A platform that is used by the hardware of the N2510. To expand the system capacity smoothly, you only need to add certain boards to the shelf and need not replace the server. This helps reduce the investments of the customer.
AIS	See **Alarm Indication Signal**
Alarm	A message reported when a fault is detected by a device or by the network management system during the process of polling devices. Each alarm corresponds to a recovery alarm. After a recovery alarm is received, the status of the corresponding alarm changes to cleared.
alarm acknowledgement	An operation performed on an alarm. Through this operation, the status of an alarm is changed from unacknowledged to acknowledged, which indicates that the user starts handling the alarm. The process during which when an alarm is generated, the operator needs to acknowledge the alarm and take the right step to clear the alarm.
alarm correlation rule analyzing	A process of analyzing the alarms that meet alarm correlation rules. If alarm 2 is generated within 5 seconds after alarm 1 is generated and meets the alarm correlation analysis rules, the EMS masks alarm 2 or improves its severity level according to the alarm correlation rules.
alarm delay time	The alarm delay time consists of the start delay time and the end delay time. When an NE detects an alarm for a period, the period is the start delay time. When an NE detects that the alarm disappears for a period, the period is the end delay time. Unnecessary alarms that are caused by error reports or jitters can be avoided by setting the delay time.

Copyright © Huawei Technologies Co., Ltd.

alarm indication	On the cabinet of an NE, there are four indicators in different colors indicating the current status of the NE. When the green indicator is on, it indicates that the NE is powered on. When the red indicator is on, it indicates that a critical alarm is generated. When the orange indicator is on, it indicates that a major alarm is generated. When the yellow indicator is on, it indicates that a minor alarm is generated. The ALM alarm indicator on the front panel of a board indicates the current status of the board. (Metro)
Alarm Indication Signal	A code sent downstream in a digital network as an indication that an upstream failure has been detected and alarmed. It is associated with multiple transport layers. Note: See ITU-T Rec. G.707/Y.1322 for specific AIS signals.
alarm mask	On the host, an alarm management method through which users can set conditions for the system to discard (not to save, display, or query for) the alarm information meeting the conditions.
alarm reporting to the EMS immediately	On a device, an alarm is reported to the EMS at once after the alarm is generated. On the EMS client, the corresponding alarm information is displayed on the alarm panel.
alarm severity	The significance of a change in system performance or events. According to ITU-T recommendations, an alarm can have one of the following severities:Critical, Major, Minor, Warning.
alarm status	The devices in the network report traps to the NMS, which displays the alarm statuses in the topological view. The status of an alarm can be critical, major, minor and prompt.
alarm synchronization	When alarm synchronization is implemented, the EMS checks the alarm information in its database and on the NEs. If the alarm information on the two locations is inconsistent, the alarm information on the NEs is synchronized to the EMS database to replace the original records.
ALC link	A piece of end-to-end configuration information, which exists in the equipment (single station) as an ALC link node. Through the ALC function of each node, it fulfils optical power control on the line that contains the link.
ARP Proxy	When a host sends an ARP request to another host, the request is processed by the DSLAM connected to the two hosts. The process is called ARP proxy. This protocol helps save the bandwidth in the networking of a low-rate WAN or helps implement the layer 3 communication between access devices in the networking of layer 2 isolation.
Asynchronous Transfer Mode	A data transfer technology based on cell, in which packets allocation relies on channel demand. It supports fast packet switching to achieve efficient utilization of network resources. The size of a cell is 53 bytes, which consist of 48-byte payload and 5-byte header.
ATAE	See **advanced telecom application environment**
ATM	See **Asynchronous Transfer Mode**
Authority and Domain Based Management	The function of the NMS for authority management. With this function, you can: 1. Partition and control the management authority 2. Manage device nodes and service data by region 3. Allocate users with different management and operation rights for different regions
auto-negotiation	An optional function of the IEEE 802.3u Fast Ethernet standard that enables devices to automatically exchange information over a link about speed and duplex abilities.

Copyright © Huawei Technologies Co., Ltd.

B

bandwidth	A range of transmission frequencies that a transmission line or channel can carry in a network. In fact, it is the difference between the highest and lowest frequencies the transmission line or channel. The greater the bandwidth, the faster the data transfer rate.
BASE	A kind of bus or plane used to load software, transmit alarms and maintain information exchange.
basic input/output system	A firmware stored in the computer mainboard. It contains basic input/output control programs, power-on self test (POST) programs, bootstraps, and system setting information. The BIOS provides hardware setting and control functions for the computer.
BFD	See **Bidirectional Forwarding Detection**
Bidirectional Forwarding Detection	A simple Hello protocol, similar to the adjacent detection in the route protocol. Two systems periodically send BFD detection messages on the channel between the two systems. If one system does not receive the detection message from the other system for a long time, you can infer that the channel is faulty. Under some conditions, the TX and RX rates between systems need to be negotiated to reduce traffic load.
BIOS	See **basic input/output system**
board	Board refers to an electronic part that can be plugged in to provide new capability. It comprises chips and electronic components and these components are always on a flat and hard base and connected through conductive paths. A board provides ports for upstream connections or service provisioning.
Bond	Bond: On the SUSE Linux OS, the bond technology is used to form a virtual layer between the physical layer and the data link layer. This technology allows two server NICs connecting to a switch to be bound to one IP address. The MAC addresses of the two NICs are also automatically bound as one MAC address. In this manner, a virtual NIC is formed. The bond technology supports two modes: double-live and primary/secondary. In double-live mode, after receiving request data from a remote server, the virtual NIC on the server determines data transmission based on an algorithm, improving network throughput and usability of the server. In primary/secondary mode, if an NIC does not function properly, services will be automatically switched to the other NIC, ensuring service protection. The SUSE Linux OS supports the binding of NICs in primary/secondary mode.

C

C/S	See **client/server software architecture**
CAR	See **committed access rate**
CAU	See **Client Auto Update**
CDE	See **Common Desktop Environment**
CIR	See **Committed Information Rate**
client	A device that sends requests, receives responses, and obtains services from the server.
Client Auto Update	This function helps you to automatically detect the update of the client version and upgrade the client. This keeps the version of the client is the same as that of the server.

Copyright © Huawei Technologies Co., Ltd.

Client/Server	The model of interaction in a distributed system in which a program at one site sends a request to a program at another site and awaits a response. The requesting program is called a client. The program satisfying the request is called the server. It is usually easier to build client software than build the server software.
client/server software architecture	A message-based and modular software architecture that comprises servers and clients. Compared with the centralized, mainframe, and time sharing computing, the client/server software architecture improves the usability, flexibility, interoperability, and scalability. In this architecture, a client is defined as the party that requires services and a server is defined as the party that provides services. The client/server architecture reduces network traffic by providing a query response rather than transferring all files.
cluster	A mechanism adopted to improve the system performance. Several devices of the same type form a cluster. The exterior of a cluster is some like a kind of equipment. In the interior of a cluster, the nodes share the load.
committed access rate	A traffic control method that uses a set of rate limits to be applied to a router interface. CAR is a configurable method by which incoming and outgoing packets can be classified into QoS (Quality of Service) groups, and by which the input or output transmission rate can be defined.
Committed Information Rate	The rate at which a frame relay network agrees to transfer information in normal conditions. Namely, it is the rate, measured in bit/s, at which the token is transferred to the leaky bucket.
Common Desktop Environment	The Common Desktop Environment (CDE) is an integrated graphical user interface for open systems desktop computing. It delivers a single, standard graphical interface for the management of data and files (the graphical desktop) and applications. CDE's primary benefits -- deriving from ease-of-use, consistency, configurability, portability, distributed design, and protection of investment in today's applications -- make open systems desktop computers as easy to use as PCs, but with the added power of local and network resources available at the click of a mouse.
Common Object Request Broker Architecture	A specification developed by the Object Management Group in 1992 in which pieces of programs (objects) communicate with other objects in other programs, even if the two programs are written in different programming languages and are running on different platforms. A program makes its request for objects through an object request broker, or ORB, and thus does not need to know the structure of the program from which the object comes. CORBA is designed to work in object-oriented environments. See also IIOP, object (definition 2), Object Management Group, object-oriented.
Common Object Request Broker Architecture	A specification developed by the Object Management Group in 1992 in which pieces of programs (objects) communicate with other objects in other programs, even if the two programs are written in different programming languages and are running on different platforms. A program makes its request for objects through an object request broker, or ORB, and thus does not need to know the structure of the program from which the object comes. CORBA is designed to work in object-oriented environments. See also IIOP, object (definition 2), Object Management Group, object-oriented.
CORBA	See **Common Object Request Broker Architecture**
CORBA	See **Common Object Request Broker Architecture**

Copyright © Huawei Technologies Co., Ltd.

D

Data Communication Channel	Data Communications Channel. The data channel that uses the D1-D12 bytes in the overhead of an STM-N signal to transmit information on operation, management, maintenance and provision (OAM&P) between NEs. The DCC channels that are composed of bytes D1-D3 is referred to as the 192 kbit/s DCC-R channel. The other DCC channel that are composed of bytes D4-D12 is referred to as the 576 kbit/s DCC-M channel.
data communication network	A communication network used in a TMN or between TMNs to support the data communication function.
data replication link	A link used for data replication between the production machine and redundancy machine. It is separated from the network of the primary links.
DCC	See **Data Communication Channel**
DCN	See **data communication network**
DDN	See **digital data network**
Delay	An average time taken by the service data to transmit across the network.
DG	disk group
DHCP	See **Dynamic Host Configuration Protocol**
digital data network	A high-quality data transport tunnel that combines the digital channel (such as fiber channel, digital microwave channel, or satellite channel) and the cross multiplex technology.
disk mirroring	A technique in which all or part of a hard disk is duplicated onto one or more other hard disks, each of which ideally is attached to its own controller. With disk mirroring, any change made to the original disk is simultaneously made to the other disks so that if the original disk becomes damaged or corrupted, the mirror disks will contain a current, undamaged collection of the data from the original disk.
Dynamic Host Configuration Protocol	A client-server networking protocol. A DHCP server provides configuration parameters specific to the DHCP client host requesting, generally, information required by the host to participate on the Internet network. DHCP also provides a mechanism for allocation of IP addresses to hosts.

E

E1	A European standard for high-speed data transmission at 2.048 Mbit/s. It provides 32 x 64 kbit/s channels.
ECC	See **embedded control channel**
embedded control channel	A logical channel that uses a data communications channel (DCC) as its physical layer, to enable transmission of operation, administration, and maintenance (OAM) information between NEs.
Equipment Serial Number	A 32-bit number assigned by the mobile station manufacturer, uniquely identifying the mobile station equipment.
ESN	See **Equipment Serial Number**

Copyright © Huawei Technologies Co., Ltd.

F

Fabric	A kind of bus/plane used to exchange system service data.
File Transfer Protocol	A member of the TCP/IP suite of protocols, used to copy files between two computers on the Internet. Both computers must support their respective FTP roles: one must be an FTP client and the other an FTP server.
FTP	See **File Transfer Protocol**

G

gateway	A device to connect two network segments which use different protocols. It is used to translate the data in the two network segments.
gateway network element	A network element that is used for communication between the NE application layer and the NM application layer
GE	The IEEE standard dubbed 802.3z, which includes support for transmission rates of1 Gbps (gigabit per second)--1,000 Mbps (megabits per second)--over an Ethernet network.
GMT	See **Greenwich Mean Time**
GNE	See **gateway network element**
graphical user interface	A visual computer environment that represents programs, files, and options with graphical images, such as icons, menus, and dialog boxes, on the screen.
Greenwich Mean Time	The mean solar time at the Royal Greenwich Observatory in Greenwich near London in England, which by convention is at 0 degrees geographic longitude.
GUI	See **graphical user interface**

H

HA	See **High Availability**
HA system	See **high availability system**
half-duplex	A transmitting mode in which a half-duplex system provides for communication in both directions, but only one direction at a time (not simultaneously). Typically, once a party begins receiving a signal, it must wait for the transmitter to stop transmitting, before replying.
High Availability	The ability of a system to continuously perform its functions during a long period, which may exceeds the suggested working time of the independent components. You can obtain the high availability (HA) by using the error tolerance method. Based on learning cases one by one, you must also clearly understand the limitations of the system that requires an HA ability and the degree to which the ability can reach.
high availability system	The high availability system (HA) system indicates that two servers are adopted by a same computer. When the primary server is faulty, the secondary server provides the environment on which the software runs through the related technology.
History alarm	The confirmed alarms that have been saved in the memory and other external memories.

Copyright © Huawei Technologies Co., Ltd.

host	The computer system that is connected with disks, disk subsystems, or file servers and on which data is stored and I/Os are accessed. A host can be a large computer, server, workstation, PC, multiprocessor computer, and computer cluster system.

I

IANA	See **Internet assigned numbers authority**
ICA	See **independent computing architecture**
ICMP	See **Internet Control Message Protocol**
IE	See **Internet Explorer**
IEEE	See **Institute of Electrical and Electronics Engineers**
iMAP	See **integrated management application platform**
independent computing architecture	An architecture that logically separates application execution from user interfaces to transmit only keyboard actions, mouse responses, and screen updates on the network.
Institute of Electrical and Electronics Engineers	A society of engineering and electronics professionals based in the United States but boasting membership from numerous other countries. The IEEE focuses on electrical, electronics, computer engineering, and science-related matters.
integrated management application platform	N/A
International Standard Organization	One of two international standards bodies responsible for developing international data communications standards. International Organization for Standardization (ISO) works closely with the International Electro- technical Commission (IEC) to define standards of computing. They jointly published the ISO/IEC SQL-92 standard for SQL.
International Telecommunication Union Telecommunication Standardization	An organization that establishes recommendations and coordinates the development of telecommunication standards for the entire world.
Internet assigned numbers authority	The organization operated under the IAB. IANA delegates authority for IP address-space allocation and domain-name assignment to the NIC and other organizations. IANA also maintains a database of assigned protocol identifiers used in the TCP/IP suite, including autonomous system numbers.
Internet Control Message Protocol	A network-layer (ISO/OSI level 3) Internet protocol that provides error correction and other information relevant to IP packet processing. For example, it can let the IP software on one machine inform another machine about an unreachable destination. See also communications protocol, IP, ISO/OSI reference model, packet (definition 1).
Internet Explorer	Microsoft's Web browsing software. Introduced in October 1995, the latest versions of Internet Explorer include many features that allow you to customize your experience on the Web. Internet Explorer is also available for the Macintosh and UNIX platforms.

Copyright © Huawei Technologies Co., Ltd.

Internet Protocol	The TCP/IP standard protocol that defines the IP packet as the unit of information sent across an Internet and provides the basis for connectionless, best-effort packet delivery service. IP includes the ICMP control and error message protocol as an integral part. The entire protocol suite is often referred to as TCP/IP because TCP and IP are the two fundamental protocols. IP is standardized in RFC 791.
Internet Protocol Version 6	A update version of IPv4. It is also called IP Next Generation (IPng). The specifications and standardizations provided by it are consistent with the Internet Engineering Task Force (IETF).Internet Protocol Version 6 (IPv6) is also called. It is a new version of the Internet Protocol, designed as the successor to IPv4. The specifications and standardizations provided by it are consistent with the Internet Engineering Task Force (IETF).The difference between IPv6 and IPv4 is that an IPv4 address has 32 bits while an IPv6 address has 128 bits.
inventory	A physical inventory in the U2000, that is, a physical resource such as a telecommunications room, rack, NE, subrack, board, subboard, port, optical module, fiber/cable, fiber and cable pipe, link resource, interface resource, access service, ONU, or NE e-label that can be managed on the U2000, and the relationship between resources.
IP	See **Internet Protocol**
IPv4	The abbreviation of Internet Protocol version 4. IPv4 utilizes a 32bit address which is assigned to hosts. An address belongs to one of five classes (A, B, C, D, or E) and is written as 4 octets separated by periods and may range from 0.0.0.0 through to 255.255.255.255. Each address consists of a network number, an optional subnetwork number, and a host number. The network and subnetwork numbers together are used for routing, and the host number is used to address an individual host within the network or subnetwork. IPv4 addresses may also be represented using CIDR (Classless Inter Domain Routing).
IPv6	See **Internet Protocol Version 6**
ISO	See **International Standard Organization**
ITU-T	See **International Telecommunication Union Telecommunication Standardization**

J

Java Virtual Machine	The environment in which Java programs run. The Java Virtual Machine gives Java programs a software-based computer they can interact with. Because the Java Virtual Machine is not a real computer but exists in software, a Java program can run on any physical computing platform.
JRE	Java runtime environment
JVM	See **Java Virtual Machine**

K

keyboard, video, and mouse	A hardware device installed in the integrated configuration cabinet. KVM serves as the input and output device for the components inside the cabinet. It consists of a screen, a keyboard, and a mouse.
KVM	See **keyboard, video, and mouse**

Copyright © Huawei Technologies Co., Ltd.

L

LAN	See **Local Area Network**
LCT	See **Local Craft Terminal**
LDAP	See **Lightweight Directory Access Protocol**
License	A permission that the vendor provides for the user with a specific function, capacity, and durability of a product. A license can be a file or a serial number. Usually the license consists of encrypted codes, and the operation authority varies with different level of license.
Lightweight Directory Access Protocol	An TCP/IP based network protocol that enables access to a DSA. It involves some reduced functionality from X.500 DAP specification.
Link Layer Discovery Protocol	The Link Layer Discovery Protocol (LLDP) is an L2D protocol defined in IEEE 802.1ab. Using the LLDP, the NMS can rapidly obtain the Layer 2 network topology and changes in topology when the network scales expand.
LLDP	See **Link Layer Discovery Protocol**
load balancing	The distribution of activity across two or more servers or components in order to avoid overloading any one with too many requests or too much traffic.
Local Area Network	A network formed by the computers and workstations within the coverage of a few square kilometers or within a single building. It features high speed and low error rate. Ethernet, FDDI, and Token Ring are three technologies used to implement a LAN. Current LANs are generally based on switched Ethernet or Wi-Fi technology and running at 1,000 Mbit/s (that is, 1 Gbit/s).
Local Craft Terminal	Local Craft Terminal. The terminal software that is used for local maintenance and the management of NEs in the singer-user mode, to realize integrated management of multi-service transmission network. See also U2000.

M

MAN	See **Metropolitan Area Network**
MD5	See **Message-Digest Algorithm 5**
MDP	See **message dispatch process**
message dispatch process	N/A
Message-Digest Algorithm 5	A one-way hashing algorithm that produces a 128-bit hash. Both MD5 and Secure Hash Algorithm (SHA) are variations on MD4 and are designed to strengthen the security of the MD5 hashing algorithm.
Metropolitan Area Network	A metropolitan area network (MAN) is a network that interconnects users with computer resources in a geographic area or region larger than that covered by even a large local area network (LAN) but smaller than the area covered by a wide area network (WAN). The term is applied to the interconnection of networks in a city into a single larger network (which may then also offer efficient connection to a wide area network). It is also used to mean the interconnection of several local area networks by bridging them with backbone lines. The latter usage is also sometimes referred to as a campus network.

Copyright © Huawei Technologies Co., Ltd.

modem	A device or program that enables a computer to transmit data over, for example, telephone or cable lines. Computer information is stored digitally, whereas information transmitted over telephone lines is transmitted in the form of analog waves. A modem converts between these two forms.
MS	Manual Switch
MSTP	See **multi-service transmission platform**
MSuite	NMS maintenance suite
multi-service transmission platform	A platform based on the SDH platform, capable of accessing, processing and transmitting TDM services, ATM services, and Ethernet services, and providing unified management of these services.

N

NBI	See **northbound interface**
NE	See **network element**
network element	A network element (NE) contains both the hardware and the software running on it. One NE is at least equipped with one system control board which manages and monitors the entire network element. The NE software runs on the system control board.
network layer	The network layer is layer 3 of the seven-layer OSI model of computer networking. The network layer provides routing and addressing so that two terminal systems are interconnected. In addition, the network layer provides congestion control and traffic control. In the TCP/IP protocol suite, the functions of the network layer are specified and implemented by IP protocols. Therefore, the network layer is also called IP layer.
Network Management System	A system in charge of the operation, administration, and maintenance of a network.
Network Time Protocol	The Network Time Protocol (NTP) defines the time synchronization mechanism. It synchronizes the time between the distributed time server and the client.
new technology file system	An advanced file system designed for use specifically with the Windows NT operating system. It supports long filenames, full security access control, file system recovery, extremely large storage media, and various features for the Windows NT POSIX subsystem. It also supports object-oriented applications by treating all files as objects with user-defined and system-defined attributes.
NMS	See **Network Management System**
northbound interface	The interface that connects to the upper-layer device to realize service provisioning, report alarms and performance statistics.
NTFS	See **new technology file system**
NTP	See **Network Time Protocol**

O

OAM	See **operation, administration and maintenance**

Copyright © Huawei Technologies Co., Ltd.

Object Set	A collection of managed objects. 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.
OMC	See **Operation and Maintenance Center**
ONU	See **Optical Network Unit**
Operation and Maintenance Center	An Operations and Maintenance Centre is an element within a network management system responsible for the operations and maintenance of a specific element or group of elements. For example an OMC-Radio may be responsible for the management of a radio subsystem where as an OMC-Switch may be responsible for the management of a switch or exchange. However, these will in turn be under the control of a NMC (Network Management Centre) which controls the entire network.
Operation Rights	Operation Rights specify the concrete operation that the user can perform. The operation right aims at the security objects. If one user has no right to manage one device, he or she cannot operate the device.
Operation Set	A collection of operations. Classifying operations into operation sets helps to manage user operation rights. Operations performed by different users have different impacts on system security. Operations with similar impacts are classified into an operation set. Users or user groups entitled to an operation set can perform all the operations in the operation set. The NMS provides some default operation sets. If the default operation sets cannot meet the requirements for right allocation, users can create operation sets as required.
Operation System	Operation System is abbreviated to OS. OS is the interface between users and computers. It manages all the system resources of the computer, and also provides an abstract computer for users. With the help of OS, users can use the computers without any direct operation on hardware. For the computer system, OS is a set of programs used to manage all system resources; for users, OS provides a simple and abstract method to use the system resources.
operation, administration and maintenance	A group of network support functions that monitor and sustain segment operation, activities that are concerned with, but not limited to, failure detection, notification, location, and repairs that are intended to eliminate faults and keep a segment in an operational state and support activities required to provide the services of a subscriber access network to users/subscribers.
Operations Support System	A system whose main function is to run applications that manage network elements, networks and services.
Optical Network Unit	A form of Access Node that converts optical signals transmitted via fiber to electrical signals that can be transmitted via coaxial cable or twisted pair copper wiring to individual subscribers.
OS	See **Operation System**
OSS	See **Operations Support System**

P

packet loss ratio	The ratio of total lost packet outcomes to total transmitted packets in a population of interest.

Copyright © Huawei Technologies Co., Ltd.

packet transport network	N/A
PC	See **Personal Computer**
Peak Information Rate	Peak Information Rate . A traffic parameter, expressed in bit/s, whose value should be not less than the committed information rate.
Personal Computer	A computer used by an individual at a time in a business, a school, or at home.
PIR	See **Peak Information Rate**
PMU	The unit that is used to monitor power supply in the equipment.
Point-to-Point Protocol over Ethernet	PPPoE, point-to-point protocol over Ethernet, is a network protocol for encapsulating PPP frames in Ethernet frames. It is used mainly with DSL services. It offers standard PPP features such as authentication, encryption, and compression.
port	1. Of a device or network, a point of access where signals may be inserted or extracted, or where the device or network variables may be observed or measured. (188) 2. In a communications network, a point at which signals can enter or leave the network en
Power and environment monitoring unit	The power and environment monitoring unit is installed at the top of the cabinet of the SDH equipment and is used to monitor the environment variables, such as the power supply and temperature. With external signal input through the relay, fire alarm, smoke alarm, burglary alarm, etc. can be monitored as well. With the display on NMS system, the change of environment can be monitored timely and accurately. For the equipment installed with a power & environment monitoring board, the following parameters can be set: relay switch output control, temperature alarm threshold, relay usage and alarm setting, query of DIP switch status, etc.
PPPoE	See **Point-to-Point Protocol over Ethernet**
private network	A network which provides services to a specific set of users only (see Recommendation I.570).
PSTN	See **public switched telephone network**
PTN	See **packet transport network**
public switched telephone network	Public Switched Telephone Network. A telecommunications network established to perform telephone services for the public subscribers.Sometimes called POTS.

R

RADIUS	See **remote authentication dial-in user service**
RADIUS	See **Remote Authentication Dial in User Service**
RAID	See **Redundant Arrays of Independent Disks**

Copyright © Huawei Technologies Co., Ltd.

Redundant Arrays of Independent Disks	A data storage scheme that allows data to be stored and replicated in a hardware disk group (logical hard disk) consisting of multiple hard disks (physical hard disks). When multiple physical disks are set up to use the RAID technique, they are said to be in a RAID array. The hard disks in a RAID array provides higher data reliability and input/output performance. There are various defined levels of RAID, each offering differing trade-offs among access speed, reliability, and cost. At present, there are seven basic RAID levels from RAID 0 to RAID 6. These basic RAID levels can be further combined to form new RAID levels, such as RAID 10 (a combination of RAID 0 and RAID 1).
Remote Authentication Dial in User Service	RADIUS was originally used to manage the scattered users who use the serial interface and modem, and it has been widely used in NAS. NAS delivers the information of users on authentication, authorization and accounting to the RADIUS server. RADIUS stipulates how the user and accounting information is transferred between NAS and RADIUS. The RADIUS server is responsible for receiving the connection request from users to complete authentication, and returning the configurations of the users to NAS.
remote authentication dial-in user service	A security service that authenticates and authorizes dial-up users and is a centralized access control mechanism. RADIUS uses the User Datagram Protocol (UDP) as its transmission protocol to ensure real-time quality. RADIUS also supports the retransmission and multi-server mechanisms to ensure good reliability.
replicated volume group	N/A
replication link	A link used for data replication between the production machine and redundancy machine. It is physically separated from the network of the primary links.
Rlink	See **data replication link**
RTN	Radio Transmission Node
RVG	See **replicated volume group**

S

Script file	It is the text file describing the physical information and configuration information of the entire network, including the NE configuration file, port naming file, end-to-end configuration file, NE physical view script file, NMS information file and service implementation data script file.
SDH	See **Synchronous Digital Hierarchy**
Secure File Transfer Protocol (SFTP)	A network protocol designed to provide secure file transfer over SSH.
Secure Shell (SSH)	A set of standards and an associated network protocol that allows establishing a secure channel between a local and a remote computer. A feature to protect information and provide powerful authentication function for a network when a user logs in to the network through an insecure network. It prevents IP addresses from being deceived and plain text passwords from being captured.
Secure Sockets Layer	A protocol for ensuring security and privacy in Internet communications. SSL supports authentication of client, server, or both, as well as encryption during a communications session.

Copyright © Huawei Technologies Co., Ltd.

Security Log	Security logs record the security operations on the NMS, such as logging in to the server, modifying the password, and exiting from the NMS server.
Serial Line Interface Protocol	Serial Line Interface Protocol, defines the framing mode over the serial line to implement transmission of messages over the serial line and provide the remote host interconnection function with a known IP address.
server	1. On a local area network, a computer running administrative software that controls access to the network and its resources, such as printers and disk drives, and provides resources to computers functioning as workstations on the network. 2. On the Internet or other network, a computer or program that responds to commands from a client. For example, a file server may contain an archive of data or program files; when a client submits a request for a file, the server transfers a copy of the file to the client. 3. A network device that provides services to network users by managing shared resources, often used in the context of a client-server architecture for a LAN.
SFTP	See **Secure File Transfer Protocol (SFTP)**
SSH	See **Secure Shell (SSH)**
shelf management module	The shelf management board of the ATAE server.
Signal Noise Ratio	The SNR or S/N (Signal to Noise Ratio) of the amplitude of the desired signal to the amplitude of noise signals at a given point in time. SNR is expressed as 10 times the logarithm of the power ratio and is usually expressed in dB (Decibel).
Signal to Noise Ratio Margin	The signal-to-noise ratio margin represents the amount of increased received noise (in dB) relative to the noise power that the system is designed to tolerate and still meet the target BER of accounting for all coding gains included in the design.
Simple Mail Transfer Protocol	The TCP/IP (Transmission Control Protocol/Internet Protocol) protocol which facilitates the transfer of electronic-mail messages, specifies how two systems are to interact, and the format of messages used to control the transfer of electronic mail.
Simple Network Management Protocol	A network management protocol of TCP/IP. It enables remote users to view and modify the management information of a network element. This protocol ensures the transmission of management information between any two points. The polling mechanism is adopted to provide basic function sets. According to SNMP, agents, which can be hardware as well as software, can monitor the activities of various devices on the network and report these activities to the network console workstation. Control information about each device is maintained by a management information block.
Simple Network Time Protocol	A protocol that is adapted from the Network Time Protocol (NTP) and synchronizes the clocks of computers over the Internet.
SLIP	See **Serial Line Interface Protocol**
SMM	See **shelf management module**
SMTP	See **Simple Mail Transfer Protocol**
SNMP	See **Simple Network Management Protocol**
SNR	See **Signal Noise Ratio**
SNRM	See **Signal to Noise Ratio Margin**

Copyright © Huawei Technologies Co., Ltd.

SNTP	See **Simple Network Time Protocol**
SONET	See **Synchronous Optical Network**
SQL	See **structured query language**
SSL	See **Secure Sockets Layer**
static route	A route that cannot adapt to the change of network topology. Operators must configure it manually. When a network topology is simple, the network can work in the normal state if only the static route is configured. It can improve network performance and ensure bandwidth for important applications. Its disadvantage is as follows: When a network is faulty or the topology changes, the static route does not change automatically. It must be changed by the operators.
Stelnet	Secure Shell Telnet
structured query language	A database query and programming language widely used for accessing, querying, updating, and managing data in relational database systems.
SVM	Solaris Volume Manager
Switching restoration time	It refers to the period of time between the start of detecting and the moment when the line is switched back to the original status after protection switching occurs in the MSP sub-network.
Synchronous Digital Hierarchy	SDH is a transmission scheme that follows ITU-T G.707, G.708, and G.709. It defines the transmission features of digital signals such as frame structure, multiplexing mode, transmission rate level, and interface code. SDH is an important part of ISDN and B-ISDN. It interleaves the bytes of low-speed signals to multiplex the signals to high-speed counterparts, and the line coding of scrambling is only used only for signals. SDH is suitable for the fiber communication system with high speed and a large capacity since it uses synchronous multiplexing and flexible mapping structure.
Synchronous Optical Network	Synchronous Optical Network, is a method for communicating digital information using lasers or light-emitting diodes (LEDs) over optical fiber. The method was developed to replace the Plesiochronous Digital Hierarchy (PDH) system for transporting large amounts of telephone and data traffic and to allow for interoperability between equipment from different vendors. SONET defines interface standards at the physical layer of the OSI seven-layer model. The standard defines a hierarchy of interface rates that allow data streams at different rates to be multiplexed. SONET establishes Optical Carrier (OC) levels from 51.8 Mbps (OC-1) to 9.95 Gbps (OC-192).
SYSLOG	Syslog is an industry standard protocol for recording device logs.

T

TCP	See **Transmission Control Protocol**
TCP/IP	See **Transmission Control Protocol/Internet Protocol**
Telecommunication Management Network	The Telecommunications Management Network is a protocol model defined by ITU-T for managing open systems in a communications network.An architecture for management, including planning, provisioning, installation, maintenance, operation and administration of telecommunications equipment, networks and services.

Copyright © Huawei Technologies Co., Ltd.

Telnet	Standard terminal emulation protocol in the TCP/IP protocol stack. Telnet is used for remote terminal connection, enabling users to log in to remote systems and use resources as if they were connected to a local system. Telnet is defined in RFC 854.
TFTP	See **Trivial File Transfer Protocol**
Time zone	A division of the earth's surface, usually extending across 15 degrees of longitude devised such that the standard time is the time at a meridian at the centre of the zone.
timing task management	The system can create a timing task (such as backing up, loading and recovering a task), run a timing task automatically, and suspend or resume a timing task.
TMN	See **Telecommunication Management Network**
Transmission Control Protocol	One of the core protocols of the Internet protocol suite. Using TCP, applications on networked hosts can create connections to one another, over which they can exchange streams of data. TCP guarantees reliable and in-order delivery of data from the sender to the receiver. TCP also distinguishes data for multiple connections by concurrent applications running on the same host.
Transmission Control Protocol/Internet Protocol	Common name for the suite of protocols developed to support the construction of worldwide internetworks.
Trivial File Transfer Protocol	A small and simple alternative to FTP for transferring files. TFTP is intended for applications that do not need complex interactions between the client and server. TFTP restricts operations to simple file transfers and does not provide authentication. TFTP is small enough to be contained in ROM to be used for bootstrapping diskless machines.

U

UDP	See **User Datagram Protocol**
UPS	Uninterruptible Power Supply
User Datagram Protocol	A TCP/IP standard protocol that allows an application program on one device to send a datagram to an application program on another. User Datagram Protocol (UDP) uses IP to deliver datagrams. UDP provides application programs with the unreliable connectionless packet delivery service. Thus, UDP messages can be lost, duplicated, delayed, or delivered out of order. UDP is used to try to transmit the data packet, that is, the destination device does not actively confirm whether the correct data packet is received.

V

VCS	See **Veritas Cluster Server**
Veritas Cluster Server	A High-availability cluster software, for Unix, Linux and Microsoft Windows computer systems, created by Veritas Software. It provides application cluster capabilities to systems running Databases, file sharing on a network, electronic commerce websites or other applications.
Veritas Volume Manager	A software product from veritas Inc.. The Veritas Volume Manager is used to manage disk storage.
Veritas Volume Replicator	A wide area network data replication solution offered by VERITAS for multiple operating systems. These include. AIX, HPUX and Solaris.

Copyright © Huawei Technologies Co., Ltd.

Virtual Local Area Network	A logical grouping of two or more nodes which are not necessarily on the same physical network segment but which share the same IP network number. This is often associated with switched Ethernet.
Virtual Router Redundancy Protocol	A protocol used for multicast or multicast LANs such as an Ethernet. A group of routers (including an active router and several backup routers) in a LAN is regarded as a virtual router, which is called a backup group. The virtual router has its own IP address. The host in the network communicates with other networks through this virtual router. If the active router in the backup group fails, one of the backup routers become the active one and provides routing service for the host in the network.
VLAN	See **Virtual Local Area Network**
volume	A logical unit for disk virtualization management, and basic object for host applications.
VRRP	See **Virtual Router Redundancy Protocol**
VVM	See **Veritas Volume Manager**

W

WAN	See **Wide Area Network**
wavelength division multiplexing	A technology that utilizes the characteristics of broad bandwidth and low attenuation of single mode optical fiber, uses multiple wavelengths as carriers, and allows multiple channels to transmit simultaneously in a single fiber.
WDM	See **wavelength division multiplexing**
Wide Area Network	A network composed of computers which are far away from each other which are physically connected through specific protocols. WAN covers a broad area, such as a province, a state or even a country.
Wireless Local Area Network	A generic term covering a multitude of technologies providing local area networking via a radio link. Examples of WLAN technologies include WiFi (Wireless Fidelity), 802.11b and 802.11a, HiperLAN, Bluetooth, etc.
WLAN	See **Wireless Local Area Network**
work station	A terminal or microcomputer, usually one that is connected to a mainframe or to a network, at which a user can perform applications.
WS	See **work station**

Copyright © Huawei Technologies Co., Ltd.