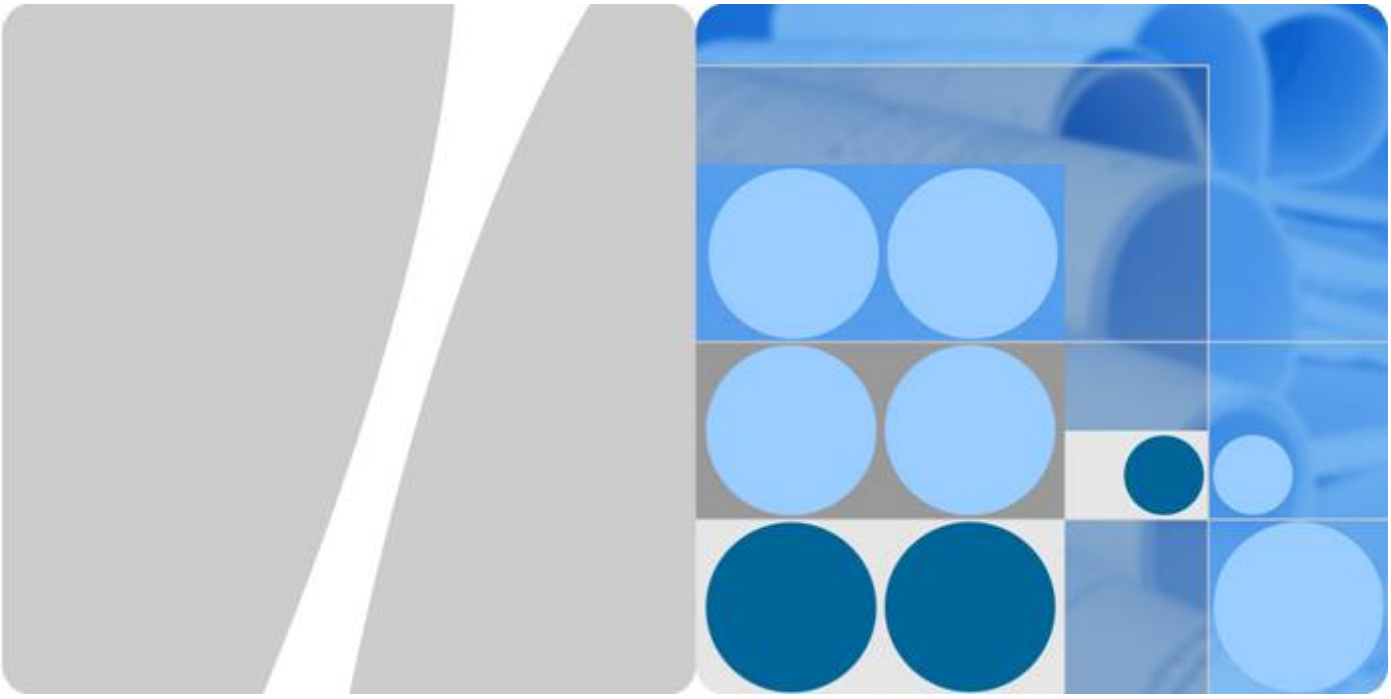


iManager U2000 Unified Network Management System

V100R002C01

Troubleshooting

Issue 05

Date 2010-11-19

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 the warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

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

Website: http://www.huawei.com

Email: support@huawei.com

About This Document

Related Version

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

Product Name	Version
iManager U2000	V100R002C01

Intended Audience

This document describes the procedure for handling a fault, information collecting, fault identifying, fault handling, and suggestions on U2000 troubleshooting.

This document is intended for:

- U2000 system administrators
- Technical support engineers

Symbol Conventions

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

Symbol	Description
 DANGER	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.
 WARNING	Indicates a hazard with a medium or low level of risk, which if not avoided, could result in minor or moderate injury.
 CAUTION	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.

Symbol	Description
TIP	Indicates a tip that may help you solve a problem or save time.
NOTE	Provides additional information to emphasize or supplement important points of the main text.

Command Conventions

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

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

GUI Conventions

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

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

Change History

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

Changes in Issue 05 (2010-11-19)

The fifth commercial release has the following updates:

Fixed some bugs.

Changes in Issue 04 (2010-09-24)

The forth commercial release has the following updates:

Fixed some bugs.

Changes in Issue 03 (2010-08-16)

The third commercial release has the following updates:

Fixed some bugs.

Changes in Issue 02 (2010-07-16)

The second commercial release has the following updates:

Fixed some bugs.

Changes in Issue 01 (2010-05-18)

Initial release.

Contents

Figures

Tables

1 Basic Principles of Troubleshooting

You need to locate and clear a fault by observing the troubleshooting principles and cautions.

Troubleshooting Principles

To analyze, locate, and clear a fault, observe the following principles:

- Restore the system monitoring as soon as possible.
- Before locating a fault, collect the fault data in a timely manner, and save the collected data to a mobile storage medium or another computer in the network.
- When determining the troubleshooting scheme, evaluate the impact first, to ensure the normal transmission of services.
- You can refer to the documents related to third-party hardware or call the customer service center of third-party hardware to troubleshoot third-party hardware faults.
- If the fault point cannot be located or the fault cannot be cleared, contact Huawei to obtain technical support:Tel: 400-8302118. Cooperate with engineers from Huawei for the troubleshooting, to minimize the period of service interruption.

Troubleshooting Cautions

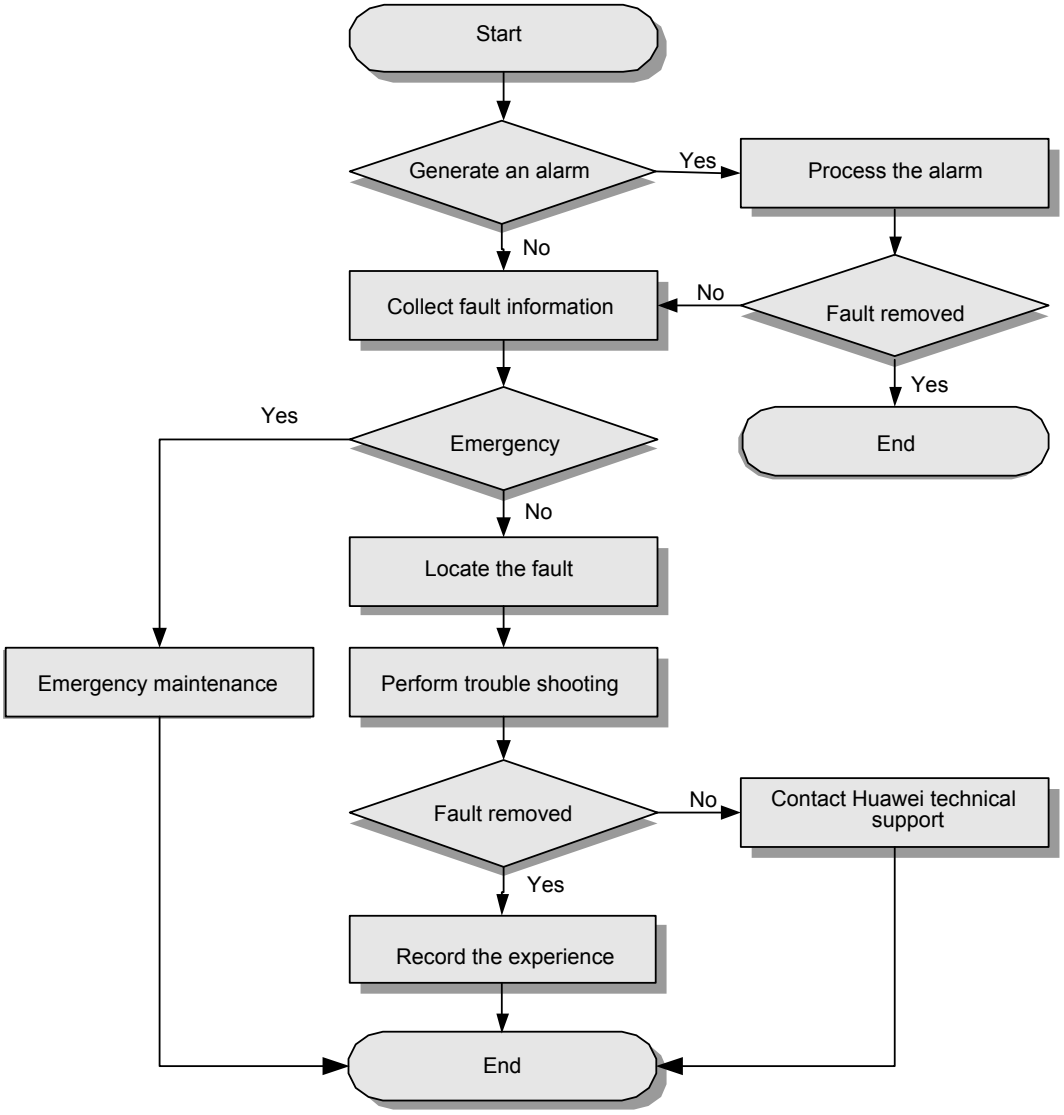
- Analyze the fault symptom, and handle the fault after locating the cause. If the cause is unknown, do not perform operations blind, to prevent the problem from being enlarged. The repairing of faults on the U2000 does not affect the NE running.
- Before handling a fault, keep all onsite records concerning the fault and do not delete any data or log randomly.
- Before any modification, back up the data of the U2000 by exporting the script or backing up the NMS data.
- After the system recovers, observe the running status, to make sure that the fault is cleared. Complete the related handling report in a timely manner.

2 Troubleshooting Process

When the U2000 is abnormal because of mis-operations, external causes such as power failure, and software and hardware faults of the U2000 , the network may fail to be monitored. In this case, you can locate the fault and repair the system by referring to the troubleshooting process and observing the troubleshooting principles and cautions. If the problem persists, contact the local office or customer service center of Huawei.

Figure 2-1 shows the troubleshooting process.

Figure 2-1 Troubleshooting process



NOTE

- Normally, the troubleshooting consists of three stages: locating the fault, collecting the information, and clearing the fault.
- If an alarm or abnormal event occurs on the U2000, clear the fault according to the prompt.

3 Fault Data Collection

In the case of a system fault, you need to collect the related data in a timely manner, to locate and handle the fault.

When a fault occurs on the U2000, see **Table 3-1** to collect the fault data.

NOTE

It is recommended that you use the Quick Step tool to collect the related data. For details, refer to the *iManager U2000 User Guide (Quick Step)*.

Table 3-1 Fault data collection items

Collection Item	Description
Time and place	Collect the information about the time and place of the fault. The time should be accurate to the minute.
Symptom description	Describe the symptom when the fault occurs. The fault can be located better based on a more specific description.
Measures taken and result	After you take some preliminary troubleshooting measures in field, new problems may occur. Therefore, you need to record the procedure of taking measures and the subsequent result in details.

Collection Item	Description

Version information	● View the version information about the U2000.
	– In the Solaris or SUSE Linux OS, the default directory storing the **imap.cfg** file is **/opt/U2000/server/etc/conf**.
	– In the Windows OS, the default directory storing the **imap.cfg** file is **D:\U2000\server\etc\conf**.
	The last several lines of the **imap.cfg** file displays the version information about the U2000.
	● In the Solaris or SUSE Linux OS, do as follows to view the system information:
	Log in to the OS as the **root** user. Then, run the following command:
	`# uname -a`
	● In the SUSE Linux OS, you can also run the following command to view the version of SUSE Linux:
	`# cat /etc/SuSE-release`
	● View the version information about the database:
	In the Solaris OS, run the following commands:
	`# su - sybase`
	`$ cd /opt/sybase/OCS-*/bin`
	`$ isql -SDBSVR -Usa -Psa's_password`
	`1> select @@version`
	`2> go`
	In the Windows OS, run the following commands in the command line interface (CLI):
	`> isql -SDBSVR -Usa -Psa's_password`
	`1> select @@version`
	`2> go`
	In the SUSE Linux OS, log in to the OS as the **oracle** user. Then, run the following commands:
	`$ sqlplus / as sysdba`
	`> startup`
	`> select * from v$version;`

IP information	Run the following commands to view the IP address and MAC address: ● On Solaris or SUSE Linux, log in as user root and run the **ifconfig -a** command. ● On Windows, open the command prompt window and run the **ipconfig /all** command.
Alarm information	Collect the alarm information, especially the U2000 alarms or abnormal events.

Collection Item	Description
Log information	● log information about the OS – Windows: Choose **Start** > **Run** from the desktop. Enter **eventvwr.msc** and then press Enter. In **Event Viewer**, select the corresponding event name, and right-click to save the log information of the operating system. – Solaris: **/var/adm**. You can also use the **/opt/SUNWexplo/bin/explorer** to collect log information about the Solaris OS. – SUSE Linux: **/var/log**. ● log information about the database – SQL Server: the ERRORLOG files in the directory of ***MSSQLServer_installation_directory*\MSSQL\LOG**. For example: all files in the directory of **C:\MSSQL2000\MSSQL\LOG**. – Sybase: **$SYBASE/$SYBASE_ASE/install/DBSVR.log**. For example: **/opt/sybase/ASE-15_0/install/DBSVR.log**. – Oracle: **$ORACLE_BASE/diag/rdbms/*db_name*/*instance_name*/trace/alert_U2KDB.log**. For example: **/opt/oracle/diag/rdbms/u2kdb/U2KDB/trace/alert_U2KDB.log**. Run the following command to view the log directory: `SQL> show parameter background_dump_dest` ● log information about the U2000 – Server logs – Windows: **%IMAPROOT%\server\log**. For example: **D:\U2000\server\log**. – Solaris or SUSE Linux: **$IMAPROOT/server/log**. For example: **/opt/U2000/server/log**. – Client logs – Windows: **%IMAPROOT%\client\log**. For example: **D:\U2000\client\log**. – Solaris or SUSE Linux: **$IMAPROOT/client/log**. For example: **/opt/U2000/client/log**. – Installation and deployment logs – Windows: **%HWENGRROOT%\logs**. For example: **C:\HWENGR\logs**. – Solaris or SUSE Linux: **$HWENGRROOT/logs**. For example: **/opt/HWENGR/logs**. For the details about collecting the log information about the U2000, refer to **Log Management** in the *iManager U2000 Administrator Guide*.
Networking diagram	If the fault is caused by networking problems, you need to view the networking diagram.

Collection Item	Description
ICMR-related files	If the server runs on Solaris or SUSE Linux, you need to collect the ICMR-related files: ● All files in the /etc/ICMR directory ● Files in the /var/ICMR directory

4 The NMS Alarm References

About This Chapter

This section lists relevant alarms of the NMS, including the alarm description, the affect of the alarm on the system, possible causes of the alarm and the manual handling of the alarm.

4.1 ALM-100 The CPU Usage Is High

Description

The U2000 consecutively samples the CPU usage. In a sampling period (number of consecutive CPU overloads * interval of performance monitoring refreshments, the default value is 300s) , if the CPU usage is larger than the generating threshold each time, the U2000 generates this alarm. If the CPU usage is smaller than the clearance threshold each time, the U2000 generates a corresponding cleared alarm.

NOTE

- To set the number of consecutive CPU overloads, interval of performance monitoring refreshments, thresholds for generating a high CPU usage alarm and clearing this alarm. Log in to the U2000 system monitor client. Choose **Administration** > **Settings** from the main menu. And then set these thresholds on the **Server Monitor** tab.
- If a server has more than one CPU, the U2000 continuously samples the usage of each CPU.
- In a dual-node system or distributed system, the U2000 continuously samples the CPU usage of each U2000 server.

Attribute

Alarm ID	Alarm Severity	Alarm Type
100	Major	QoS

Parameters

Name	Meaning
Host	Name of the host that generated the alarm.
Operating System	Operating system name of the host that generated the alarm.
Threshold	Threshold for generating alarm. When the value reaches the threshold, an alarm is generated.
Clearance threshold	Threshold for clearing alarm. When the value becomes smaller than the threshold, a clearance alarm is generated.
CPU Usage	Current CPU usage.

Impact on the System

- The U2000 responds slowly, and operations time out.
- The realtime reporting times out, and the information cannot be collected in time.

- The system processes services slowly. As a result, messages may be accumulated, and the system may crash.

System Actions

None.

Possible Causes

- The U2000 is busy temporarily.
- The U2000 server is performing an operation that occupies many system resources or takes a long time.
- The threshold for generating a high CPU usage alarm of the U2000 server is specified to a small value.
- The hardware performance of the server is low. Therefore, the U2000 cannot run properly.

Procedure

1 The U2000 is busy temporarily.

(1) Log in to the U2000 client.

(2) Choose **Fault** > **Browse Current Alarm** from the main menu.

(3) In the **Filter** window, click **OK**.

(4) In the **Browse Current Alarm** window, view **First Occurrence Time** of the alarm.

Check whether the following situations exist:

- The alarm is not consecutively generated, and is automatically cleared in ten minutes. In addition, the alarm is seldom generated. It is generated once each day at most.
- The alarm affects the system running (including the northbound interface operations, performance statistics collecting, alarm reporting, and user operations) slightly or for a short time. The performance delay does not exceed a period, the alarm delay does not exceed 30 seconds, and the GUI response takes less than ten seconds. In addition, the alarm is automatically cleared in 30 minutes.
- When the high CPU usage alarm is generated, a large number of alarms or events are reported (this is not a mandatory condition).

Solution:

- If so, it indicates that the system is busy temporarily. You do not need to process the alarm. If more than 100 alarms or events are reported each second when the high CPU usage alarm is generated, you need to process the reported alarms or events in time. The alarm processing is complete so far.
- If not, go to **2**.

2 The U2000 server is performing an operation that occupies many system resources or takes a long time.

Check the task that the system is performing, and stop the operation that occupies many system resources or takes a long time.

3 The threshold for generating a high CPU usage alarm of the U2000 server is specified to a small value.

(1) Log in to the U2000 system monitor client. Choose **Administration** > **Settings** from the main menu. In the displayed **System Monitor Settings** window, click the **Server Monitor** tab. Check whether the threshold for generating a high CPU usage alarm is proper.

Check whether the following situations exist:

- Check whether the threshold for generating a high CPU usage alarm is changed from 90% (default value) to a smaller value and whether the alarm is generated but the system runs properly with fast responses.
- The alarm is generated once each day at least.

Solution:

- If so, In the **System Monitor Settings** window, click the **Server Monitor** tab. Increase the threshold for generating a high CPU usage alarm to 90%, and increase the threshold for alarm clearance to 70% (default value). Then go to **3.2**.
- If not, go to **4**.

(2) After a sampling period, choose **Fault** > **Browse Current Alarm** from the main menu. In the **Filter** window, click **OK**. In the displayed **Browse Current Alarm** window, check whether the high CPU usage alarm is cleared.

- If so, The alarm processing is complete.
- If not, go to **4**.

4 The hardware performance of the server is low. Therefore, the U2000 cannot run properly.

If the hardware performance of the server is low:

- The hardware requirements corresponding to the management scope of the U2000 are beyond the actual hardware capability of the server.
- The alarm is generated consecutively or frequently.

Go to **5**.

5 Collect the information about alarm handling, and contact technical support personnel of the Huawei Technologies Co., Ltd..

----End

4.2 ALM-106 The OMC Service Is Terminated Abnormally

Description

If an U2000 service exits abnormally, this alarm is generated. After the U2000 service is recovered, this alarm is cleared.

Attribute

Alarm ID	Alarm Severity	Alarm Type
106	Major	Processing error

Parameters

Name	Meaning
Server name	Name of the server that generated the alarm.
SvcAgent	Process name of the service that terminated abnormally.
SvcName	Service name that terminated abnormally.

Impact on the System

- The functions of this service are unavailable.
- The other services that depend on the exited service will also exit.

System Actions

None.

Possible Causes

- The service is terminated manually. For example, a process is ended manually.
- The account password of the operating system or database is changed illegally.
- Another exception occurs. For example, database connections are not enough or the tempdb database is full.

Procedure

1 In alarm details, check whether the U2000 service is running properly.

(1) Log in to the U2000 server as an administrator.

(2) Set the environment variable.

- In Solaris or SuSE Linux, run the following commands:

  # **cd** *soft_path*

  #**. ./svc_profile.sh**

  NOTE

  soft_path indicates the path **$installation path of the NMS**.

- In Windows, the environment variable of the U2000 automatically takes effect.

(3) On the CLI, run the following command to view the output:

svc_adm -cmd status -svcname *service name*

In the command, *service name* indicates the name of the service that exits abnormally. The name is the consistent with the alarm parameter.

- According to the output of the command, if the service status is `running`, go to **3**.
- According to the output of the command, if the service status is `not running`, go to **2**.

2 Start the U2000 service that exits abnormally.

On the U2000 server, run the following command to start the stopped U2000 service:

svc_adm -cmd startsvc *service name*

In the command, *service name* indicates the name of the service that exits abnormally. The name is the consistent with the alarm parameter.

- If the service is started successfully, go to **3** to ensure that the alarm is cleared.
- If the service is not started, collect fault information. For details on how to collect fault information, see *U2000 Administrator Guide*. Then go to **4**.

3 Log in to the U2000 client, and choose **Fault** > **Browse Current Alarm** from the main menu. In the **Browse Current Alarm** window, check whether the alarm about abnormal exit of the U2000 service is cleared.

- If the alarm is not cleared, go to **4**.
- If the alarm is cleared successfully, the operation ends.

4 Collect the information about alarm handling, and contact technical support personnel of the Huawei Technologies Co., Ltd..

----End

4.3 ALM-114 The Number of Login Attempts Reaches the Maximum

Description

The U2000 generates this alarm in any of the following scenarios:

- The user logged in does not exist on the U2000.
- The user logged in is inactive on the U2000.
- The password of the user for login is incorrect, and the number of login attempts reaches the maximum.

When the lock duration reaches the automatic unlocking time specified in the account policy or another user with the unlocking right manually unlocks the account, the corresponding clearance alarm is generated.

NOTE

To set the account policy, you can choose **Administration** > **NMS Security** > **Security Policies** from the main menu, and then click the **Account Policy** tab in the **Security Policy** dialog box.

Attribute

Alarm ID	Alarm Severity	Alarm Type
114	Critical	Security service or mechanism violation

Parameters

Name	Meaning
User name	Name of user that number of password attempts for logging in to the system reaches the maximum number.
Maximum login attempts	Maximum number of login attempts before an alarm is generated. The parameter value is the same as the number of invalid login times that is specified in the account policy.
Client (IP address/Host)	Clients on which the user has attempted to log in to the U2000 server. Clients are represented by using IP addresses or host names.

Impact on the System

The user account is locked. The user needs to wait the unlocking until the account is automatically unlocked by the system. The user can also ask the administrator to unlock the account.

System Actions

None.

Possible Causes

The user uses an incorrect password to log in for consecutive times.

Procedure

1 The alarm does not need to be handled.

----End

4.4 ALM-102 The Memory Usage Is Too High

Description

The U2000 consecutively samples the memory usage. In a sampling period (number of consecutive memory overloads * interval of performance monitoring refreshments, the default value is 300s) , if the memory usage is larger than the generating threshold each time, the U2000 generates this alarm. If the memory usage is smaller than the clearance threshold each time, the U2000 generates a corresponding cleared alarm.

NOTE

- To set the thresholds for generating a busy memory alarm and clearing this alarm. Log in to the U2000 system monitor client. Choose **Administration** > **Settings** from the main menu. And then set these thresholds on the **Server Monitor** tab.
- In a two-node or distributed system, the U2000 continuously samples the memory usage of each server.

Attribute

Alarm ID	Alarm Severity	Alarm Type
102	Major	QoS

Parameters

Name	Meaning
Host	Name of the host that generated the alarm.
Operating System	Operating system name of the host.
Threshold	Threshold for generating alarm.
Clearance threshold	Threshold for clearing alarm.
Memory Usage	Current memory usage.

Impact on the System

- The available memory space of the system is insufficient. The U2000 responds slowly, and operations time out.
- The swap space is used frequently; therefore, the U2000 performance is degraded. The realtime reporting from the northbound interface, performance module, and fault module times out, and the information cannot be collected in time.
- An error may occur when processes are running. The system processes services slowly. As a result, messages may be accumulated, and the system may crash.

System Actions

None.

Possible Causes

- The disk usage of the swap partition is too high.
- The threshold for generating a high memory usage alarm of the U2000 server is specified to a small value.
- The U2000 server is performing an operation that occupies many system resources.
- The hardware performance of the server is low. Therefore, the U2000 cannot run properly.

Procedure

1 The disk usage of the swap partition is too high.

(1) Log in to the U2000 server.

- In Solaris, run **df -k** to view the record with **Mounted on** as **/tmp** and **Filesystem** as **swap**. Then check whether the disk usage of the swap partition that is mounted to **/tmp** is too high.
- If the disk usage of the swap partition that is mounted to **/tmp** exceeds 50%, there may be too many useless files in **/tmp**. In this case, run **cd /tmp** to access **/tmp**. Then run **ls -l** to query the file information, and check whether useless temporary files exist in **/tmp**. If so, run **rm** to clean up useless temporary files exist in **/tmp**. Finally, go to **1.2**.
- If the disk usage of the swap partition is smaller than 50%, go to **2**.

NOTE

If you wonder whether certain files can be deleted, contact Huawei Technologies Co., Ltd. technical support personnel.

(2) After a sampling period, choose **Fault** > **Browse Current Alarm** from the main menu. In the **Filter** window, click **OK**. In the displayed **Browse Current Alarm** window, check whether the high memory usage alarm is cleared.

- If so, the alarm processing is complete.
- If not, go to **2**.

2 The threshold for generating a high memory usage alarm of the U2000 server is specified to a small value.

(1) Log in to the U2000 system monitor client. Choose **Administration** > **Settings** from the main menu. In the displayed **System Monitor Settings** window, click the **Server Monitor** tab. Check whether the threshold for generating a high memory usage alarm is proper.

Check whether the threshold for generating a high memory usage alarm is changed from 95% (default value) to a smaller value and whether the alarm is generated but the system runs properly with fast responses.

Solution:

- If so, it indicates that the threshold for generating a high memory usage alarm is specified to a small value. In this case, go to **2.2**.
- If not, go to **3**.

(2) In the **System Monitor Settings** window, click the **Server Monitor** tab. Increase the threshold for generating a high memory usage alarm to 95%, and increase the threshold for alarm clearance to 85% (default value). Then go to **2.3**.

(3) Choose **Fault** > **Browse Current Alarm** from the main menu. In the **Browse Current Alarm** window, check whether the high memory usage alarm is cleared.

- If so, the alarm processing is complete.
- If not, go to **3**.

3 The U2000 server is performing an operation that occupies many system resources.

Check whether the following situations exist:

- Normally, this alarm is not generated.
- When the alarm is generated, the system is performing an operation that occupies many system resources.

Solution:

- If so, it indicates that the system is performing an operation that occupies many system resources. In this case, the alarm will be cleared automatically without manual intervention. The alarm processing is complete.
- If not, go to 4.

4 The hardware performance of the server is low. Therefore, the U2000 cannot run properly.

If hardware performance of the server is low:

- The hardware requirements corresponding to the management scope of the U2000 are beyond the actual hardware capability of the server.
- The alarm is generated consecutively or frequently.

Go to 5.

5 Collect the information about alarm processing, and contact technical support personnel of the Huawei Technologies Co., Ltd..

----End

4.5 ALM-33 The Server Is Disconnected from the Database

Description

When the U2000 detects an exception on the connection between itself and the database, this alarm is generated. When the U2000 detects the recovery of the connection between itself and the database, this alarm is cleared.

Attribute

Alarm ID	Alarm Severity	Alarm Type
33	Major	Processing error

Parameters

Name	Meaning
Host	Name of the host that generated the alarm.
Database service	Database service name of the host.
Database	Database name of the host.
Tablespace	Database table space name of the host.
Error Number	The number of the database error.

Impact on the System

- The operations relating to the database fail.
- The U2000 functions are unavailable.

System Actions

None.

Possible Causes

- The database services run abnormally.
- The database services do not run.
- The database password is changed.

Procedure

1. Choose **Fault** > **Browse Current Alarm** from the main menu. In the **Browse Current Alarm** window, view the error code in the additional information of alarm details.
   - If no error code exists, go to **3**.
   - If the corresponding error code exists, go to **2**.
2. According to the error code in the additional information to solve the problem.
   - Search the error code details to obtain a solution.

     NOTE
     - You can search for the Sybase error code details on the **http://infocenter.sybase.com** website.
     - You can search for the Oracle error code details on the **http://www.oracle.com** website.
     - You can search for the SQL Server error code details on the **http://www.microsoft.com** website.
   - If the problem is solved, the operation ends.
   - If the problem persists, go to **4**.
3. Check the database whether the database process exists, the initial password of the database is changed, and log in to the database normally.
   - If the problem is solved, the operation ends.
   - If the problem persists, go to **4**.
4. Collect the information about alarm handling, and contact technical support personnel of the Huawei Technologies Co., Ltd..

----End

4.6 ALM-34 The Disk Usage Is Too High (Warning)

Description

When the disk or partition(volume) usage is larger than the generating threshold for the warning severity, the U2000 generates this alarm. When the disk or partition usage is smaller than the clearance threshold for the warning severity, the alarm is cleared.

Attribute

Alarm ID	Alarm Severity	Alarm Type
34	Warning	QoS

Parameters

Name	Meaning
Host	Name of the host that generated the alarm.
Operating System	Operating system name of the host.
Disk	Disk path of the host.
Threshold	Threshold for generating alarm.
Clearance threshold	Threshold for clearing alarm.
Capacity	Disk capacity.
Usage	Current disk usage.

Impact on the System

The **write** operation of the U2000 service may fail, and a database exception may result.

System Actions

None.

Possible Causes

- There are too many useless disk files.
  - The recycle bin is not cleared.
  - In Solaris, the swap partition occupies large space. As a result, the log size of the Sybase database is too large.
  - The U2000 server has received a large amount of data, including NE alarms, events, and logs. The data is exported from the database to disk files in a short time.
  - There are too many temporary data files and backup files.
- The threshold for generating a high disk usage alarm of the U2000 server is specified to a small value.
- The disk space is insufficient. Therefore, the U2000 cannot run properly.

Procedure

1 There are too many useless disk files.

(1) Clear the recycle bin.

Clear the recycle bin. (In SUSE Linux and Solaris, perform this operation through the Xwindows.)

(2) Delete useless disk files from the Windows operating system.

NOTE

If you cannot determine which files can be deleted, contact Huawei technical support engineers.

- In Windows, check for and delete useless files through **Explore** and **Table 4-1**. When the operations are complete, go to **1.8**.

Table 4-1 Cleaning up disks in Windows

Disk	Directory or File	Potential Useless File	Cleanup
C:	-	Useless temporary files	Use **Explore** to delete useless files and clear the recycle bin.
D:	**%installation path of the NMS%\var\ThresholdExport\FM**	Too many alarm/event log dump files	Reserve the dump files generated on the current day, use **Explore** to delete the other dump files, and clear the recycle bin.
	%installation path of the NMS%\var\ThresholdExport\Log	Too many security/operation/system log dump files	

Disk	Directory or File	Potential Useless File	Cleanup
	%installation path of the NMS%\var\ThresholdExport\Dol	Too many device log dump files	
Other directories	-	● History backups of the installation package, patch package, adaptation-layer installation package, and so on ● Temporary path of daily backups ● History trace files ● Backup files during uninstall ● Useless temporary files ● Extra large log files ● Core files	● Use **Explore** to delete useless files and clear the recycle bin. ● In the DOS environment, run **break > log file name** to clear log files, for example, **break > vsftpd.log**. ● To obtain the location of core files, run **drwtsn32** through the command line interface.

- For SUSE Linux and Solaris, go to **1.3**.

(3) Run **df -k** to check which disks cause high disk usage.

If other locations except for **Disk** in the alarm parameter also has high disk usage but do not generate alarms, you can also clean up them.

(4) Run **cd** to access the directory with high disk usage. Then run **du -k | sort -nr > /tmp/du_k.txt** to query the sizes of all files and subdirectories under this directory. Sort the files and subdirectories, and place them in **du_k.txt**.

(5) Run **more** */tmp/du_k.txt* to view **du_k.txt** and find the subdirectory that causes high disk usage.

(6) Run **cd** to access the subdirectory that causes high disk usage. Then run **ls -l > /tmp/ls_l.txt** to query the sizes of all files and subdirectories under this subdirectory. Sort the files and subdirectories, and place them in **ls_l.txt**.

(7) Run **more /tmp/ls_l.txt** to view **ls_l.txt** and find the subdirectory or file that causes high disk usage. Use this method repeatedly until you find the files that cause high disk usage.

Then clean up these files. For details on how to determine and clear useless files, see **Table 4-2**. When the operations are complete, go to **1.8**.

Table 4-2 Cleaning up disks in Solaris and SUSE Linux

Disk	Directory or File	Potential Useless File	Cleanup
/	-	● Useless temporary files ● Extra large log files	● Run **rm** to delete useless files. ● Run **> log file name** to clear log files, for example, **> vsftpd.log**.
/opt	**$installation path of the NMS/var/ThresholdExport/Log**	Too many security/operation/system log dump files	Reserve the dump files generated on the current day, and run **rm** to delete the other dump files.
	$installation path of the NMS/var/ThresholdExport/Dol	Too many device log dump files	Reserve the dump files generated on the current day, and run **rm** to delete the other dump files.

Disk	Directory or File	Potential Useless File	Cleanup

	/opt/sybase/ASE-15_0/install (in Solaris)	● Check whether the log files of the Sybase databases are too large. The name format of database log files is **database instance name.log**, for example, **SYB.log**.
		● In Solaris, run **df -k** to view the record with **Mounted on** as **/tmp** and **Filesystem** as **swap**. Then check whether the disk usage of the swap partition that is mounted to **/tmp** exceeds 50%.
		● Check whether there is the companied **4.4 ALM-102 The Memory Usage Is Too High** or **4.2 ALM-106 The OMC Service Is Terminated Abnormally** alarm. (This is not mandatory.)
			a. Run the following command to clean up Sybase database logs (the following takes SYB.log as an example):
			`#cd /opt/sybase/ASE-15_0/install`
			`#> SYB.log`
			b. If the disk usage of the swap partition that is mounted to **/tmp** exceeds 50%, there may be too many useless files and temporary files in **/tmp**. In this case, run **cd /tmp** to access **/tmp**, then run **ls -l** to query the file information, and finally run **rm** to delete files.

/export/home	**/export/home/omc/var/ThresholdExport/FM**	Too many alarm/event log dump files	Reserve the dump files generated on the current day, and run **rm** to delete the other dump files.

Disk	Directory or File	Potential Useless File	Cleanup
Other directories	-	● History backups of the installation package, patch package, adaptation-layer installation package, and so on ● Temporary path of daily backups ● History trace files ● Backup files during uninstall ● Useless temporary files ● Extra large log files ● Core files.	● Run **rm** to delete useless files. ● Run **> log file name** to clear log files, for example, **> vsftpd.log**. ● The core files indicate the files with the prefix as core in **$iMAP/var/logs**.

(8) After a **Hard disk status refresh interval**, choose **Fault** > **Browse Current Alarm** from the main menu. In the **Filter** window, click **OK**. In the displayed **Browse Current Alarm** window, check whether the high disk usage alarm is cleared.

- If so, the alarm processing is complete.
- If not, go to **2**.

2 The threshold for generating a high disk usage alarm of the U2000 server is specified to a small value.

(1) Log in to the U2000 system monitor client. Choose **Administration** > **Settings** from the main menu. In the displayed **System Monitor Settings** window, click the **Hard Disk Monitor** tab. Check whether the threshold for generating a high disk usage alarm is larger than or equal to 60% (default value).

- If so, go to **3**.
- If not, increase the threshold for generating a high disk usage alarm to 60%, and increase the threshold for alarm clearance to 55% (default value). Then go to **2.2**.

(2) After a **Hard disk status refresh interval**, choose **Fault** > **Browse Current Alarm**. In the **Filter** window, click **OK**. In the displayed **Browse Current Alarm** window, check whether the high disk usage alarm is cleared.

- If so, the alarm processing is complete.
- If not, go to **3**.

3 The disk space is insufficient. Therefore, the U2000 cannot run properly.

Go to **4**.

4 Collect the information about alarm handling, and contact technical support personnel of the Huawei Technologies Co., Ltd..

----End

Related Information

4.7 ALM-35 The Disk Usage Is Too High (Minor)

4.8 ALM-36 The Disk Usage Is Too High (Major)

4.9 ALM-101 The Disk Usage Is Too High (Critical)

4.7 ALM-35 The Disk Usage Is Too High (Minor)

Description

When the disk or partition usage is larger than the generating threshold for the minor severity, the U2000 generates this alarm. When the disk or partition usage is smaller than the clearance threshold for the minor severity, the U2000 generates a corresponding cleared alarm.

Attribute

Alarm ID	Alarm Severity	Alarm Type
35	Minor	QoS

Parameters

Name	Meaning
Host	Name of the host that generated the alarm.
Operating System	Operating system name of the host that generated the alarm.
Disk	Disk path of the host that generated the alarm.
Threshold	Threshold for generating alarm.
Clearance threshold	Threshold for clearing alarm.
Capacity	Disk capacity.
Usage	Current disk usage.

Impact on the System

The **write** operation of the U2000 service may fail, and a database exception may result.

System Actions

None.

Possible Causes

- There are too many useless disk files.

- The recycle bin is not cleared.
- In Solaris, the swap partition occupies large space. As a result, the log size of the Sybase database is too large.
- The U2000 server has received a large amount of data, including NE alarms, events, and logs. The data is exported from the database to disk files in a short time.
- There are too many temporary data files and backup files.

- The threshold for generating a high disk usage alarm of the U2000 server is specified to a small value.
- The disk space is insufficient. Therefore, the U2000 cannot run properly.

Procedure

1 There are too many useless disk files.

(1) Clear the recycle bin.

Clear the recycle bin. (In SUSE Linux and Solaris, perform this operation through the Xwindows.)

(2) Delete useless disk files from the Windows operating system.

NOTE

If you cannot determine which files can be deleted, contact Huawei technical support engineers.

- In Windows, check for and delete useless files through **Explore** and **Table 4-3**. When the operations are complete, go to **1.8**.

Table 4-3 Cleaning up disks in Windows

Disk	Directory or File	Potential Useless File	Cleanup
C:	-	Useless temporary files	Use **Explore** to delete useless files and clear the recycle bin.
D:	**%installation path of the NMS%\var\ThresholdExport\FM**	Too many alarm/event log dump files	Reserve the dump files generated on the current day, use **Explore** to delete the other dump files, and clear the recycle bin.

Disk	Directory or File	Potential Useless File	Cleanup
	%installation path of the NMS%\var\ThresholdExport\Log	Too many security/operation/system log dump files	
	%installation path of the NMS%\var\ThresholdExport\Dol	Too many device log dump files	
Other directories	-	● History backups of the installation package, patch package, adaptation-layer installation package, and so on ● Temporary path of daily backups ● History trace files ● Backup files during uninstall ● Useless temporary files ● Extra large log files ● Core files	● Use **Explore** to delete useless files and clear the recycle bin. ● In the DOS environment, run **break > log file name** to clear log files, for example, **break > vsftpd.log**. ● To obtain the location of core files, run **drwtsn32** through the command line interface.

- For SUSE Linux and Solaris, go to **1.3**.

(3) Run **df -k** to check which disks cause high disk usage.

If other locations except for **Disk** in the alarm parameter also has high disk usage but do not generate alarms, you can also clean up them.

(4) Run **cd** to access the directory with high disk usage. Then run **du -k | sort -nr > /tmp/du_k.txt** to query the sizes of all files and subdirectories under this directory. Sort the files and subdirectories, and place them in **du_k.txt**.

(5) Run **more** */tmp/du_k.txt* to view **du_k.txt** and find the subdirectory that causes high disk usage.

(6) Run **cd** to access the subdirectory that causes high disk usage. Then run **ls -l > /tmp/ls_l.txt** to query the sizes of all files and subdirectories under this subdirectory. Sort the files and subdirectories, and place them in **ls_l.txt**.

(7) Run **more /tmp/ls_l.txt** to view **ls_l.txt** and find the subdirectory or file that causes high disk usage. Use this method repeatedly until you find the files that cause high disk usage. Then clean up these files. For details on how to determine and clear useless files, see **Table 4-4**. When the operations are complete, go to **1.8**.

Table 4-4 Cleaning up disks in Solaris and SUSE Linux

Disk	Directory or File	Potential Useless File	Cleanup
/	-	● Useless temporary files ● Extra large log files	● Run **rm** to delete useless files. ● Run **> log file name** to clear log files, for example, **> vsftpd.log**.
/opt	**$installation path of the NMS/var/ThresholdExport/Log**	Too many security/operation/system log dump files	Reserve the dump files generated on the current day, and run **rm** to delete the other dump files.
	$installation path of the NMS/var/ThresholdExport/Dol	Too many device log dump files	Reserve the dump files generated on the current day, and run **rm** to delete the other dump files.

Disk	Directory or File	Potential Useless File	Cleanup

	/opt/sybase/ASE-15_0/install (in Solaris)	● Check whether the log files of the Sybase databases are too large. The name format of database log files is **database instance name.log**, for example, **SYB.log**.
		● In Solaris, run **df -k** to view the record with **Mounted on** as **/tmp** and **Filesystem** as **swap**. Then check whether the disk usage of the swap partition that is mounted to **/tmp** exceeds 50%.
		● Check whether there is the companied **4.4 ALM-102 The Memory Usage Is Too High** or **4.2 ALM-106 The OMC Service Is Terminated Abnormally** alarm. (This is not mandatory.)
			a. Run the following command to clean up Sybase database logs (the following takes SYB.log as an example):
			`#cd /opt/sybase/ASE-15_0/install`
			`#> SYB.log`
			b. If the disk usage of the swap partition that is mounted to **/tmp** exceeds 50%, there may be too many useless files and temporary files in **/tmp**. In this case, run **cd /tmp** to access **/tmp**, then run **ls -l** to query the file information, and finally run **rm** to delete files.

/export/home	**/export/home/omc/var/ThresholdExport/FM**	Too many alarm/event log dump files	Reserve the dump files generated on the current day, and run **rm** to delete the other dump files.

Disk	Directory or File	Potential Useless File	Cleanup
Other directories	-	● History backups of the installation package, patch package, adaptation-layer installation package, and so on ● Temporary path of daily backups ● History trace files ● Backup files during uninstall ● Useless temporary files ● Extra large log files ● Core files.	● Run **rm** to delete useless files. ● Run **> log file name** to clear log files, for example, **> vsftpd.log**. ● The core files indicate the files with the prefix as core in **$iMAP/var/logs**.

(8) After a **Hard disk status refresh interval**, choose **Fault** > **Browse Current Alarm** from the main menu. In the **Filter** window, click **OK**. In the displayed **Browse Current Alarm** window, check whether the high disk usage alarm is cleared.

- If so, the alarm processing is complete.
- If not, go to **2**.

2 The threshold for generating a high disk usage alarm of the U2000 server is specified to a small value.

(1) Log in to the U2000 system monitor client. Choose **Administration** > **Settings** from the main menu. In the displayed **System Monitor Settings** window, click the **Hard Disk Monitor** tab. Check whether the threshold for generating a high disk usage alarm is larger than or equal to 70% (default value).

- If so, go to **3**.
- If not, increase the threshold for generating a high disk usage alarm to 70%, and increase the threshold for alarm clearance to 65% (default value). Then go to **2.2**.

(2) After a **Hard disk status refresh interval**, choose **Fault** > **Browse Current Alarm**. In the **Filter** window, click **OK**. In the displayed **Browse Current Alarm** window, check whether the high disk usage alarm is cleared.

- If so, the alarm processing is complete.
- If not, go to **3**.

3 The disk space is insufficient. Therefore, the U2000 cannot run properly.

Go to **4**.

4 Collect the information about alarm handling, and contact technical support personnel of the Huawei Technologies Co., Ltd..

----End

Related Information

4.6 ALM-34 The Disk Usage Is Too High (Warning)

4.8 ALM-36 The Disk Usage Is Too High (Major)

Description

When the disk or partition usage is larger than the generating threshold for the major severity, the U2000 generates this alarm. When the disk or partition usage is smaller than the clearance threshold for the major severity, the U2000 generates a corresponding cleared alarm.

Attribute

Alarm ID	Alarm Severity	Alarm Type
36	Major	QoS

Parameters

Name	Meaning
Host	Name of the host that generated the alarm.
Operating System	Operating system name of the host that generated the alarm.
Disk	Disk path of the host that generated the alarm.
Threshold	Threshold for generating alarm.
Clearance threshold	Threshold for clearing alarm.
Capacity	Disk capacity.
Usage	Current disk usage.

Impact on the System

The **write** operation of the U2000 service may fail, and a database exception may result.

System Actions

None.

Possible Causes

- There are too many useless disk files.

- The recycle bin is not cleared.
- In Solaris, the swap partition occupies large space. As a result, the log size of the Sybase database is too large.
- The U2000 server has received a large amount of data, including NE alarms, events, and logs. The data is exported from the database to disk files in a short time.
- There are too many temporary data files and backup files.

- The threshold for generating a high disk usage alarm of the U2000 server is specified to a small value.
- The disk space is insufficient. Therefore, the U2000 cannot run properly.

Procedure

1 There are too many useless disk files.

(1) Clear the recycle bin.

Clear the recycle bin. (In SUSE Linux and Solaris, perform this operation through the Xwindows.)

(2) Delete useless disk files from the Windows operating system.

NOTE

If you cannot determine which files can be deleted, contact Huawei technical support engineers.

- In Windows, check for and delete useless files through **Explore** and Table 4-5. When the operations are complete, go to **1.8**.

Table 4-5 Cleaning up disks in Windows

Disk	Directory or File	Potential Useless File	Cleanup
C:	-	Useless temporary files	Use **Explore** to delete useless files and clear the recycle bin.
D:	**%installation path of the NMS%\var\ThresholdExport\FM**	Too many alarm/event log dump files	Reserve the dump files generated on the current day, use **Explore** to delete the other dump files, and clear the recycle bin.

Disk	Directory or File	Potential Useless File	Cleanup
	%installation path of the NMS%\var\ThresholdExport\Log	Too many security/operation/system log dump files	
	%installation path of the NMS%\var\ThresholdExport\Dol	Too many device log dump files	
Other directories	-	● History backups of the installation package, patch package, adaptation-layer installation package, and so on ● Temporary path of daily backups ● History trace files ● Backup files during uninstall ● Useless temporary files ● Extra large log files ● Core files	● Use **Explore** to delete useless files and clear the recycle bin. ● In the DOS environment, run **break > log file name** to clear log files, for example, **break > vsftpd.log**. ● To obtain the location of core files, run **drwtsn32** through the command line interface.

- For SUSE Linux and Solaris, go to **1.3**.

(3) Run **df -k** to check which disks cause high disk usage.

If other locations except for **Disk** in the alarm parameter also has high disk usage but do not generate alarms, you can also clean up them.

(4) Run **cd** to access the directory with high disk usage. Then run **du -k | sort -nr > /tmp/du_k.txt** to query the sizes of all files and subdirectories under this directory. Sort the files and subdirectories, and place them in **du_k.txt**.

(5) Run **more** */tmp/du_k.txt* to view **du_k.txt** and find the subdirectory that causes high disk usage.

(6) Run **cd** to access the subdirectory that causes high disk usage. Then run **ls -l > /tmp/ls_l.txt** to query the sizes of all files and subdirectories under this subdirectory. Sort the files and subdirectories, and place them in **ls_l.txt**.

(7) Run **more /tmp/ls_l.txt** to view **ls_l.txt** and find the subdirectory or file that causes high disk usage. Use this method repeatedly until you find the files that cause high disk usage. Then clean up these files. For details on how to determine and clear useless files, see **Table 4-6**. When the operations are complete, go to **1.8**.

Table 4-6 Cleaning up disks in Solaris and SUSE Linux

Disk	Directory or File	Potential Useless File	Cleanup
/	-	● Useless temporary files ● Extra large log files	● Run **rm** to delete useless files. ● Run **> log file name** to clear log files, for example, **> vsftpd.log**.
/opt	**$installation path of the NMS/var/ThresholdExport/Log**	Too many security/operation/system log dump files	Reserve the dump files generated on the current day, and run **rm** to delete the other dump files.
	$installation path of the NMS/var/ThresholdExport/Dol	Too many device log dump files	Reserve the dump files generated on the current day, and run **rm** to delete the other dump files.

Disk	Directory or File	Potential Useless File	Cleanup

	/opt/sybase/ASE-15_0/install (in Solaris)	● Check whether the log files of the Sybase databases are too large. The name format of database log files is **database instance name.log**, for example, **SYB.log**.
		● In Solaris, run **df -k** to view the record with **Mounted on** as **/tmp** and **Filesystem** as **swap**. Then check whether the disk usage of the swap partition that is mounted to **/tmp** exceeds 50%.
		● Check whether there is the companied **4.4 ALM-102 The Memory Usage Is Too High** or **4.2 ALM-106 The OMC Service Is Terminated Abnormally** alarm. (This is not mandatory.)
			a. Run the following command to clean up Sybase database logs (the following takes SYB.log as an example):
			`#cd /opt/sybase/ASE-15_0/install`
			`#> SYB.log`
			b. If the disk usage of the swap partition that is mounted to **/tmp** exceeds 50%, there may be too many useless files and temporary files in **/tmp**. In this case, run **cd /tmp** to access **/tmp**, then run **ls -l** to query the file information, and finally run **rm** to delete files.

/export/home	**/export/home/omc/var/ThresholdExport/FM**	Too many alarm/event log dump files	Reserve the dump files generated on the current day, and run **rm** to delete the other dump files.

Disk	Directory or File	Potential Useless File	Cleanup
Other directories	-	● History backups of the installation package, patch package, adaptation-layer installation package, and so on ● Temporary path of daily backups ● History trace files ● Backup files during uninstall ● Useless temporary files ● Extra large log files ● Core files.	● Run **rm** to delete useless files. ● Run **> log file name** to clear log files, for example, **> vsftpd.log**. ● The core files indicate the files with the prefix as core in **$iMAP/var/logs**.

(8) After a **Hard disk status refresh interval**, choose **Fault** > **Browse Current Alarm** from the main menu. In the **Filter** window, click **OK**. In the displayed **Browse Current Alarm** window, check whether the high disk usage alarm is cleared.

- If so, the alarm processing is complete.
- If not, go to **2**.

2 The threshold for generating a high disk usage alarm of the U2000 server is specified to a small value.

(1) Log in to the U2000 system monitor client. Choose **Administration** > **Settings** from the main menu. In the displayed **System Monitor Settings** window, click the **Hard Disk Monitor** tab. Check whether the threshold for generating a high disk usage alarm is larger than or equal to 80% (default value).

- If so, go to **3**.
- If not, increase the threshold for generating a high disk usage alarm to 80%, and increase the threshold for alarm clearance to 75% (default value). Then go to **2.2**.

(2) After a **Hard disk status refresh interval**, choose **Fault** > **Browse Current Alarm**. In the **Filter** window, click **OK**. In the displayed **Browse Current Alarm** window, check whether the high disk usage alarm is cleared.

- If so, the alarm processing is complete.
- If not, go to **3**.

3 The disk space is insufficient. Therefore, the U2000 cannot run properly.

Go to **4**.

4 Collect the information about alarm handling, and contact technical support personnel of the Huawei Technologies Co., Ltd..

----End

Related Information

4.6 ALM-34 The Disk Usage Is Too High (Warning)

4.7 ALM-35 The Disk Usage Is Too High (Minor)

4.9 ALM-101 The Disk Usage Is Too High (Critical)

4.9 ALM-101 The Disk Usage Is Too High (Critical)

Description

When the disk or partition usage is larger than the generating threshold for the critical severity, the U2000 generates this alarm. When the disk or partition usage is smaller than the clearance threshold for the critical severity, the U2000 generates a corresponding cleared alarm.

Attribute

Alarm ID	Alarm Severity	Alarm Type
101	Critical	QoS

Parameters

Name	Meaning
Host	Name of the host that generated the alarm.
Operating System	Operating system name of the host that generated the alarm.
Disk	Disk path of the host that generated the alarm.
Threshold	Threshold for generating alarm.
Clearance threshold	Threshold for clearing alarm.
Capacity	Disk capacity.
Usage	Current disk usage.

Impact on the System

The **write** operation of the U2000 service may fail, and a database exception may result.

System Actions

None.

Possible Causes

- There are too many useless disk files.

- The recycle bin is not cleared.
- In Solaris, the swap partition occupies large space. As a result, the log size of the Sybase database is too large.
- The U2000 server has received a large amount of data, including NE alarms, events, and logs. The data is exported from the database to disk files in a short time.
- There are too many temporary data files and backup files.

- The threshold for generating a high disk usage alarm of the U2000 server is specified to a small value.
- The disk space is insufficient. Therefore, the U2000 cannot run properly.

Procedure

1 There are too many useless disk files.

(1) Clear the recycle bin.

Clear the recycle bin. (In SUSE Linux and Solaris, perform this operation through the Xwindows.)

(2) Delete useless disk files from the Windows operating system.

NOTE

If you cannot determine which files can be deleted, contact Huawei technical support engineers.

- In Windows, check for and delete useless files through **Explore** and Table 4-7. When the operations are complete, go to **1.8**.

Table 4-7 Cleaning up disks in Windows

Disk	Directory or File	Potential Useless File	Cleanup
C:	-	Useless temporary files	Use **Explore** to delete useless files and clear the recycle bin.
D:	**%installation path of the NMS%\var\ThresholdExport\FM**	Too many alarm/event log dump files	Reserve the dump files generated on the current day, use **Explore** to delete the other dump files, and clear the recycle bin.

Disk	Directory or File	Potential Useless File	Cleanup
	%installation path of the NMS%\var\ThresholdExport\Log	Too many security/operation/system log dump files	
	%installation path of the NMS%\var\ThresholdExport\Dol	Too many device log dump files	
Other directories	-	● History backups of the installation package, patch package, adaptation-layer installation package, and so on ● Temporary path of daily backups ● History trace files ● Backup files during uninstall ● Useless temporary files ● Extra large log files ● Core files	● Use **Explore** to delete useless files and clear the recycle bin. ● In the DOS environment, run **break > log file name** to clear log files, for example, **break > vsftpd.log**. ● To obtain the location of core files, run **drwtsn32** through the command line interface.

- For SUSE Linux and Solaris, go to **1.3**.

(3) Run **df -k** to check which disks cause high disk usage.

If other locations except for **Disk** in the alarm parameter also has high disk usage but do not generate alarms, you can also clean up them.

(4) Run **cd** to access the directory with high disk usage. Then run **du -k | sort -nr > /tmp/du_k.txt** to query the sizes of all files and subdirectories under this directory. Sort the files and subdirectories, and place them in **du_k.txt**.

(5) Run **more** */tmp/du_k.txt* to view **du_k.txt** and find the subdirectory that causes high disk usage.

(6) Run **cd** to access the subdirectory that causes high disk usage. Then run **ls -l > /tmp/ls_l.txt** to query the sizes of all files and subdirectories under this subdirectory. Sort the files and subdirectories, and place them in **ls_l.txt**.

(7) Run **more /tmp/ls_l.txt** to view **ls_l.txt** and find the subdirectory or file that causes high disk usage. Use this method repeatedly until you find the files that cause high disk usage. Then clean up these files. For details on how to determine and clear useless files, see **Table 4-8**. When the operations are complete, go to **1.8**.

Table 4-8 Cleaning up disks in Solaris and SUSE Linux

Disk	Directory or File	Potential Useless File	Cleanup
/	-	● Useless temporary files ● Extra large log files	● Run **rm** to delete useless files. ● Run **> log file name** to clear log files, for example, **> vsftpd.log**.
/opt	**$installation path of the NMS/var/ThresholdExport/Log**	Too many security/operation/system log dump files	Reserve the dump files generated on the current day, and run **rm** to delete the other dump files.
	$installation path of the NMS/var/ThresholdExport/Dol	Too many device log dump files	Reserve the dump files generated on the current day, and run **rm** to delete the other dump files.

Disk	Directory or File	Potential Useless File	Cleanup

	/opt/sybase/ASE-15_0/install (in Solaris)	● Check whether the log files of the Sybase databases are too large. The name format of database log files is **database instance name.log**, for example, **SYB.log**.
		● In Solaris, run **df -k** to view the record with **Mounted on** as **/tmp** and **Filesystem** as **swap**. Then check whether the disk usage of the swap partition that is mounted to **/tmp** exceeds 50%.
		● Check whether there is the companied **4.4 ALM-102 The Memory Usage Is Too High** or **4.2 ALM-106 The OMC Service Is Terminated Abnormally** alarm. (This is not mandatory.)
			a. Run the following command to clean up Sybase database logs (the following takes SYB.log as an example):
			`#cd /opt/sybase/ASE-15_0/install`
			`#> SYB.log`
			b. If the disk usage of the swap partition that is mounted to **/tmp** exceeds 50%, there may be too many useless files and temporary files in **/tmp**. In this case, run **cd /tmp** to access **/tmp**, then run **ls -l** to query the file information, and finally run **rm** to delete files.

/export/home	**/export/home/omc/var/ThresholdExport/FM**	Too many alarm/event log dump files	Reserve the dump files generated on the current day, and run **rm** to delete the other dump files.

Disk	Directory or File	Potential Useless File	Cleanup
Other directories	-	● History backups of the installation package, patch package, adaptation-layer installation package, and so on ● Temporary path of daily backups ● History trace files ● Backup files during uninstall ● Useless temporary files ● Extra large log files ● Core files.	● Run **rm** to delete useless files. ● Run **> log file name** to clear log files, for example, **> vsftpd.log**. ● The core files indicate the files with the prefix as core in **$iMAP/var/logs**.

(8) After a **Hard disk status refresh interval**, choose **Fault** > **Browse Current Alarm** from the main menu. In the **Filter** window, click **OK**. In the displayed **Browse Current Alarm** window, check whether the high disk usage alarm is cleared.

- If so, the alarm processing is complete.
- If not, go to **2**.

2 The threshold for generating a high disk usage alarm of the U2000 server is specified to a small value.

(1) Log in to the U2000 system monitor client. Choose **Administration** > **Settings** from the main menu. In the displayed **System Monitor Settings** window, click the **Hard Disk Monitor** tab. Check whether the threshold for generating a high disk usage alarm is larger than or equal to 90% (default value).

- If so, go to **3**.
- If not, increase the threshold for generating a high disk usage alarm to 90%, and increase the threshold for alarm clearance to 85% (default value). Then go to **2.2**.

(2) After a **Hard disk status refresh interval**, choose **Fault** > **Browse Current Alarm**. In the **Filter** window, click **OK**. In the displayed **Browse Current Alarm** window, check whether the high disk usage alarm is cleared.

- If so, the alarm processing is complete.
- If not, go to **3**.

3 The disk space is insufficient. Therefore, the U2000 cannot run properly.

Go to **4**.

4 Collect the information about alarm handling, and contact technical support personnel of the Huawei Technologies Co., Ltd..

----End

Related Information

4.6 ALM-34 The Disk Usage Is Too High (Warning)

4.7 ALM-35 The Disk Usage Is Too High (Minor)

4.8 ALM-36 The Disk Usage Is Too High (Major)

4.10 ALM-40 The ESN of the Server Does not Match that in the License File.

Description

The ESN of the U2000 server does not match that in the U2000 license file.

Attribute

Alarm ID	Alarm Severity	Alarm Type
40	Major	Processing error

Parameters

Name	Meaning
Active server	Name of the server that generated the alarm.

Impact on the System

The services or functions controlled by the license are unavailable.

System Actions

None.

Possible Causes

The ESN of the U2000 server does not match that in the U2000 license file.

Procedure

1 Apply for another license or contact technical support personnel of the Huawei Technologies Co., Ltd..

----End

4.11 ALM-42 The Database Usage Is Too High (Warning)

Description

When the database usage is larger than the threshold for the warning severity, the U2000 generates this alarm. When the database usage is smaller than the threshold for the warning severity, this alarm is cleared.

NOTE

- To set the threshold for high database usage alarm. Log in to the U2000 system monitor client. Choose **Administration** > **Settings** from the main menu. In the **System Monitor Settings** dialog box, select the **Database Monitor** tab. And then set the threshold on the **Database Monitor** tab.
- The default threshold for the warning alarm is 85%. If the database usage increases to 85%, a warning alarm is generated. If the disk usage is smaller than 85%, this alarm is cleared.

Attribute

Alarm ID	Alarm Severity	Alarm Type
42	Warning	QoS

Parameters

Name	Meaning
Host	Name of the host that generated the alarm.
Database service	Database service name of the host.
Database	Database name of the host.
Tablespace **NOTE** This parameter is applicable to the Oracle database only.	Database table space name of the host.
Size	Database capacity.
Threshold	Threshold for generating alarm.
Usage	Current database usage.

Impact on the System

If the database usage is too high, the operations associated with the U2000 database may fail. For example, saving the alarm information to the database fails.

System Actions

None.

Possible Causes

- A large number of alarms or events are reported in a short period.
- The threshold of the database usage of the U2000 is specified to a small value.
- The period for U2000 data export/dump or other parameters are set improperly. As a result, the usage of the database associated with the alarm is too high.

Procedure

1 A large number of alarms or events are reported in a short period.

(1) Check whether **Database** in the alarm information is the alarm database.

- If it is the alarm database, go to step **1.2**.
- If it is not the alarm database, go to step **2**.

(2) Log in to the U2000 client. Choose **Fault** > **Browse Current Alarm** from the main menu. In the **Browse Current Alarm** window, check whether a large number of alarms (more than 300 alarms per second) are reported in a short period. Choose **Fault** > **Browse Event Logs** from the main menu. In the **Query Event Logs** window, check whether a large number of events (more than 300 events per second) are reported in a short period.

- If a large number of alarms or events are reported in a short period, go to step **1.3**.
- If a small number of alarms or events are reported in a short period, go to step **2**.

(3) Handle the large number of alarms or events that an NE has reported in a short period.

Set an alarm or event mask rule to mask these alarms or events. In the **Task Management** window, instantly perform the timing task of dumping alarms or events, and identify the cause for these alarms or events.

(4) Log in to the U2000 client. Choose **Fault** > **Browse Current Alarm** from the main menu. In the **Browse Current Alarm** window, check whether the high database usage alarm is cleared.

- If the alarm is cleared, the handling is complete.
- If the alarm is not cleared, go to step **2**.

2 The threshold of the database usage of the U2000 is specified to a small value.

(1) Log in to the U2000 system monitor client. Choose **Administration** > **Settings** from the main menu. In the **System Monitor Settings** dialog box, select the **Database Monitor** tab. Then check whether the threshold for generating a high database usage alarm is proper.

- If the threshold for generating a high database usage alarm is equal to or larger than 85% (default value), go to **3**.
- If the threshold for generating a high database usage alarm is smaller than 85%, increase it to 98%, and then go to **2.2**.

(2) After a **Database status refresh interval**, log in to the U2000 client. Choose **Fault** > **Browse Current Alarm** from the main menu. In the **Filter** window, click **OK**. In the displayed **Browse Current Alarm** window, check whether the high database usage alarm is cleared.

- If the alarm is cleared successfully, the operation ends.

- If the alarm is not cleared, go to **3**.

3 The period for U2000 data export/dump or other parameters are set improperly. As a result, the usage of the database associated with the alarm is too high.

(1) Log in to the U2000 client, and then choose **Fault** > **Query Alarm Log Statistics** from the main menu.

(2) In the **Statistic Filter** window, select the **Basic Setting** tab. In **Occurrence Time Range**, change the value of **Latest** to **90**, and then click **OK** to collect statistics on the history alarm records generated in recent 90 days.

(3) In the displayed **Confirm** dialog box, click **Yes**.

- If there are a large number of history alarm records, it indicates that the data export/dump period or other parameters may be set improperly. As a result, the amount of data written to the database is larger than that of dumped data in a short time. In this case, go to **3.4**.
- If there are not a large number of history alarm records, go to **4**.

(4) Log in to the U2000 client. Choose **Administration** > **Task Schedule** > **Task Management** from the main menu. In the navigation tree on the left of the **Task Management** window, choose **Task Type** > **Database Capacity Management** > **Alarm/Event Log Dump**. In the **Task Management** window, right-click **Alarm/Event Log Dump** task in the task list and choose **Run At Once**.

(5) In the **Task Management** window, right-click **Alarm/Event Log Dump** task in the task list and choose **Attribute**. In the **Attribute** dialog box, select the **Extended Parameters** tab. Change the value of **Storage period in database(day)** to a smaller value, for example, 30 days.

(6) After a Database status refresh interval, choose **Fault** > **Browse Current Alarm** from the main menu. In the **Filter** window, click **OK**. In the displayed **Browse Current Alarm** window, check whether the high database usage alarm is cleared.

- If the alarm is cleared successfully, the operation ends.
- If the alarm is not cleared, go to **4**.

4 Collect the information about alarm handling, and contact technical support personnel of the Huawei Technologies Co., Ltd..

----End

Related Information

4.12 ALM-43 The Database Usage Is Too High (Minor)

4.13 ALM-44 The Database Usage Is Too High (Major)

4.14 ALM-103 The Database Usage Is Too High (Critical)

4.12 ALM-43 The Database Usage Is Too High (Minor)

Description

When the database usage is larger than the threshold for the minor severity, the U2000 generates this alarm. When the database usage is smaller than the threshold for the minor severity, the U2000 generates a corresponding cleared alarm.

NOTE

- To set the threshold for high database usage alarm. Log in to the U2000 system monitor client. Choose **Administration** > **Settings** from the main menu. In the **System Monitor Settings** dialog box, select the **Database Monitor** tab. And then set the threshold on the **Database Monitor** tab.
- The default threshold for the minor alarm is 90%. If the database usage increases to 90%, a minor alarm is generated. If the disk usage is smaller than 90%, this alarm is cleared.

Attribute

Alarm ID	Alarm Severity	Alarm Type
43	Minor	QoS

Parameters

Name	Meaning
Host	Name of the host that generated the alarm.
Database service	Database service name of the host.
Database	Database name of the host.
Tablespace **NOTE** This parameter is applicable to the Oracle database only.	Database table space name of the host.
Size	Database capacity.
Threshold	Threshold for generating alarm.
Usage	Current database usage.

Impact on the System

If the database usage is too high, the operations associated with the U2000 database may fail. For example, saving the alarm information to the database fails.

System Actions

None.

Possible Causes

- A large number of alarms or events are reported in a short period.
- The threshold of the database usage of the U2000 is specified to a small value.

- The period for U2000 data export/dump or other parameters are set improperly. As a result, the usage of the database associated with the alarm is too high.

Procedure

1 A large number of alarms or events are reported in a short period.

(1) Check whether **Database** in the alarm information is the alarm database.

- If it is the alarm database, go to step **1.2**.
- If it is not the alarm database, go to step **2**.

(2) Log in to the U2000 client. Choose **Fault** > **Browse Current Alarm** from the main menu. In the **Browse Current Alarm** window, check whether a large number of alarms (more than 300 alarms per second) are reported in a short period. Choose **Fault** > **Browse Event Logs** from the main menu. In the **Query Event Logs** window, check whether a large number of events (more than 300 events per second) are reported in a short period.

- If a large number of alarms or events are reported in a short period, go to step **1.3**.
- If a small number of alarms or events are reported in a short period, go to step **2**.

(3) Handle the large number of alarms or events that an NE has reported in a short period.

Set an alarm or event mask rule to mask these alarms or events. In the **Task Management** window, instantly perform the timing task of dumping alarms or events, and identify the cause for these alarms or events.

(4) Log in to the U2000 client. Choose **Fault** > **Browse Current Alarm** from the main menu. In the **Browse Current Alarm** window, check whether the high database usage alarm is cleared.

- If the alarm is cleared, the handling is complete.
- If the alarm is not cleared, go to step **2**.

2 The threshold of the database usage of the U2000 is specified to a small value.

(1) Log in to the U2000 system monitor client. Choose **Administration** > **Settings** from the main menu. In the **System Monitor Settings** dialog box, select the **Database Monitor** tab. Then check whether the threshold for generating a high database usage alarm is proper.

- If the threshold for generating a high database usage alarm is equal to or larger than 90% (default value), go to **3**.
- If the threshold for generating a high database usage alarm is smaller than 90%, increase it to 90%, and then go to **2.2**.

(2) After a **Database status refresh interval**, log in to the U2000 client. Choose **Fault** > **Browse Current Alarm** from the main menu. In the **Filter** window, click **OK**. In the displayed **Browse Current Alarm** window, check whether the high database usage alarm is cleared.

- If the alarm is cleared successfully, the operation ends.
- If the alarm is not cleared, go to **3**.

3 The period for U2000 data export/dump or other parameters are set improperly. As a result, the usage of the database associated with the alarm is too high.

(1) Log in to the U2000 client, and then choose **Fault** > **Query Alarm Log Statistics** from the main menu.

(2) In the **Statistic Filter** window, select the **Basic Setting** tab. In **Occurrence Time Range**, change the value of **Latest** to **90**, and then click **OK** to collect statistics on the history alarm records generated in recent 90 days.

(3) In the displayed **Confirm** dialog box, click **Yes**.

- If there are a large number of history alarm records, it indicates that the data export/ dump period or other parameters may be set improperly. As a result, the amount of data written to the database is larger than that of dumped data in a short time. In this case, go to **3.4**.
- If there are not a large number of history alarm records, go to **4**.

(4) Log in to the U2000 client. Choose **Administration** > **Task Schedule** > **Task Management** from the main menu. In the navigation tree on the left of the **Task Management** window, choose **Task Type** > **Database Capacity Management** > **Alarm/ Event Log Dump**. In the **Task Management** window, right-click **Alarm/Event Log Dump** task in the task list and choose **Run At Once**.

(5) In the **Task Management** window, right-click **Alarm/Event Log Dump** task in the task list and choose **Attribute**. In the **Attribute** dialog box, select the **Extended Parameters** tab. Change the value of **Storage period in database(day)** to a smaller value, for example, 30 days.

(6) After a Database status refresh interval, choose **Fault** > **Browse Current Alarm** from the main menu. In the **Filter** window, click **OK**. In the displayed **Browse Current Alarm** window, check whether the high database usage alarm is cleared.

- If the alarm is cleared successfully, the operation ends.
- If the alarm is not cleared, go to **4**.

4 Collect the information about alarm handling, and contact technical support personnel of the Huawei Technologies Co., Ltd..

----End

Related Information

4.11 ALM-42 The Database Usage Is Too High (Warning)

4.13 ALM-44 The Database Usage Is Too High (Major)

4.14 ALM-103 The Database Usage Is Too High (Critical)

4.13 ALM-44 The Database Usage Is Too High (Major)

Description

When the database usage is larger than the threshold for the major severity, the U2000 generates this alarm. When the database usage is smaller than the threshold for the major severity, the U2000 generates a corresponding cleared alarm.

NOTE

- To set the threshold for high database usage alarm. Log in to the U2000 system monitor client. Choose **Administration** > **Settings** from the main menu. In the **System Monitor Settings** dialog box, select the **Database Monitor** tab. And then set the threshold on the **Database Monitor** tab.
- The default threshold for the major alarm is 95%. If the database usage increases to 95%, a major alarm is generated. If the disk usage is smaller than 95%, this alarm is cleared.

Attribute

Alarm ID	Alarm Severity	Alarm Type
44	Major	QoS

Parameters

Name	Meaning
Host	Name of the host that generated the alarm.
Database service	Database service name of the host.
Database	Database name of the host.
Tablespace **NOTE** This parameter is applicable to the Oracle database only.	Database table space name of the host.
Size	Database capacity.
Threshold	Threshold for generating alarm.
Usage	Current database usage.

Impact on the System

If the database usage is too high, the operations associated with the U2000 database may fail. For example, saving the alarm information to the database fails.

System Actions

None.

Possible Causes

- A large number of alarms or events are reported in a short period.
- The threshold of the database usage of the U2000 is specified to a small value.

- The period for U2000 data export/dump or other parameters are set improperly. As a result, the usage of the database associated with the alarm is too high.

Procedure

1 A large number of alarms or events are reported in a short period.

(1) Check whether **Database** in the alarm information is the alarm database.

- If it is the alarm database, go to step **1.2**.
- If it is not the alarm database, go to step **2**.

(2) Log in to the U2000 client. Choose **Fault** > **Browse Current Alarm** from the main menu. In the **Browse Current Alarm** window, check whether a large number of alarms (more than 300 alarms per second) are reported in a short period. Choose **Fault** > **Browse Event Logs** from the main menu. In the **Query Event Logs** window, check whether a large number of events (more than 300 events per second) are reported in a short period.

- If a large number of alarms or events are reported in a short period, go to step **1.3**.
- If a small number of alarms or events are reported in a short period, go to step **2**.

(3) Handle the large number of alarms or events that an NE has reported in a short period.

Set an alarm or event mask rule to mask these alarms or events. In the **Task Management** window, instantly perform the timing task of dumping alarms or events, and identify the cause for these alarms or events.

(4) Log in to the U2000 client. Choose **Fault** > **Browse Current Alarm** from the main menu. In the **Browse Current Alarm** window, check whether the high database usage alarm is cleared.

- If the alarm is cleared, the handling is complete.
- If the alarm is not cleared, go to step **2**.

2 The threshold of the database usage of the U2000 is specified to a small value.

(1) Log in to the U2000 system monitor client. Choose **Administration** > **Settings** from the main menu. In the **System Monitor Settings** dialog box, select the **Database Monitor** tab. Then check whether the threshold for generating a high database usage alarm is proper.

- If the threshold for generating a high database usage alarm is equal to or larger than 95% (default value), go to **3**.
- If the threshold for generating a high database usage alarm is smaller than 95%, increase it to 95%, and then go to **2.2**.

(2) After a **Database status refresh interval**, log in to the U2000 client. Choose **Fault** > **Browse Current Alarm** from the main menu. In the **Filter** window, click **OK**. In the displayed **Browse Current Alarm** window, check whether the high database usage alarm is cleared.

- If the alarm is cleared successfully, the operation ends.
- If the alarm is not cleared, go to **3**.

3 The period for U2000 data export/dump or other parameters are set improperly. As a result, the usage of the database associated with the alarm is too high.

(1) Log in to the U2000 client, and then choose **Fault** > **Query Alarm Log Statistics** from the main menu.

(2) In the **Statistic Filter** window, select the **Basic Setting** tab. In **Occurrence Time Range**, change the value of **Latest** to **90**, and then click **OK** to collect statistics on the history alarm records generated in recent 90 days.

(3) In the displayed **Confirm** dialog box, click **Yes**.

- If there are a large number of history alarm records, it indicates that the data export/ dump period or other parameters may be set improperly. As a result, the amount of data written to the database is larger than that of dumped data in a short time. In this case, go to **3.4**.
- If there are not a large number of history alarm records, go to **4**.

(4) Log in to the U2000 client. Choose **Administration** > **Task Schedule** > **Task Management** from the main menu. In the navigation tree on the left of the **Task Management** window, choose **Task Type** > **Database Capacity Management** > **Alarm/ Event Log Dump**. In the **Task Management** window, right-click **Alarm/Event Log Dump** task in the task list and choose **Run At Once**.

(5) In the **Task Management** window, right-click **Alarm/Event Log Dump** task in the task list and choose **Attribute**. In the **Attribute** dialog box, select the **Extended Parameters** tab. Change the value of **Storage period in database(day)** to a smaller value, for example, 30 days.

(6) After a Database status refresh interval, choose **Fault** > **Browse Current Alarm** from the main menu. In the **Filter** window, click **OK**. In the displayed **Browse Current Alarm** window, check whether the high database usage alarm is cleared.

- If the alarm is cleared successfully, the operation ends.
- If the alarm is not cleared, go to **4**.

4 Collect the information about alarm handling, and contact technical support personnel of the Huawei Technologies Co., Ltd..

----End

Related Information

4.11 ALM-42 The Database Usage Is Too High (Warning)

4.12 ALM-43 The Database Usage Is Too High (Minor)

4.14 ALM-103 The Database Usage Is Too High (Critical)

4.14 ALM-103 The Database Usage Is Too High (Critical)

Description

When the database usage is larger than the threshold for the critical severity, the U2000 generates this alarm. When the database usage is smaller than the threshold for the critical severity, this alarm is cleared.

NOTE

- To set the threshold for high database usage alarm. Log in to the U2000 system monitor client. Choose **Administration** > **Settings** from the main menu. In the **System Monitor Settings** dialog box, select the **Database Monitor** tab. And then set the threshold on the **Database Monitor** tab.
- The default threshold for the critical alarm is 98%. If the database usage increases to 98%, a critical alarm is generated. If the disk usage is smaller than 98%, this alarm is cleared.

Attribute

Alarm ID	Alarm Severity	Alarm Type
103	Critical	QoS

Parameters

Name	Meaning
Host	Name of the host that generated the alarm.
Database service	Database service name of the host.
Database	Database name of the host.
Tablespace **NOTE** This parameter is applicable to the Oracle database only.	Database table space name of the host.
Size	Database capacity.
Threshold	Threshold for generating alarm.
Usage	Current database usage.

Impact on the System

If the database usage is too high, the operations associated with the U2000 database may fail. For example, saving the alarm information to the database fails.

System Actions

None.

Possible Causes

- A large number of alarms or events are reported in a short period.
- The threshold of the database usage of the U2000 is specified to a small value.

- The period for U2000 data export/dump or other parameters are set improperly. As a result, the usage of the database associated with the alarm is too high.

Procedure

1 A large number of alarms or events are reported in a short period.

(1) Check whether **Database** in the alarm information is the alarm database.

- If it is the alarm database, go to step **1.2**.
- If it is not the alarm database, go to step **2**.

(2) Log in to the U2000 client. Choose **Fault** > **Browse Current Alarm** from the main menu. In the **Browse Current Alarm** window, check whether a large number of alarms (more than 300 alarms per second) are reported in a short period. Choose **Fault** > **Browse Event Logs** from the main menu. In the **Query Event Logs** window, check whether a large number of events (more than 300 events per second) are reported in a short period.

- If a large number of alarms or events are reported in a short period, go to step **1.3**.
- If a small number of alarms or events are reported in a short period, go to step **2**.

(3) Handle the large number of alarms or events that an NE has reported in a short period.

Set an alarm or event mask rule to mask these alarms or events. In the **Task Management** window, instantly perform the timing task of dumping alarms or events, and identify the cause for these alarms or events.

(4) Log in to the U2000 client. Choose **Fault** > **Browse Current Alarm** from the main menu. In the **Browse Current Alarm** window, check whether the high database usage alarm is cleared.

- If the alarm is cleared, the handling is complete.
- If the alarm is not cleared, go to step **2**.

2 The threshold of the database usage of the U2000 is specified to a small value.

(1) Log in to the U2000 system monitor client. Choose **Administration** > **Settings** from the main menu. In the **System Monitor Settings** dialog box, select the **Database Monitor** tab. Then check whether the threshold for generating a high database usage alarm is proper.

- If the threshold for generating a high database usage alarm is equal to or larger than 98% (default value), go to **3**.
- If the threshold for generating a high database usage alarm is smaller than 98%, increase it to 98%, and then go to **2.2**.

(2) After a **Database status refresh interval**, log in to the U2000 client. Choose **Fault** > **Browse Current Alarm** from the main menu. In the **Filter** window, click **OK**. In the displayed **Browse Current Alarm** window, check whether the high database usage alarm is cleared.

- If the alarm is cleared successfully, the operation ends.
- If the alarm is not cleared, go to **3**.

3 The period for U2000 data export/dump or other parameters are set improperly. As a result, the usage of the database associated with the alarm is too high.

(1) Log in to the U2000 client, and then choose **Fault** > **Query Alarm Log Statistics** from the main menu.

(2) In the **Statistic Filter** window, select the **Basic Setting** tab. In **Occurrence Time Range**, change the value of **Latest** to **90**, and then click **OK** to collect statistics on the history alarm records generated in recent 90 days.

(3) In the displayed **Confirm** dialog box, click **Yes**.

- If there are a large number of history alarm records, it indicates that the data export/dump period or other parameters may be set improperly. As a result, the amount of data written to the database is larger than that of dumped data in a short time. In this case, go to **3.4**.
- If there are not a large number of history alarm records, go to **4**.

(4) Log in to the U2000 client. Choose **Administration** > **Task Schedule** > **Task Management** from the main menu. In the navigation tree on the left of the **Task Management** window, choose **Task Type** > **Database Capacity Management** > **Alarm/Event Log Dump**. In the **Task Management** window, right-click **Alarm/Event Log Dump** task in the task list and choose **Run At Once**.

(5) In the **Task Management** window, right-click **Alarm/Event Log Dump** task in the task list and choose **Attribute**. In the **Attribute** dialog box, select the **Extended Parameters** tab. Change the value of **Storage period in database(day)** to a smaller value, for example, 30 days.

(6) After a **Database status refresh interval**, choose **Fault** > **Browse Current Alarm** from the main menu. In the **Filter** window, click **OK**. In the displayed **Browse Current Alarm** window, check whether the high database usage alarm is cleared.

- If the alarm is cleared successfully, the operation ends.
- If the alarm is not cleared, go to **4**.

4 Collect the information about alarm handling, and contact technical support personnel of the Huawei Technologies Co., Ltd..

----End

Related Information

4.11 ALM-42 The Database Usage Is Too High (Warning)

4.12 ALM-43 The Database Usage Is Too High (Minor)

4.13 ALM-44 The Database Usage Is Too High (Major)

4.15 ALM-130 The Alarm Report Buffering Blocked

Description

If the buffer capacity for alarm reporting reaches the upper limit, the alarm report buffering is blocked. In this case, the ALM-130 alarm is generated. If the buffer capacity for alarm reporting is smaller than the upper limit, the alarm report buffering is unblocked. In this case, the ALM-130 alarm is cleared.

Attribute

Alarm ID	Alarm Severity	Alarm Type
130	Major	QoS

Impact on the System

The alarms reporting are delayed. A part of alarms cannot be displayed on the client and the U2000 in time.

System Actions

None.

Possible Causes

- Certain NEs are exceptional; therefore, they report a large number of alarms in a short period.
- Many correlation rules are set; therefore, the system analyzes them slowly.

Procedure

1. Choose **Fault** > **Settings** > **Correlation** from the main menu. In the **Correlation** window, check whether the alarm correlation rule is already set.
   - If the alarm correlation rule is already set, go to **3**.
   - If the alarm correlation rule is not set, go to **2**.
2. Choose **Fault** > **Browse Current Alarm** or **Fault** > **Browse Event Logs** from the main menu, check whether a NE reports alarms or events frequently.
   - If the NE exists, go to **4**.
   - If the NE does not exist, go to **6**.
3. Choose **Fault** > **Settings** > **Correlation** from the main menu. In the **Correlation** window, disable the existing correlation rule. Go to **5**.
4. Choose **Fault** > **Settings** > **Mask Rule** from the main menu. In the **Mask Rule** window, set the mask rules to mask alarms and events of the NE that reports alarms or events frequently. Go to **5**.
5. Wait for 10 minutes. After that, check whether the alarm is cleared.
   - If the alarm is cleared, the fault is successfully removed.
   - If the alarm is not cleared, go to **6**.
6. Collect the information about alarm handling, and contact technical support personnel of the Huawei Technologies Co., Ltd..

----End

4.16 ALM-47 Memory Usage of Service Is Too High

Description

If the memory usage of service reaches the preset threshold, the alarm is generated. If the memory usage of service is smaller than the preset threshold, the alarm is cleared.

Attribute

Alarm ID	Alarm Severity	Alarm Type
47	Major	QoS

Parameters

Name	Meaning
Host	Name of the host that generated the alarm.
Operating System	Operating system name of the host that generated the alarm.
Service name	Service name of the host that generated the alarm.

Impact on the System

The response speed of the U2000 server is low.

System Actions

None.

Possible Causes

- Services are busy; therefore, the memory usage increases.
- A program error occurs.
- The threshold for the memory usage of service is small.

Procedure

1. Services are busy; therefore, the memory usage increases.

   When the service processing is complete, check whether the memory usage of service decreases.

   - If the memory usage of service decreases, the alarm is cleared, and the operation ends.
   - If the memory usage of service does not decrease, go to **5**.

2. A program error occurs.

- If the service processing is normal, go to **3**.
- If the service processing is abnormal (for example, the memory usage keeps increasing), go to **5**.

3 The threshold for the memory usage of service is small.

In the corresponding configuration file **%installation path of the NMS%\etc\conf*svc.xml (Windows)** or **$installation path of the NMS/etc/conf/*svc.xml (Solaris and SUSE Linux)**, increase the value of vm_threshold by 10%. Run the following command and then go to **4**.

- In Solaris and SUSE Linux, please run:

  #**SettingTool -cmd import *svc.xml**

  #**svc_adm -cmd reload -type sac**

- In Windows, please run:

  >**SettingTool -cmd import *svc.xml**

  >**svc_adm -cmd reload -type sac**

NOTE

If the **vm_threshold** is not present in the configuration file, please contact technical support personnel of the Huawei Technologies Co., Ltd..

4 Restart the U2000 service. For the corrective commands, see the *U2000 Administrator Guide*.

- If the alarm is cleared successfully, the operation ends.
- If the alarm is not cleared, go to **5**.

5 Collect the information about alarm handling, and contact technical support personnel of the Huawei Technologies Co., Ltd..

----End

Related Information

4.1 ALM-100 The CPU Usage Is High

4.4 ALM-102 The Memory Usage Is Too High

4.17 ALM-50 Task execution failure alarm

Description

Executing the integrated task management task failed.

Attribute

Alarm ID	Alarm Severity	Alarm Type
50	Minor	QoS

Parameters

Name	Meaning
Task name	Name of the task failing to be executed.
Execution result	Task execution result, for example `Task processing error or failure`.
Result information	Possible causes for an execution result.

Impact on the System

None.

System Actions

None.

Possible Causes

- The service corresponding to the task is exceptional.
- The tasks of alarm/event overflow dump and alarm/event log dump are executed at the same time.

Procedure

1. If the task cannot be started, check whether the corresponding service of the task is running normally in the **System Monitor Browser** window.

   For example, if the **Alarm Synchronization** task fails, check whether the state of **FaultService** is **Running** in the **System Monitor Browser** window.

   - If the service is started successfully, perform 2.
   - If the service is not started, perform 3.

2. In the **Task Management** window, check whether the tasks of alarm/event overflow dump and alarm/event log dump are executed at the same time.

   Assume that the start time of the task of alarm/event overflow dump is 2007-01-01 09:00:00 and that the start time of the task of alarm/event log dump is 2007-01-01 10:00:00. The task of alarm/event log dump is executed once a day, whereas the task of alarm/event overflow dump is executed every ten minutes. Therefore, both tasks were executed on 2007-01-01 10:00:00.

   - If the two tasks are executed at the same time, change the task start time to ensure that the two tasks are executed at different time. If the alarm still exists, perform 3; otherwise, the handling is complete.
   - If the two tasks are executed at the different time, perform 3.

3. Collect the information about alarm handling, and contact technical support personnel of the Huawei Technologies Co., Ltd..

----End

4.18 ALM-116 The Primary Server Cannot Communicate with the Secondary Server

Description

The primary server cannot communicate with the secondary server. The primary server fails to detect the secondary server.

Attribute

Alarm ID	Alarm Severity	Alarm Type
116	Critical	Communication system

Impact on the System

None.

System Actions

None.

Possible Causes

- The ResourceMonitor process of the secondary server is not started.
- The network is faulty.

Procedure

1 The ResourceMonitor process of the secondary server is not started.

(1) Log in to the secondary server, and then run the following command:

daem_ps | grep ResourceMonitor

If the running is normal, the information of the ResourceMonitor and ResourceMonitorDeploy processes is displayed.

```
root  7529     1   0   Dec 15 ?           0:00 ./ResourceMonitorDeploy -cmd
start -ipaddr 10.71.156.70
root  7530  7529   0   Dec 15 ?           7:24 ./ResourceMonitor -cmd start -
ipaddr 10.71.156.70 -port 31021 -logpath /space/V
```

- If these two processes are displayed, go to **2**.
- If these two processes are not displayed, it indicates that the ResourceMonitor process is not started or exits abnormally.

(2) Log in to the secondary server and check whether the ResourceMonitor process is started successfully. Run the following commands:

start_daem

daem_ps | grep ResourceMonitor

- If the ResourceMonitor process is started successfully and the alarm is cleared, the operation ends.
- If the ResourceMonitor process is started successfully but the alarm is not cleared, go to **2**.
- If the ResourceMonitor process is not started, go to **3**.

2 The network is faulty.

(1) Log in to the primary server, and then run the following command:

ping IP address of the secondary server

- If running the command succeeds, the cause for the alarm may be that the ResourceMonitor process is faulty. In this case, go to **3**.
- If running the command fails, the cause for the alarm may be that the network is faulty.

(2) Check that the hardware is working properly. For example, check that the network cable is properly connected or that the switch is working normally.

(3) Run the following command to check whether the network is working properly:

ping IP address of the secondary server

- If the alarm is not cleared, go to **3**.
- If the alarm is cleared, the operation ends.

3 Collect the information about alarm handling, and contact technical support personnel of the Huawei Technologies Co., Ltd..

----End

4.19 ALM-121 Sending Remote Notification Message Failed

Description

The remote notification client fails to send short messages.

Attribute

Alarm ID	Alarm Severity	Alarm Type
121	Major	Processing error

Impact on the System

The specified user fails to receive remote notification short messages.

System Actions

None.

Possible Causes

The communication parameters are incorrect.

Procedure

1. Choose **Fault** > **Settings** > **Remote Notification** from the main menu. In the **Remote Notification** window, check whether the remote notification rule is set and enabled.
   - If it is already set and enabled, go to **2**.
   - If it is not set and enabled, go to **3**.
2. In the **Remote Notification** window, check whether SMS number is correct in the remote notification rule.
   - If it is incorrect, change it to the correct number, and the operation ends.
   - If it is correct, go to **3**.
3. Log in to the remote notification client. Choose **Settings** > **Communication Parameter** from the main menu, and check whether communication parameter is set.
   - If it is already set, go to **5**.
   - If it is not set, go to **4**.
4. Choose **Add**. Set the communication parameter, and then select **Enable**.
5. In the **Remote Notification** window, choose **Settings** > **Communication Parameter** from the main menu. Select an enabled communication parameter, and then click **Modify**. In the **Modify Notification Device Communication Settings** window, click the **Communication Settings** tab. In the **Send Point** area, click **Test on Server** or **Test on Client**.
   - If the test succeeds, the operation ends.
   - If the test fails, go to **6**.
6. Collect the information about alarm handling, and contact technical support personnel of the Huawei Technologies Co., Ltd..

----End

4.20 ALM-117 Avalanche Alarm

Description

According to the alarm/event frequency analysis rule, when the number of an alarm/event generated in the specified **Time range** is larger than the **Alarm account**, the alarm is generated. When the number of an alarms/event generated in the specified **Time range** is smaller than the **Alarm account**, this alarm is cleared.

NOTE

To set the alarm/event frequency analysis rule, choose **Fault** > **Settings** > **Correlation** from the main menu. Select the **Alarm/Event Frequency Analysis** tab, click **Add** to set the alarm/event name, time range, alarm count and handling policy.

Attribute

Alarm ID	Alarm Severity	Alarm Type
117	Major	Processing error

Parameters

Name	Meaning
Alarm name	Name of the alarm that causes an avalanche alarm.
NE name	Name of the NE that generates an avalanche alarm.
Equipment alarm serial number	Serial number of the root alarm that causes an avalanche alarm.
Location information	Location information about the root alarm that causes an avalanche alarm.

Impact on the System

The alarm processing efficiency of the U2000 server is affected.

System Actions

None.

Possible Causes

- The ratio of **Alarm account** to **Time range** in the frequency analysis rule for avalanche alarm is too small.
- Certain NEs are exceptional; therefore, they report a large number of alarms in a short period.

Procedure

1. Check whether the avalanche alarm is generated before the fault service is started.

   Log in to the U2000 system monitor client. On the **Service Monitor** tab, view the start time of **Fault Process**.

   - If the alarm is generated before the fault service is started, select this alarm from the current alarm, and then click **Clear**, the operation ends.
   - If the is generated after the fault service is started, go to **2**.

2. The ratio of **Alarm account** to **Time range** in the frequency analysis rule for avalanche alarm is too small.

   Log in to the U2000 client. Choose **Fault** > **Settings** > **Correlation** from the main menu. On the **Alarm/Event Frequency Analysis** tab, view the triggering condition of the rule that is consistent with the alarm name described in the avalanche alarm location information.

   - If the ratio of **Alarm account** to **Time range** is too small (for example, 10 alarms per second), change time range and alarm count to proper values, and the operation ends.
   - If the ratio of **Alarm account** to **Time range** is proper, go to **3**.

3. Certain NEs are exceptional; therefore, they report a large number of alarms in a short period.

   Choose **Fault** > **Settings** > **Mask Rule**. In the **Mask Rule** window, set mask rules to mask the frequently reported alarms.

- If the avalanche alarm is cleared ten minutes later, the operation ends. When the NE debugging is complete, cancel the mask rules.
- If the avalanche alarm is not cleared ten minutes later, go to 4.

4 Collect the information about alarm handling, and contact technical support personnel of the Huawei Technologies Co., Ltd..

----End

4.21 ALM-120 The number of records in the database table has reached the threshold

Description

If the usage of a table in the database on the NMS server exceeds the threshold, this alarm is generated.

Attribute

Alarm ID	Alarm Severity	Alarm Type
120	Minor	QoS

Parameters

Name	Meaning
Server name	Name of the server that generates an alarm.
Database name	Name of the database on the server.
Table name	Name of the table whose usage exceeds the threshold.

Impact on the System

None.

System Actions

The U2000 automatically dumps data.

Possible Causes

- There is a large amount of temporary data.
- The specified threshold is too small.

Procedure

1 There is a large amount of temporary data.

(1) Log in to the U2000 client.

(2) Choose **Fault** > **Browse Current Alarm** from the main menu.

(3) In the **Filter** window, click **OK**.

(4) In the **Browse Current Alarm** window, view **First Occurrence Time** of the alarm.

Check whether the following condition is met: The alarm is not consecutively generated, and is automatically cleared in 30 minutes. In addition, the alarm is seldom generated. It is generated once each day at most.

Processing method:

- If the condition is met, it indicates that there is a large amount of temporary data. You do not need to process the alarm. The alarm processing is complete so far.
- If the condition is not met, go to **2**.

2 Increase the threshold of the used database space.

(1) Log in to the U2000 client.

(2) Choose **Administration** > **Task Schedule** > **Task Management** from the main menu.

(3) In the navigation tree on the left of the **Task Management** tab, choose **Task Type** > **Overflow Dump** > **Alarm Overflow Dump** and **Task Type** > **Overflow Dump** > **Event Overflow Dump**. In the right area, double-click the **Alarm Overflow Dump** and **Event Overflow Dump** tasks.

(4) In the **Attribute** dialog box, click the **Extened Parameters** tab, and then increase **Record Threshold-crossing Value**.

3 Collect the information about alarm handling, and contact technical support personnel of the Huawei Technologies Co., Ltd..

----End

4.22 ALM-119 Alarm of the Switchover to the Slave Syslog Server

Description

If services are switched to the slave syslog server after connection to the master syslog server fails, this alarm is generated. If services are switched back to the master syslog server after connection to the master syslog server succeeds, this alarm is cleared.

Attribute

Alarm ID	Alarm Severity	Alarm Type
119	Major	Environment system

Parameters

Name	Meaning
Master server IP address	IP address of the master syslog server.
Master server port	Port of the master syslog server.
Slave server IP address	IP address of the slave syslog server.
Slave server port	Port of the slave syslog server.

Impact on the System

Logs delivered through the Syslog protocol are then forwarded to the slave syslog server instead of the master syslog server.

System Actions

After the U2000 fails to connect to the master syslog server, services are switched to the slave syslog server.

Possible Causes

- The master syslog server is not running.
- The network connection of the master syslog server is not correct.

Procedure

1 The master syslog server is not running.

Check whether the master syslog server is running normally.

- If the master syslog server is not running, start it, and the operation ends.
- If the master syslog server is running normally, go to **2**.

NOTE

The syslog server is a third-party server. For details on how to check whether it is running normally and whether it is started, see the relevant description of the third-party syslog server.

2 The network connection of the master syslog server is not correct.

Check whether the network connection of the master syslog server is correct.

- If the network connection is incorrect, rectify the network fault. The operation ends.
- If the network connection is correct, go to **3**.

3 Collect the information about alarm handling, and contact technical support personnel of the Huawei Technologies Co., Ltd..

----End

4.23 ALM-118 Alarm of the Failure to Connect the Master and Slave Syslog Servers

Description

If connecting to the master and slave syslog servers fails, this alarm is generated. If connecting to the master or slave syslog server succeeds, the alarm is cleared.

Attribute

Alarm ID	Alarm Severity	Alarm Type
118	Major	Environment system

Parameters

Name	Meaning
Master server IP address	IP address of the master syslog server.
Master server port	Port of the master syslog server.
Slave server IP address	IP address of the slave syslog server.
Slave server port	Port of the slave syslog server.

Impact on the System

The Syslog protocol cannot be used to forward logs. Otherwise, both the master and slave syslog servers fail to receive logs, and the logs to be forwarded are increasing.

System Actions

None.

Possible Causes

- The master and slave syslog servers are not running.
- The network connections of the master and slave syslog servers are not correct.

Procedure

1 The master and slave syslog servers are not running.

Check whether the master and slave syslog servers are running normally.

- If the master and slave syslog servers are not running, start them, and the operation ends.
- If the master and slave syslog servers are running normally, go to **2**.

NOTE

The syslog server is a third-party server. For details on how to check whether it is running normally and whether it is started, see the relevant description of the third-party syslog server.

2 The network connections of the master and slave syslog servers are not correct.

Check whether the network connections of the master and slave syslog servers are correct.

- If the network connections are incorrect, rectify the network faults. The operation ends.
- If the network connections are correct, go to 3.

3 Collect the information about alarm handling, and contact technical support personnel of the Huawei Technologies Co., Ltd..

----End

4.24 ALM-296 The NE Capacity Reached the Threshold Alarm

Description

If the number of accessed NEs on the U2000 reaches the threshold specified in the license, this alarm is generated. If the number of accessed NEs is smaller than the threshold specified in the license, this alarm is cleared.

NOTE

You can set the NE capacity threshold in the license by choosing **Administration** > **Settings** > **NE License Alert** from the main menu.

Attribute

Alarm ID	Alarm Severity	Alarm Type
296	Critical	Processing error

Impact on the System

A message is displayed, prompting that the NE capacity has reached the threshold and that you need to apply for a new license to increase the NE capacity. Functions are not affected.

System Actions

None.

Possible Causes

- The NE capacity threshold for generating an alarm is small.
- The NE capacity is small.

Procedure

1. Choose **Administration** > **Settings** > **NE License Alert** from the main menu in the client to check whether the alarm threshold for licenses is too low.
   - If the alarm threshold of license is too low, go to **3**.
   - If the alarm threshold of license is not low, go to **2**.
2. Choose **Help** > **License Management** > **License Information** from the main menu in the client to check whether the NE capacity is sufficient.
   - If the NE capacity is insufficient, you need to purchase a new license to increase the NE capacity. In this case, go to **4**.
   - If the NE capacity is sufficient, the operation ends.
3. Specify another alarm threshold (90% is recommended) in the license.
   - If the alarm is cleared, the operation ends.
   - If the alarm is not cleared, go to **4**.
4. Collect the information about alarm handling, and contact technical support personnel of the Huawei Technologies Co., Ltd..

----End

4.25 ALM-297 The OMC License Expired

Description

When the OMC license expires, this alarm is generated. After the license is updated, this alarm is cleared.

Attribute

Alarm ID	Alarm Severity	Alarm Type
297	Critical	Processing error

Impact on the System

- When the license expires, the U2000 supports a grace period (usually 90 days). In this period, you can use the U2000 functions normally. The U2000, however, provides prompts on an increasing frequency.
- When the grace period expires, you cannot use the U2000 functions.

System Actions

None.

Possible Causes

The U2000 license expires.

Procedure

- Contact Huawei technical support engineers to apply for a new U2000 license.

----End

4.26 ALM-298 The User in the Administrators or SMManagers Group Changes a User's Password

Description

This alarm is generated when the password of **Administrator** is changed or the user in the security administrators group changes another user's password.

Attribute

Alarm ID	Alarm Severity	Alarm Type
298	Critical	Security service or mechanism violation

Parameters

Name	Meaning
User name	Name of user that changed a user's password.

Impact on the System

Alarm of a high risk operation: The user whose password is changed cannot log in to the U2000 by using the old password.

System Actions

None.

Procedure

1 The alarm does not need to be handled.

----End

4.27 ALM-299 An OMC User Is Added to the Administrators, SMManagers or Sub Domain User Group

Description

This alarm is generated when a U2000 user is added to the Administrators, SMManagers or Sub Domain User group.

Attribute

Alarm ID	Alarm Severity	Alarm Type
299	Critical	Security service or mechanism violation

Parameters

Name	Meaning
User name	Name of added user.

Impact on the System

Alarm of a high risk operation. A user with high rights is added.

System Actions

None.

Procedure

1 The alarm does not need to be handled.

----End

4.28 ALM-801 OMC License Beyond Limitation

Description

If the number of managed NEs exceeds the NE quantity defined in the license, the system generates this alarm. If the number of managed NEs is smaller than or equal to the NE quantity defined in the license, this alarm is cleared.

Attribute

Alarm ID	Alarm Severity	Alarm Type
801	Critical	Processing error

Parameters

Name	Meaning
LicenseID	Serial number of a license.

Name	Meaning
LicenseCapacity	NE quantity defined in a license.
LicenseConsumption	Consumed capacity of a license.
Beyondtime	Time when the number of consumed NEs of a license exceeds the threshold.

Impact on the System

If the number of NEs managed by the current NMS exceeds the NE quantity defined in the license, you cannot add NEs to be managed to the NMS.

System Actions

None.

Possible Causes

The number of NEs managed by the current NMS exceeds the NE quantity defined in the license.

Procedure

1. Log in to the U2000 client.
2. Deleted unnecessary NEs to release licenses.
3. Choose **Help** > **License Management** > **License Information** from the main menu. In the **License Information** dialog box, query the license information about resources on the **Resource control item** tab, view the quantity defined in the license. Apply for a new license based on the number of NEs to be managed in the current NMS.

----End

4.29 ALM-1108 Process abnormally exit

Description

The monitored process stops running or exits.

Attribute

Alarm ID	Alarm Severity	Alarm Type
1108	Major	Quality of service alarm

Parameters

Name	Meaning
HostName	Host Name
ProcessCmd	Process Startup Command

Impact on the System

The service may be interrupted.

System Actions

None.

Procedure

1. View the process startup command in the alarm location information to check the process that exits.
   - If the process is a system process or a service process=>**2**.
   - If the process is not a system process or a service process=>**5**.
2. Observe the process for a while, and check whether the process can be started automatically.
   - If the process can be started, and the alarm is cleared=>**5**.
   - If the process cannot be started, and the alarm cannot be cleared=>**3**.
3. Search for the startup command of the process that exits, and run the command.
   - If the alarm is cleared=>**5**.
   - If the alarm persists=>**4**.
4. Contact Huawei technical support engineers for solution or submit a fault report at **http://gcrms-ovs.huawei.com**.
5. End.

----End

Clearing

When the fault is eliminated, the system will auto-clear the alarm. Manual clearing is not required.

4.30 Communication Failure Between the U2000 and an NE

Description

The alarm is generated when the communication between the U2000 and NE fails.

Attribute

Alarm ID	Alarm Severity	Alarm Type
100	Critical	Communication

Parameters

None.

Impact on the System

You cannot query the U2000 data and set parameters on the device.

Possible Causes

- Cause 1: The device is powered off.
- Cause 2: The device is restarted.
- Cause 3: The SNMP protocol configured on the device and the U2000 is different.
- Cause 4: The firewall is enabled on the device or the PC that runs the U2000.
- Cause 5: The device is busy.

Procedure

1. If the device is powered off, do as follows:
   (1) Check the power supply status of the device. If the power connector is improperly connected, reconnect the power lines. If the power supply unit is faulty, replace it.
2. If the device is restarted, no handling measures are required.
3. If the SNMP protocol configured on the device and the U2000 is different, do as follows:
   (1) Choose **Administration** > **NE Communicate Parameter** > **NE Access Protocol Parameters** from the main menu. Check the settings of the SNMP parameters of the device on the U2000.
   (2) Run the **display snmp-agent community read/write** command to check whether the read community and write community of the SNMPv1 protocol on the device are the same as those on the U2000.
   (3) Make changes on the parameter settings so that the settings of the SNMP parameters on the device and the U2000 are the same.
4. If the firewall is enabled on the server, disable the firewall.
5. If the device is busy, retry later.
6. Contact Huawei technical support engineers to handle the alarm.

----End

Related Information

None.

4.31 COMMU_BREAK_BTWN_NE_AND_BAKGNE

Description

The COMMU_BREAK_BTWN_NE_AND_BAKGNE alarm is generated when the communication between an NE and its secondary gateway NE is interrupted.

Attribute

Alarm ID	Alarm Severity	Alarm Type
7	Major	Communication

Parameters

None

Impact on the System

The NE fails to communicate with the U2000 through the secondary gateway NE. If the primary gateway NE is faulty, the NE may fail to communicate with the U2000.

Possible Causes

- Cause 1: The secondary gateway NE fails to communicate with the U2000.
- Cause 2: The secondary gateway NE fails to communicate with the NE.

Procedure

1. Cause 1: The secondary gateway NE fails to communicate with the U2000.
   (1) In the physical view on the U2000, right-click the LocalNM and choose **Browse Current Alarms** to check for the GNE_CONNECT_FAIL alarm. If there is the **GNE_CONNECT_FAIL** alarm related to the secondary gateway NE, handle the alarm according to the recommended procedure.
   (2) In the **Browse Current Alarms** window, check whether the **GNE_CONNECT_FAIL** alarm stops. If the **GNE_CONNECT_FAIL** alarm stops, proceed with the next step.
2. Cause 2: The secondary gateway NE fails to communicate with the NE.
   (1) Eliminate human factors.
   - Check whether the ECC route planning is reasonable. If not, re-plan and re-configure the ECC route.
   - Check whether the NE ID is repeated. If the NE ID is repeated, modify the NE ID so that the NE ID is unique on the entire network.

     To check whether the NE ID is duplicate, do as follows: Choose **Inventory** > **Physical Inventory** > **NE** from the main menu. Click the **NE List** tab. Select **All Records** and check whether there are duplicate NE IDs in the NE list.

- Check for the mis-operation of looping back the first VC-4. In the NE Explorer, choose **Interface Management** and check whether an interface is looped back. If an interface is looped back by mistake, cancel the loopback.

  NOTE

  For the intermediate frequency board: In the NE Explorer, select the board and choose**Configuration** > **Digital Interface** from the Function Tree.

(2) Eliminate external factors.

- Check the external devices between the secondary gateway NE and the NE, such as the network cable, network interface card, and router. Rectify the fault, if there is any.
- Check whether the ECC link between the secondary gateway NE and the NE is normal.

(3) Check whether the board hardware is faulty. If yes, replace the board.

(4) Check whether the COMMU_BREAK_BTWN_NE_AND_BAKGNE alarm stops.

3 If the alarm persists, contact a Huawei engineer.

----End

Related Information

None.

4.32 NE_COMMU_GNE_SWITCH

Description

The NE_COMMU_GNE_SWITCH alarm indicates that a switching of the GNE for the current NE occurs. That is, the original standby GNE becomes active.

Attribute

Alarm ID	Alarm Severity	Alarm Type
25	Major	Communication

Parameters

None.

Impact on the System

None.

Possible Causes

A switching (manual or automatic) of the GNE for the current NE occurs. That is, the original standby GNE becomes active.

Procedure

- You can clear this alarm by switching the GNE back to the original active GNE.
- If the fault persists, contact Huawei technical support engineers.

----End

Related Information

None.

4.33 GNE_CONNECT_FAIL

Description

The GNE_CONNECT_FAIL alarm is generated when the communication between the U2000 and gateway NE fails.

Attribute

Alarm ID	Alarm Severity	Alarm Type
4	Critical	Communication

Parameters

None.

Impact on the System

- The configuration data and parameters of the gateway NE cannot be queried or set.
- The U2000 fails to configure the NEs connected to the gateway NE and perform operations on these NEs.

Possible Causes

The possible causes of the GNE_CONNECT_FAIL alarm are as follows:

- Cause 1: The parameter settings about DCN communication of the gateway NE are incorrect.
- Cause 2: The parameter settings about DCN communication of a non-gateway NE connected to the gateway NE are incorrect.
- Cause 3: The physical link between the U2000 and the gateway NE is broken.

Procedure

1. Cause 1: The parameter settings about DCN communication of the gateway NE are incorrect.
   (1) Choose **System** > **DCN Management** from the Main Menu, and click the **GNE** tab.
   (2) Check whether the IP address and port number of the faulty gateway NE are correct.

- If correct, proceed to Steps 1.c to 1.e.
- If incorrect, proceed to Step 2.

(3) **Optional:** Right-click the faulty gateway NE and choose **Modify GNE**. In the displayed **Modify GNE** dialog box, correctly set the communication parameters, and then click **Apply**.

(4) The **Warning** dialog box is displayed to indicate that this operation may interrupt communication, click **OK**.

(5) If the alarm persists, proceed with the next step.

2 Cause 2: The parameter settings about DCN communication of a non-gateway NE connected to the gateway NE are incorrect.

(1) In NE Explorer, select the non-gateway NE and choose **Communication** > **Communication Parameters** from Function Tree.

(2) Check whether the subnet mask of the non-gateway NE is the same as the subnet mask of the gateway NE. If not, proceed with the next step.

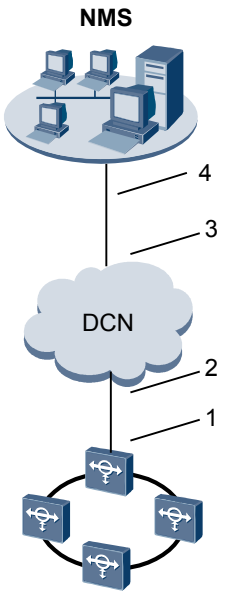
(3) Set the subnet masks of the non-gateway NE and gateway NE to the same. Then click **Apply**.

(4) If the alarm persists, proceed with the next step.

3 Cause 3: The physical link between the U2000 and the gateway NE is broken.

(1) Check whether the STAT or Run indicator on the SCC of the gateway NE blinks. If not, power on the equipment.

(2) Set the communication parameters (IP address and subnet mask) on a laptop computer the same as the communication parameters on the U2000. Run the **ping IP address of the NE** command at the four detection points in the following figure in turn to locate the faulty point of the physical link.



NOTE

For example,

- Ping the IP address of the gateway NE at detection point 1. If the IP address of the gateway NE can be pinged, check whether the STAT indicator (red) on the SCC board is on. If on, see the *Troubleshooting* of the equipment to replace the SCC. If off, see the *Troubleshooting* of the equipment to replace the communication board.
- Ping the IP address of the gateway NE at detection point 2. If the IP address of the gateway NE can be pinged, you can infer that the cable is normal. Otherwise, replace the cable.
- Ping the IP address of the gateway NE at detection points 3 and 4 in turn to check whether the intermediate routing equipment is faulty. If the intermediate routing equipment is faulty, remove the fault.
- After removing the physical faults, log in to the U2000 to check whether the alarm stops . If the alarm persists, proceed with the next step.

4 If the alarm persists, contact a Huawei engineer.

----End

Related Information

None.

4.34 GNE_MGR_LIMIT_OVER

Description

The GNE_MGR_LIMIT_OVER alarm is generated when the number of NEs connected to a gateway NE exceeds the limit. Currently, the default limit is 50.

Attribute

Alarm ID	Alarm Severity	Alarm Type
9	Warning	Service

Parameters

None

Impact on the System

The number of NEs connected to a gateway NE exceeds the limit. As a result, the U2000 may fail to reach the NEs, and to normally monitor and manage the alarms.

NOTE

By default, the U2000 detects the alarm every 60 minutes. When the number of non-gateway NEs of the gateway NE exceeds 50, this alarm is reported. When the number of non-gateway NEs is smaller than 50, this alarm is cleared.

Possible Causes

- Cause 1: The connection between the U2000 and a gateway NE is faulty. As a result, the NEs connected to the gateway NE are switched to the secondary gateway NE to resume communication with the U2000. Then, the number of NEs connected to the secondary gateway NE increases and exceeds the limit.
- Cause 2: The connection between the U2000 and a non-gateway NE is faulty. As a result, the NE is automatically switched to the secondary gateway NE to resume communication with the U2000. Then, the number of NEs connected to the secondary gateway NE increases and exceeds the limit.
- Cause 3: A non-gateway NE is manually switched to a new gateway NE. As a result, the number of NEs connected to the new gateway NE increases and exceeds the limit.

Procedure

1. Cause 1: The connection between the U2000 and a gateway NE is faulty.
   (1) Check for the GNE_CONNECT_FAIL alarm on the U2000 . If there is the GNE_CONNECT_FAIL alarm, handle the alarm according to **4.33 GNE_CONNECT_FAIL**.
   (2) Check whether the GNE_MGR_LIMIT_OVER alarm stops. If the GNE_MGR_LIMIT_OVERE alarm stops, proceed with the next step.
2. Cause 2: The connection between the U2000 and a non-gateway NE is faulty.
   (1) Check for the NE_COMMU_BREAK alarm on the U2000 . If there is the NE_COMMU_BREAK alarm, handle the alarm according to **4.37 NE_COMMU_BREAK**.
   (2) Check whether GNE_MGR_LIMIT_OVER alarm stops. If the GNE_MGR_LIMIT_OVERE alarm stops, proceed with the next step.
3. Cause 3: A non-gateway NE is manually switched to a new gateway NE.
   (1) Choose **Administration** > **DCN Management**from the Main Menu.Re-assign a gateway NE for each NE to ensure that the number of NEs connected to each gateway NE does not exceed 50.
4. If the alarm persists, contact a Huawei engineer.

----End

Related Information

None.

4.35 GNE_NUM_LIMIT_OVER

Description

The GNE_NUM_LIMIT_OVER alarm is generated when the number of gateway NEs permitted by the NE explorer exceeds the limit. Currently, the default limit is 500.

Attribute

Alarm ID	Alarm Severity	Alarm Type
22	Major	Equipment

Parameters

None

Impact on the System

In case of the GNE_NUM_LIMIT_OVER alarm, the number of gateway NEs managed by the NE explorer exceeds the limit. This may result in timeout service processing or restart of the NE explorer.

Possible Causes

The number of gateway NEs managed by the NE explorer exceeds the limit.

Procedure

1. Choose **Administration** > **Settings** > **NE**Partition from the Main Menu.Migrate certain gateway NEs to a similar NE explorer with the number of managed gateway NEs under the limit.
2. If the alarm persists, contact a Huawei engineer.

----End

Related Information

None.

4.36 MGR_LIMIT_OVER

Description

The MGR_LIMIT_OVER alarm is generated when the total number of equivalent NEs managed by the U2000 exceeds the maximum number of manageable NEs configured for the U2000.

Attribute

Alarm ID	Alarm Severity	Alarm Type
11	Critical	Service

Parameters

None.

Impact on the System

In case of the MGR_LIMIT_OVER alarm, the performance or efficiency of the U2000 may be degraded.

In this case, if you continue creating NEs, the alarm is not repeatedly reported. When the number of NEs decreases and is less than the maximum management capability of the U2000, the alarm stops.

Possible Causes

The number of NEs under the management of the U2000 exceeds the maximum management capability of the U2000.

Procedure

1. Decrease the number of NEs managed by the U2000.
   - Delete certain redundant NEs. For details on how to delete an NE.
   - Migrate NEs so that the NEs managed by the NMS are managed by multiple NMSs. For details on how to create an NE on a new NMS.
2. When upgrading the NMS, contact a Huawei engineer and ask the engineer to apply for a license of larger management capability of the NMS.

----End

Related Information

None.

4.37 NE_COMMU_BREAK

Description

The NE_COMMU_BREAK alarm is generated when the communication between an NE and the U2000 is interrupted.

Attribute

Alarm ID	Alarm Severity	Alarm Type
1	Critical	Communication

Parameters

None.

Impact on the System

The NE cannot be managed on the U2000.

Possible Causes

- Cause 1: The communication between the gateway NE that the NE connects to and the U2000 fails. Hence, the NE communication fails.
- Cause 2: The SCC of the NE is faulty.
- Cause 3: The fiber between the NE and the gateway NE that the NE connects to is broken.
- Cause 4: The network scale is large so that the ECC communication between NEs exceeds the limit of the processing capability of the NE.

Procedure

- Cause 1: The communication between the gateway NE that the NE connects to and the U2000 fails. Hence, the NE communication fails.
  1. Check whether the gateway NE reports the GNE_CONNECT_FAIL alarm. If yes, stop the alarm. For details about stopping the alarm, see **GNE_CONNECT_FAIL**.
  2. View the current alarms on the U2000 to check whether the alarm stops. If the alarm persists, proceed to the next step.
- Cause 2: The SCC of the NE is faulty.

  Check the indicators on the panel of the SCC. If the indicators are abnormal, you can infer that the SCC is faulty. For details about the indicators, see **Table 4-9**. Reset the SCC. If the indicators are still abnormal, replace the SCC. For details about the operations, see Replacing the SCC board in the *Parts Replacement* of the equipment.
- Cause 3: The fiber between the NE and the gateway NE that the NE connects to is broken.

  Measure the fiber with an OTDR meter. Check whether the fiber is broken and the broken section of the fiber according to the fiber attenuation curve. Replace the fiber if the fiber is broken.

  NOTE

  For the usage of the OTDR meter, see the operation guide of the OTDR.
- Cause 4: The network scale is large so that the ECC communication between NEs exceeds the limit of the processing capability of the NE.

  NOTE

  Check whether the planning of the ECC routes is proper. When the number of NEs on a network exceeds 100, the network must be divided into ECC networks to avoid overload of the ECC communication.

  1. Divide a subnet of a large scale into several subnets of small scales.

     NOTE

     - Allocate adjacent networks to a subnet according to the principle of managing networks by layers and areas.
     - It is recommended that the number of NEs in a subnet does not exceed 64.
  2. Select proper common NEs as gateway NEs in a subnet.

     NOTE

     When there are multiple loops and links, set the equipment that is located in sections with most loops and links as gateway NEs. In this manner, the situation that large amount of management information is transmitted through the DCC with narrow band and broad channel is avoided so as to prevent the DCN from being congested.
  3. Disable the ECC connections between redundant subnets.

- Disable the interworking between ECC subnets, which is achieved through the extended ECC (automatic or manual).
- Disable the interworking between ECC subnets, which is achieved through the STM-N electrical or optical interfaces.

- If the alarm persists, contact a Huawei engineer.

----End

Related Information

Table 4-9 Indicator description of the SCC board

Indicator	Name	Status	Description
STAT	Board Hardware Indicator	On (green)	The board works normally.
		On (red)	Critical alarm occurs to board.
		On (yellow)	Minor alarm occurs to board.
		Off	The board is not powered on.
PROG	Board Software Indicator	On (red)	Memory check failed/loading unit software failed/the FPGA file is lost/the unit software is lost.
		Blinking (red)	100ms on and 100ms off.
			BOOTROM check failed.
		Blinking quickly (green)	100ms on and 100ms off.
			Writing FLASH.
		Blinking slowly (green)	300ms on and 300ms off.
			BIOS booting/ loading FPGA/ loading unit software.

Indicator	Name	Status	Description
		On (green)	The board software or software for FPGA is uploaded successfully, or the board software is initialized successfully.
SRV	Service Alarm Indicator	On (green)	Service is normal, no service alarm occurs.
		On (red)	Critical or major alarm occurs to service.
		On (yellow)	Minor or remote alarm occurs to service.
		Off	No service is configured.
ALMC	Alarm cut indicator	On (yellow)	Currently in permanent alarm cut-off status.
		Off	Give sound warning upon alarm.

4.38 NE_NOT_LOGIN

Description

The NE_NOT_LOGIN alarm is generated when an NE is not logged in.

Attribute

Alarm ID	Alarm Severity	Alarm Type
2	Critical	Security

Parameters

None.

Impact on the System

- The configuration data of the NE cannot be queried on the NE.

- The NE cannot be managed on the U2000.

Possible Causes

- Cause 1: The communication between the NE and the U2000 is interrupted.
- Cause 2: The user logs out of the NE or fails to log in.

Procedure

- Cause 1: The communication between the NE and the U2000 is interrupted.

  For the method of solving the problem of communication interruption between the NE and the U2000, see **NE_COMMU_BREAK**.
- Cause 2: The user logs out of the NE or fails to log in.

  Use another correct user to log in the NE. For details about the operation.
- Check whether the alarm stops . If the alarm persists, proceed with the next step.
- If the alarm persists, contact a Huawei engineer.

----End

Related Information

None.

4.39 XC_LICENSE_OVERFLOW

Description

The XC_LICENSE_OVERFLOW alarm is generated when the number of subracks configured with certain cross-connect type or cross-connect capacity on the entire network exceeds the license alarm threshold.

Attribute

Alarm ID	Alarm Severity	Alarm Type
23	Major	Service

Parameters

None.

Impact on the System

The subrack with the relevant cross-connect type or cross-connect capacity cannot be created on the U2000.

Possible Causes

The number of subracks that are configured with certain cross-connect type or cross-connect capacity and managed by the U2000 exceeds the license limit.

Procedure

- Locate the fault according to the alarm.
  1. Choose **Help** > **License Information** from the main menu.
  2. Select the **Resource Control Item** tab in the displayed dialog box to find out the items whose consumption values are greater than the License values.
- Apply for and update the license file to increase the number of subracks configured with certain cross-connect type or cross-connect capacity.
- Delete unused subracks.
  1. Choose **Inventory** > **WDM Statistic Report** > **WDM NE Master/Slave Shelf Info Report** from the main menu. Browse the information report on the WDM master and slave subracks. Check the information about the subracks of each NE.
  2. Double-click the NE where the relevant subrack is located on the Main Topology to enter the NE panel.
  3. Right-click the subrack that you want delete, and then choose **Delete the Subrack**.
- Check whether the alarm stops. If the alarm persists, proceed with the next step.
- If the alarm persists, contact a Huawei engineer.

----End

Related Information

None.

4.40 XC_LICENSE_UNEXPECTED

Description

The XC_LICENSE_UNEXPECTED alarm is generated when the configuration of the cross-connect type or cross-connect capacity for a subrack is abnormal.

Attribute

Alarm ID	Alarm Severity	Alarm Type
24	Major	Service

Parameters

None.

Impact on the System

When the cross-connect type and cross-connect capacity are not configured for a subrack, the U2000 reports the alarm but the cross-connection that is performed by the integrated cross-connect board can be created on the subrack.

When the cross-connect type is none and the cross-connect capacity is a non-zero value, or when the cross-connect type is not none and the cross-connect capacity is zero, the cross-connection that is performed by the integrated cross-connect board cannot be created on the subrack.

Possible Causes

The possible causes of the alarm are as follows:

- The cross-connect type and cross-connect capacity are not configured for a subrack.
- The cross-connect type is none and the cross-connect capacity is a non-zero value.
- The cross-connect type is not none and the cross-connect capacity is zero.

Procedure

- View the license information.
  1. Choose **Help** > **License Information** from the main menu.
  2. Select the **Resource Control Item** tab in the displayed dialog box to view the license information.
- If the **Resource** of the cross-connect type or cross-connect capacity for a subrack is unavailable or the value of **Consumption** of the cross-connect type or cross-connect capacity for a subrack reaches the license value, apply for and update the license file.
- Modify the attributes of an NE subrack.
  1. Choose **Inventory** > **WDM Statistic Report** > **WDM NE Master/Slave Shelf Info Report** from the main menu. Browse the information report on the WDM master and slave subracks. Locate the NE whose subrack cross-connect type and cross-connect capacity is abnormal.
  2. Double-click the NE on the Main Topology to enter the NE panel.
  3. Right-click the subrack whose configuration is incorrect, and then choose **Modify Subrack Attribute**.
  4. In the displayed dialog box, set the cross-connect type and cross-connect capacity of the subrack to the values within the range permitted by the license file, and then click **Apply**.
  5. Click **Close** in the displayed dialog box.
- Check whether the alarm stops. If the alarm persists, proceed with the next step.
- If the alarm persists, contact a Huawei engineer.

----End

Related Information

None.

4.41 SERVICE_OUTAGE

Description

After alarms indicating faults that may affect the service communication are located to a path, the U2000 issues a command to the equipment to check the service communication. If the service is interrupted, the U2000 generates the SERVICE_OUTAGE alarm to notify the network maintenance personnel. The alarm is displayed as Major on the U2000. It can be synchronized and acknowledged, but cannot be deleted.

Attribute

Alarm Severity	Alarm Type
Major	Service

Parameters

None.

Impact on the System

After the alarm is generated, you can infer that the service is interrupted and the fault needs to be processed immediately.

Possible Causes

After alarms of the **Critical** or **Major** level on the equipment are located to a path, the U2000 issues a command to the equipment to check the service communication. If the service is interrupted, the U2000 generates the SERVICE_OUTAGE alarm.

The SERVICE_OUTAGE alarm is generated as follows:

- Alarms of the **Critical** or **Major** level are generated on the equipment. In addition, the alarms are located to the path of the U2000.
- After the alarms are located to the path, the SERVICE_OUTAGE alarm is triggered.
- The U2000 issues a command to the equipment to check the service communication. If the service is interrupted, the U2000 generates the SERVICE_OUTAGE alarm.

Procedure

1. Right-click the alarm and perform one of the following operations:
   - In the case of the MSTP E2E service, choose **Alarm Affect Object** > **Trails** from the shortcut menu.
   - In the case of the packet service, choose **Alarm Affect Object** > **PWE3 Service** from the shortcut menu.
2. Locate the path of the alarms. Right-click the affected path on the path management interface, and then choose **Alarm** > **Current Alarm** to view all the current alarms of the path.

3 Take further measures according to the other alarms of the path. For example, handle the MUT_LOS and R_LOS alarms.

----End

Related Information

None.

4.42 PROTECT_DEGRADED

Description

The PROTECT_DEGRADED is an alarm indicating that capability of protecting an affected service degrades. When the NE alarm that may interrupt a service is located to the protected service trail, the service is still in the normal state because of the protection mechanism, but the capability of protecting the service degrades. In this case, the U2000 triggers the PROTECT_DEGRADED alarm to locate the service.

Attribute

Alarm ID	Alarm Severity	Alarm Type
21	Major	Service

Impact on the System

When the PROTECT_DEGRADED alarm occurs, the capability of protecting the affected services degrades. Therefore, you need to handle the alarm immediately.

Possible Causes

A critical or major alarm that is generated by an NE and may interrupt a service is located to the service.

Procedure

1 Right-click the alarm and perform one of the following operations:

- In the case of the MSTP E2E service, choose **Alarm Affect Object** > **Trails** from the shortcut menu.
- In the case of the packet service, choose **Alarm Affect Object** > **PWE3 Service** from the shortcut menu.

2 In the window that is displayed, right-click the affected service and choose **Alarm** > **Current Alarm** from the shortcut menu to view all current alarms of the service.

3 Handle the current alarms that affect the service.

----End

5 NE Management Troubleshooting

About This Chapter

This topic describes how to troubleshoot NE management.

5.1 Failed to Create an NE

Symptom

Adding a device on the NMS fails. The system prompts **Operation failed. Failure cause: NO response from device.**

Possible Causes

The possible causes are:

- The DCN between the NMS and the NE is faulty.
- The communication parameters of the NMS or the NE are incorrectly set.
- The NE is being restarted and does not respond.

Procedure

- Check the DCN between the U2000 and the NE.
  1. Check that the U2000 and the NE are reachable. You can use the **ping** command to check the network connectivity between the NMS and the NE and the packet loss ratio.
  2. Rectify the fault according to the onsite condition.
- Check the settings of the parameters on the NMS and the NE.
  1. Check the settings of the NMS communication parameters, including the IP address and the parameters related to the gateway.
  2. Check the settings of the NE parameters, including the IP address, etc.
  3. Make sure that the settings of the parameters for the creation of the NE are the same as those on the device side.
- If the NE is being restarted and does not respond, add the NE after the restart is complete.

----End

5.2 Frequent Change of the Online and Offline Statuses of Certain NEs on the NMS

Symptom

The online and offline statuses of certain NEs frequently change.

Possible Causes

- Login users are kicked mutually due to conflict.
- The number of NEs exceeds the maximum management capability of the NMS.
- The disk space is insufficient.

Procedure

1 Check whether the same NE user is used for login in another place.

2 Check whether the number of NEs exceeds the maximum management capability of the NMS. For the performance indicators, refer to chapter "Performance Indicators" and "Management Capability" in the *iManager U2000 Product Description*.

3 Check the disk space of the server. In normal situations, the disk usage cannot exceed 80%. If the disk usage exceeds 80%, clear the disk. You can delete and back up related files to free the disk space.

----End

5.3 A Large Number of Non-GNEs on the U2000 Are Disconnected

Symptom

The U2000 server is normal, but a large number of NEs are disconnected.

Possible Causes

When networks interconnect or GNEs have a larger number of non-GNEs, ECC storm occurs due to large scale of subnets.

Procedure

1 Run the **ping** command to check whether the IP addresses of the GNEs of the disconnected NEs are normal and available.

NOTE

If a GNE fails to be connected, check the connection between the GNE and the U2000 server. First, ensure that the GNE is not disconnected.

2 If a GNE can be connected, check the ECC link of the GNE. To be specific, choose **Communication** > **NE ECC Link Management** in the NE Explorer to view ECC links.

3 If a large number of ECC links (hundreds of records) exist and change frequently, it indicates that the number of non-GNEs of the GNEs exceeds the maximum number. As a result, ECC storm occurs.

4 It is recommended that you disable the ECC ports on certain optical cards, and divide and plan ECC subnets after finding the fault point that causes the ECC storm. This helps to reduce hidden faults.

For the maximum number of non-gateway NEs connected to a gateway NE, refer to the product description of the related version. If the actual number exceeds the maximum, modify the actual number according to the planning.

----End

5.4 Abnormal Data Generated After the U2000 Restarts

Symptom

U2000 Certain NEs are missing in the NMS and the topology is disorderly displayed.

Possible Causes

The NMS database is abnormal.

Procedure

1. Initialize the database. For details, refer to **Backing Up and Restoring the U2000 Database** in the *iManager U2000 Administrator Guide*.
2. Manually recover the U2000 data. For details, refer to **Backing Up and Restoring the U2000 Database** in the *iManager U2000 Administrator Guide*.

----End

6 Faults of the Operating System

About This Chapter

This topic describes how to troubleshoot the faults of the operating system.

6.1 Solaris OS Troubleshooting

This topic describes how to troubleshoot the Solaris OS.

6.1.1 Starting the Operating System Fails

The operating system cannot be started or is started repeatedly. Therefore, a certain user fails to enter the login interface.

Locate and rectify the fault according to the following sequence:

Sequence	Current Symptom	Troubleshooting
1	The screen displays nothing.	Check whether the connection between the display and server is normal.
2	The screen displays error prompts.	Troubleshoot according to the error prompts. Rectify the fault according to the following symptoms: ● **6.1.1.1 Operating System Enters the Single-User Mode After Restart** ● **6.1.1.2 Repeated Startup of the Operating System** ● **6.1.1.3 System Prompts Unadapted Display**
3	In other cases.	Contact Huawei engineers for troubleshooting.

6.1.1.1 Operating System Enters the Single-User Mode After Restart

Symptom

The operating system enters the single-user mode after restart. A message is displayed indicating "WARNING - Unable to repair the / filesystem. Run fsck manually (fsck -F ufs /dev/rdsk/c*t*d*s*)."

NOTE

In the warning prompt "Unable to repair the / filesystem", the / may indicate another directory.

Possible Causes

The server is switched off illegally or powered off. Therefore, the file system that is running is damaged. After the powered supply is restored, the system performs a self-check during the startup of the server. If the file system is detected damaged, the self-check fails and the system enters the single-user mode during the startup.

Procedure

1. Log in to the operating system as user **root**.
2. To restore the file system, run the following command:

   ```
   # fsck -y
   ```

   CAUTION

   - If the disk capacity is large and the file system is damaged severely, it may take a long time to restore the file system by using the **fsck -y** command. During the restoration, do not perform any operation to the server. Otherwise, the operating system cannot recover.
   - The **fsck** command can be used to rectify only normal faults. For the fault on the Solaris startup parameters or kernel damage due to abnormal power failure, the command is invalid.

3. Observe the information displayed on the screen. Check whether the file systems of all partitions are correct and whether the file system of the damaged partition is restored.

   If the error information or the information that requires restoration is displayed again, run the **fsck -y** command repeatedly until such information is not displayed again.

4. To synchronize the files and restart the operating system, run the following commands:

   ```
   # sync;sync;sync;sync;sync;sync
   # init 6
   ```

----End

Suggestion and Summary

It is prohibited to shut down the server illegally. It is recommended that the server be configured with the UPS to effectively prevent power failures.

6.1.1.2 Repeated Startup of the Operating System

Symptom

On the single-server system, a message is displayed indicating "Cannot open '/etc/path_to_inst' Program terminated." Then the system is started repeatedly.

Possible Causes

The server is powered off abnormally or other abnormal operations are performed. This causes that the operating system is damaged and the **path_to_inst** system file cannot be opened. Therefore, the operating system cannot be started.

Procedure

1. During self-check of the operating system (before entering the operating system), press **STOP+A** to exit the startup. The `ok` prompt is displayed.
2. Insert the installation CD-ROM of Solaris 10. To start from the CD-ROM and enter the single-user mode, run the following command:

   `ok` **`boot cdrom -s`**

   NOTE

   Wait for 5 minutes. When SINGLE USER MODE and # are displayed, the system enters the single user start mode.
3. To search for the corresponding raw equipment name of the system root directory, run the following commands:

   `#` **`cat /etc/vfstab`**

   The terminal displays:

   NOTE

   The displayed message changes according to different actual conditions.

```
#device         device          mount           FS      fsck    mount   mount
#to mount       to fsck         point           type    pass    at boot options
#
fd      -       /dev/fd fd      -       no      -
/proc   -       /proc   proc    -       no      -
/dev/dsk/c1t0d0s1       -       -       swap    -       no      -
/dev/dsk/c1t0d0s0       /dev/rdsk/c1t0d0s0      /       ufs     1       no      -
/dev/dsk/c1t0d0s7       /dev/rdsk/c1t0d0s7      /U2000  ufs     2       yes     -
/dev/dsk/c1t0d0s6       /dev/rdsk/c1t0d0s6      /opt    ufs     2       yes     -
/devices        -       /devices        devfs   -       no      -
ctfs    -       /system/contract        ctfs    -       no      -
objfs   -       /system/object  objfs   -       no      -
swap    -       /tmp    tmpfs   -       yes     -
/dev/dsk/c1t1d0s0       /dev/rdsk/c1t1d0s0      /version        ufs     2
yes     -
```

   In the preceeding message, the corresponding raw partition of the root directory (/) is **/dev/dsk/c1t0d0s0**.
4. Set the corresponding raw equipment of the root directory to the **/mnt** directory to restore the damaged operating system.

   `#` **`mount raw_equipment_name /mnt`**

   For example, run the following commands to set the **/dev/dsk/c1t0d0s0** to the **/mnt**:

   `#` **`mount /dev/dsk/c1t0d0s0 /mnt`**

5 If **/etc/path_to_inst** is lost, run the following commands to restore it by using the **path_to_inst-INSTALL** template that is reserved in the **/etc** directory by the system.

```
# cd /mnt/etc
# cp path_to_inst-INSTALL path_to_inst
```

6 Run the following commands to synchronize the file and restart the operating system:

```
# sync;sync;sync;sync;sync;sync
# init 6
```

7 After the system restarts normally, run the **fsck -y** command to repair the file system.

----End

6.1.1.3 System Prompts Unadapted Display

Symptom

After the workstation is started, a message is displayed indicating that the display is unadapted and errors occur in the **/var/dt/Xerrors** file.

Possible Causes

The peripherals of the workstation are incorrectly connected. For example, the mouse or keyboard is not connected or connected improperly.

Procedure

1 Repair the connection of the peripherals (such as the mouse, keyboard, and display) according to the information displayed on the screen.

2 Stop the NMS processes and the database process.

3 To restart the workstation, run the following commands:

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

----End

6.1.2 Failed to Log In to the GUI of the OS

Symptom

After the Solaris OS is started, the user cannot log in to the GUI.

Possible Causes

Abnormal shutdown may damage the file system. Consequently, the user cannot log in to the GUI after the Solaris OS is started. In this case, you can use the **fsck** command to restore the file system.

Procedure

1 After the Solaris OS is started, enter the password of the **root** user according to the prompt to access the CLI.

2 Run the following command for several times to automatically rectify the fault:

```
# fsck -y
```

NOTE

The **fsck** command can be used to rectify only normal faults. For the fault on the Solaris startup parameters or kernel damage due to abnormal power failure, the command is invalid.

3 Run the following commands to restart the workstation:

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

----End

6.1.3 System Prompts That Interfaces of Graphical Tools Cannot Be Displayed

Symptom

When the graphical tools are used on Solaris, such as the smc, a message is displayed indicating "can't open to display."

Possible Causes

The **DISPLAY** environment variable may not be set in GUI mode.

Procedure

1 Log in to the GUI of the Solaris OS.

2 To query the terminal number, run the following commands as user **root**:

```
# set | grep DISPLAY
# xhost +
```

3 To set the **DISPLAY** environment variable, run the following commands:

```
# DISPLAY=local_host_name_or_IP_address:local_terminal_No.
# export DISPLAY
```

For example:

```
# set | grep DISPLAY
DISPLAY=10.70.77.62:0.0
# xhost +
# DISPLAY=10.70.77.62:0.0
# export DISPLAY
```

4 Open the interfaces of the graphical tools again.

----End

6.1.4 Failed to Eject the CD-ROM

Symptom

A CD-ROM is in the CD-ROM drive. When you use the eject command to open the drive, the system prompts **Device busy** and the CD-ROM cannot be ejected.

Possible Causes

The data in the CD-ROM is in use.

Procedure

1. Check that the data in the current CD-ROM is not in use.
2. Run the following command as the **root** user:
   ```
   # svcadm disable -t volfs
   ```
3. Press the eject button on the drive panel to take out the disk from the CD-ROM.
4. Run the following command to resume the drive:
   ```
   # svcadm enable volfs
   ```

----End

6.1.5 Operation Anomaly Caused by Insufficient Disk Space

Symptom

Certain operations are abnormal. For example, the operation system cannot be logged in to, the operation system runs at a low speed, the database cannot be started, or the U2000 cannot be started.

Possible Causes

Normally, the disk space occupancy should be 80% or below.

Procedure

1. Check the disk space. Do as follows:
   (1) Log in to the Solaris OS as the **root** user.
   (2) Run the following command to check the disk usage:
   ```
   # df -k
   ```
   (3) View the usage of the directories including the **/** directory, **/opt** directory, and **/opt/U2000** directory in the displayed information.
2. If the size of the disk space exceeds the normal value, you need to manually clear the disk. For details, refer to **Managing U2000 Files and Disks** in the *iManager U2000 Administrator Guide*.

----End

6.1.6 Slow Running of the System Caused by Insufficient Memory

Symptom

The U2000 runs at a low speed.

Possible Causes

The memory may be insufficient.

Procedure

1 To check the memory occupancy status, run the following command as user **root**:

```
# vmstat 2
```

The terminal displays:

```
kthr      memory            page            disk          faults      cpu
 r b w   swap  free  re  mf pi po fr de sr s0 s1 s3 --   in   sy   cs us sy id
 0 0 0 16940400 763008 7 30 20  6 13  0 12  2 -1  0  0  384 1773  380  1  1 98
 0 0 0 16968504 737784 2 10 24  0  0  0  0  0  0  0  0  365  450  328  0  0 99
 0 0 0 16968504 737832 0  0  0  0  0  0  0  2  0  0  0  386 1416  337  1  1 99
 0 0 0 16968504 737832 0  0  0  0  0  0  0  0  0  0  0  369  433  330  0  0 99
......
```

If the value of the **sr** column remains at a value from 200 to 300 page/sec, it indicates that the physical memory may be insufficient.

2 Close unnecessary applications.

3 If the memory occupancy remains high, you need to replace the physical memory.

----End

6.1.7 Slow Running of the System Caused by High CPU Usage

Symptom

The U2000 runs at a low speed.

Possible Causes

The CPU usage may be over high.

Procedure

1 To check the memory occupancy status, run the following command as user **root**:

```
# vmstat 2
```

The terminal displays:

```
kthr      memory            page            disk          faults      cpu
 r b w   swap  free  re  mf pi po fr de sr s0 s1 s3 --   in   sy   cs us sy id
 0 0 0 16940400 763008 7 30 20  6 13  0 12  2 -1  0  0  384 1773  380  1  1 98
 0 0 0 16968504 737784 2 10 24  0  0  0  0  0  0  0  0  365  450  328  0  0 99
 0 0 0 16968504 737832 0  0  0  0  0  0  0  2  0  0  0  386 1416  337  1  1 99
 0 0 0 16968504 737832 0  0  0  0  0  0  0  0  0  0  0  369  433  330  0  0 99
......
```

In the last column, **id** indicates the idle CPU ratio. If the idle CPU ratio remains below 10% for a long time, the dominant frequency of the CPU mainly bottlenecks the running efficiency.

2 Close unnecessary applications.

----End

6.1.8 Connection Between the SUN Server and Switch Fails Due to Auto-Negotiation Failure

Symptom

On Solaris 10, set the mode of the switch that is connected to the SUN server to 100M full-duplex. Then, the switch reports CRC errors. The connection between the SUN server and switch fails because auto-negotiation of the network card bge0 fails.

Possible Causes

In the case of certain network cards, the auto-negotiation cannot be set to the 100M full-duplex mode.

Procedure

1. Run the following command as user **root** to navigate to **rc3.d** directory.

   ```
   # cd /etc/rc3.d
   ```

2. Run the following commands and create and edit the file **S99set*bge*** by using **vi**:

   ```
   # vi S99setbge
   ndd -set /dev/bge0 adv_1000fdx_cap 0
   ndd -set /dev/bge0 adv_1000hdx_cap 0
   ndd -set /dev/bge0 adv_100fdx_cap 1
   ndd -set /dev/bge0 adv_100hdx_cap 0
   ndd -set /dev/bge0 adv_10fdx_cap 0
   ndd -set /dev/bge0 adv_10hdx_cap 0
   ndd -set /dev/bge0 adv_autoneg_cap 0
   ndd -set /dev/bge0 adv_pause_cap 0
   ndd -set /dev/bge0 adv_asym_pause_cap 0
   ```

   NOTE

   The meanings of the preceding command lines are as follows:

   ```
   ndd -set /dev/bge0 adv_1000fdx_cap 0           (Disable the 100M full-duplex)
   ndd -set /dev/bge0 adv_1000hdx_cap 0       (Disable the 100M half-duplex)
   ndd -set /dev/bge0 adv_100fdx_cap 1      (Enable the 100M full-duplex)
   ndd -set /dev/bge0 adv_100hdx_cap 0     (Disable the 100M half-duplex)
   ndd -set /dev/bge0 adv_10fdx_cap 0        (Disable the 10M full-duplex)
   ndd -set /dev/bge0 adv_10hdx_cap 0       (Disable the 10M half-duplex)
   ndd -set /dev/bge0 adv_autoneg_cap 0     (Disable the auto-negotiation)
   ```

3. To modify the attributes of the **S99setbge** file, run the following commands:

   ```
   # chmod 744 S99setbge
   # chgrp sys S99setbge
   ```

4. To modify the attributes of the **S99setbge** file, run the following command:

   ```
   # ls -l S99setbge
   ```

5. To restart the system to make the configuration of the network card take effect, run the following commands:

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

6. To check whether the network card is successfully set, run the following command:

   ```
   # kstat -p bge | grep link_
   ```

   bge0 is successfully set the 100M full-duplex mode, if the screen displays the following information:

   ```
   ......
   bge:0:parameters:link_duplex    2
   ```

```
......
bge:0:parameters:link_speed     100
......
```

The following is the mapping relations between the values of link_duplex and attributes:

- 0 indicates down.
- 1 indicates Half Duplex.
- 2 indicates Full Duplex.

----End

6.2 Linux OS Troubleshooting

This topic describes how to troubleshoot the Linux OS.

6.2.1 Failed to Log In to the GUI

6.2.1 Failed to Log In to the GUI

Symptom

After the Linux OS is started, the user cannot access the GUI.

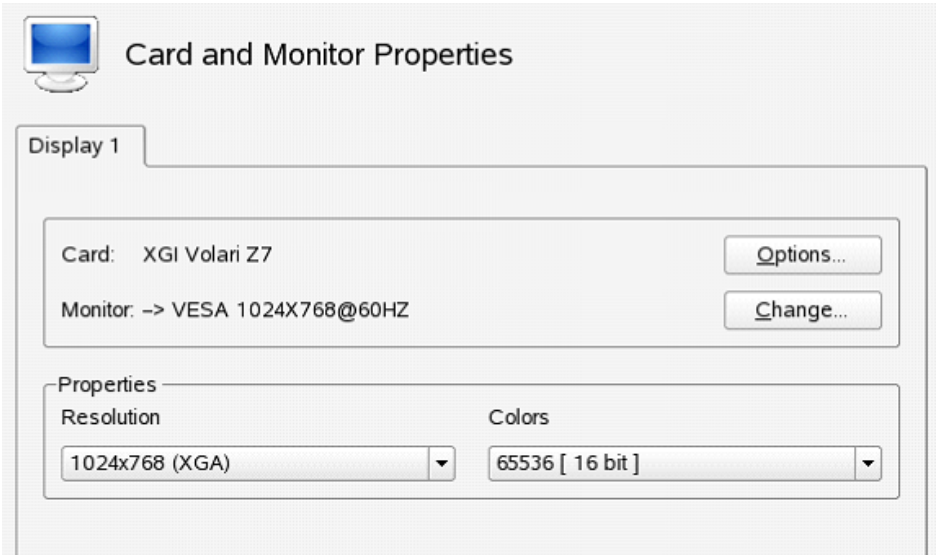
Possible Causes

The settings of the parameters on the SaX2 tool do not match those of the related parameters on the video card drive of the OS.

Procedure

1 Log in to the system as the **root** user. Run the following commands to open the GUI for configuring the SaX2 tool:

```
# init 3
# sax2
```



2 Click **Change...**. Selcet the vendor (VESA) and resolution (1024*768@60HZ), and then click **OK**. Set the resolution of the monitor to **VESA 1024*768@60HZ**.

3 Click **OK**.

----End

7 Faults of the Database

About This Chapter

This topic describes how to troubleshoot the faults of the database.

7.1 Sybase Database Troubleshooting

This topic describes how to troubleshoot the Sybase database.

7.1.1 Failure to Back Up the Database

Symptom

The backup file does not exist in the directory specified in the backup task.

Possible Causes

The possible causes of the database backup failure are as follows:

- The database is not started.
- Disk space is used up.
- Permissions for the backup directory are incorrect.
- The password of user **sa** of the database is changed incorrectly.

Procedure

1. Check whether the database is started.

   Run the **/opt/sybase/ASE-*/install/showserver** command as user **sybase**. If the dataserver and backupserver processes exist, the database service process is started.

2. Check the disk space. For details, see **6.1.5 Operation Anomaly Caused by Insufficient Disk Space**.

3. Check the permissions for and the owner of the backup directory.

   Run the **ls -al** command to check the permissions for the backup directory. The owner of the backup directory must be user **sybase** and the write, read, and execution permissions for the backup directory must be granted. For details on how to grant these permissions, see the common commands of the Solaris OS.

4. Make sure that the password of user **sa** is changed according to the related operation guide. If the password is changed incorrectly, restore the previous configuration and then use the NMS Maintenance Suite to change the password again. For details, see "Changing the Password of the Administrator of the Database" in the *U2000 Administrator Guide*.

   ----End

7.1.2 Starting the Sybase Database Fails

The **dataserver** and **backupserver** processes cannot be found after the Sybase database is started for a period of time.

Locate and rectify the fault according to the following sequence:

Sequence	Problem Location	Troubleshooting
1	Check whether the disk usage exceeds the limit.	Rectify the fault with reference to **6.1.5 Operation Anomaly Caused by Insufficient Disk Space**.
2	Check whether the configuration file for user **sybase** is incorrect.	Rectify the fault with reference to **7.1.2.5 Incorrect Configuration File for the sybase User**.
3	Check whether there is any error message in logs.	Rectify the fault according to the following error messages: ● **7.1.2.1 Prompting Permission denied in Logs** ● **7.1.2.2 Prompting Shared memory segment *.krg is in use in Logs** ● **7.1.2.3 Prompting the Incorrect Setting of the Shared Memory in Logs** ● **7.1.2.4 Prompting the Failure of Opening lv_master in Logs**
4	The preceding measures do not work.	Contact Huawei engineers for troubleshooting.

7.1.2.1 Prompting Permission denied in Logs

Symptom

In the single-server system, the Sybase database cannot be started.

The following message is displayed in the **$SYBASE/$SYBASE_ASE/install/DBSVR.log**:

```
00:00000:00000:2010/01/07 20:04:47.92 kernel  dopen: open '/opt/sybase/data/
lv_master', Permission denied
00:00000:00000:2010/01/07 20:08:18.54 kernel  dopen: open '/opt/sybase/data/
lv_master', Permission denied
```

Possible Causes

In the preceding message, **Permission denied** indicates that the authorities to the file are insufficient, which causes that the file cannot be read. Therefore, the database server cannot be started.

CAUTION

The following operations of rectifying the fault are specific only to the single server system. If similar faults occur to the HA system, contact the local office or customer service center of Huawei for troubleshooting.

Procedure

1. Determine the user (nmsuser, **sybase**, **root**, or other names) that is used to start the Sybase. The correct user should be **sybase**.
2. Check the raw partition or the file that reports **Permission denied** in the log, and check whether the user that is used to start the database has the authorities to access the file or raw partition (a disk partition without having a file system imposed over it). If the user does not have the authorities, assign authorities to the user.

   NOTE

   The equipment files are placed in the **$SYBASE/data** directory. You can change the authorities to an equipment file by running the **chmod 755** ***equipment_file_name*** command.
3. Restart the database.

----End

7.1.2.2 Prompting Shared memory segment *.krg is in use in Logs

Symptom

In the single-server system, the Sybase database cannot be started.

The following message is displayed in the **$SYBASE/$SYBASE_ASE/install/DBSVR.log**:

```
00:00000:00000:2005/07/15 17:21:32.74 kernel  Using config area from primary master
device.
00:00000:00000:2005/07/15 17:21:33.01 kernel  Warning: Using default file '/opt/
sybase/ASE-15_0/DBSVR.cfg' since a configuration file was not specified. Specify a
configuration file name in the RUNSERVER file to avoid this message.
00:00000:00000:2005/07/15 17:21:33.13 kernel  os_create_keyfile: Shared memory
segment /opt/sybase/ASE-15_0/DBSVR.krg is in use. Check if SQL Server is already
running. If NOT remove old .srg/.krg files & restart.
00:00000:00000:2005/07/15 17:21:33.18 kernel  kbcreate: couldn't get shmid for
kernel region.
00:00000:00000:2005/07/15 17:21:33.18 kernel  kistartup: could not create shared
memory
```

Possible Causes

The Sybase database server is shut down improperly. Therefore, the DBSVR.krg and DBSVR.srg junk files exist in the **$SYBASE** or **$SYBASE/$SYBASE_ASE** directory.

CAUTION

The following operations of rectifying the fault are specific only to the single server system. If similar faults occur to the HA system, contact the local office or customer service center of Huawei for troubleshooting.

Procedure

1. Log in to the operating system as user **sybase**.
2. Run the following commands, and check whether the DBSVR.krg and DBSVR.srg files exist in the **$SYBASE** or **$SYBASE/$SYBASE_ASE** directory.

```
$ cd $SYBASE
$ ls -al
$ cd $SYBASE/$SYBASE_ASE
$ ls -al
```

3. If the DBSVR.krg and DBSVR.srg files exist, run the following commands to delete the files.

```
$ rm -rf DBSVR.krg
$ rm -rf DBSVR.srg
```

4. Restart the database.

----End

7.1.2.3 Prompting the Incorrect Setting of the Shared Memory in Logs

Symptom

In the single-server system, the Sybase database cannot be started.

The following message is displayed in the **$SYBASE/$SYBASE_ASE/install/DBSVR.log**:

```
00:00000:00000:2005/07/20 17:07:15.41 kernel  Using config area from primary master
device.
00:00000:00000:2005/07/20 17:07:16.65 kernel  Warning: Using default file '/opt/
sybase/DBSVR.cfg' since a configuration file was not specified. Specify a
configuration file name in the RUNSERVER file to avoid this message.
00:00000:00000:2005/07/20 17:07:17.39 kernel  os_create_region: can't allocate
260775936 bytes
00:00000:00000:2005/07/20 17:07:17.42 kernel  kbcreate: couldn't create kernel
region.
00:00000:00000:2005/07/20 17:07:17.42 kernel  kistartup: could not create shared
memory
```

Possible Causes

The **/etc/system** file is not configured with correct shared memory.

CAUTION

The following operations of rectifying the fault are specific only to the single server system. If similar faults occur to the HA system, contact the local office or customer service center of Huawei for troubleshooting.

Procedure

1. Add **set shmsys:shminfo_shmmax=*Memory_Size*** at the end of the **/etc/system** file. Here, *Memory_Size* stands for the value of memory(MB)x1024x1024/2.
   (1) To check the memory, run the following command as user **root**:

```
# prtdiag
```

   The terminal displays:

NOTE

The displayed message changes according to different on-site equipment configuration.

```
Memory size:2GB
```

(2) Add **set shmsys:shminfo_shmmax=*Memory_Size*** at the end of the **/etc/system** file. Here, *Memory_Size* stands for the value of memory(MB)x1024x1024/2.

For example, if the memory is 2 GB (2048MB), the value of the *Memory_Size* is 2048x1024x1024/2, that is 1073741824.

Then, add the following contents at the end of the **/etc/system** file:

```
set shmsys:shminfo_shmmax=1073741824
```

TIP

- In the case of GUI, see the methods of opening and editing a file in the *Solaris Online Help*.
- In the case of CLI, edit the file by running the **vi** command. For the specific method, see the commands that are commonly used on Solaris.

2 Restart the database.

----End

7.1.2.4 Prompting the Failure of Opening lv_master in Logs

Symptom

In the single-server system, the Sybase database cannot be started.

The following message is found in the **$SYBASE/$SYBASE_ASE/install/DBSVR.log**:

```
00:00000:00000:2005/07/20 17:43:43.65 kernel  dopen: open '/opt/sybase/data/
lv_master', No such file or directory
00:00000:00000:2005/07/20 17:43:43.65 kernel  kdconfig: unable to read primary
master device
00:00000:00000:2005/07/20 17:43:43.65 kernel  kiconfig: read of config block
failed
```

Possible Causes

The equipment file of the master database is lost.

CAUTION

The following operations of rectifying the fault are specific only to the single server system. If similar faults occur to the HA system, contact the local office or customer service center of Huawei for troubleshooting.

Procedure

1 Back up the U2000 data to the local server. For details, see the chapter "Backing Up and Restoring the U2000 Database" of the *iManager U2000 Administrator Guide*.

2 Reinstall the NMS and Sybase database. For details, see the *iManager U2000 Software Installation Guide* for the corresponding solution.

CAUTION

The U2000 monitoring may be interrupted during the database reinstallation. Therefore, ensure that the database data is backed up for data restoration.

3 Initialize the U2000 database. For details, see the chapter "Backing Up and Restoring the U2000 Database" of the *iManager U2000 Administrator Guide*.

CAUTION

Data may be lost during the database initialization. Therefore, ensure that the database data is backed up before the initialization.

4 Restore the U2000 database data. For details, see the chapter "Backing Up and Restoring the U2000 Database" of the *iManager U2000 Administrator Guide*.

5 Restart the database.

----End

7.1.2.5 Incorrect Configuration File for the sybase User

Symptom

In the single-server system, the Sybase database cannot be started.

After switching to the **sybase** user by running the **su - sybase** command, a certain user runs the **showserver** command. The query result does not contain the **dataserver** and **backupserver** processes.

Possible Causes

The following configuration files for the **sybase** user may be faulty:

- The **sybase** user group does not exist.
- The **sybase** user does not exist.
- The **.profile** file does not exist in the **home** directory of the **sybase** user.
- The **.profile** file of the **sybase** user is incorrect.

CAUTION

The following operations of rectifying the fault are specific only to the single server system. If similar faults occur to the HA system, contact the local office or customer service center of Huawei for troubleshooting.

Procedure

1 To check whether the **sybase** user group exists, run the following command as the **root** user:

```
# cat /etc/group
```

The terminal displays:

```
...... sybase::101:sybase ......
```

If **sybase** is displayed before the first **:** in the preceding message, it indicates that the **sybase** user group exists. Otherwise, run the following command as the **root** user to create the **sybase** user group manually:

```
# groupadd sybase
```

2 To check whether the **sybase** user exists, run the following command as the **root** user:

```
# cat /etc/passwd
```

The terminal displays:

```
......
sybase:x:101:102::/opt/sybase:/bin/ksh
......
```

If **sybase** is displayed before the first **:** in the preceding message, it indicates that the **sybase** user exists. Otherwise, run the following command as the **root** user to create the **sybase** user manually:

```
# useradd -d /opt/sybase -g sybase -s /usr/bin/sh sybase
```

3 To check whether the **.profile** file exists in the **home** directory of the **sybase** user, run the following command as the **root** user:

```
# su - sybase
$ cd $HOME
$ ls -a
```

The terminal displays:

```
...... .profile ......
```

If the **.profile** file is displayed, it indicates that the **.profile** file exists. Otherwise, run the following command as the **root** user to create the file manually:

```
# touch /opt/sybase/.profile
```

4 To check whether the **.profile** file is correct, run the following command as the **sybase** user:

```
$ more .profile
```

The terminal displays:

```
#!/usr/bin/sh
PS1=$
export PS1
. /opt/sybase/SYBASE.sh
LANG=C
export LANG
```

If the preceding information is displayed, it indicates that the **.profile** file is correct. Otherwise, add the following information to the **.profile** file in the **/opt/sybase/** directory as the **root** user:

```
#!/usr/bin/sh
PS1=$
export PS1
. /opt/sybase/SYBASE.sh
LANG=C
export LANG
```

5 Set the host and authorities of the **/opt/sybase/** directory to the correct values.

```
# chmod -R 755 /opt/sybase
# chown -R sybase:sybase /opt/sybase
```

6 Restart the database.

----End

7.1.3 Sybase Database Is Started Abnormally

This topic describes how to troubleshoot the startup exception of the Sybase database. Locate and rectify the fault according to the log information:

Log Information	Troubleshooting
The log indicates that the equipment file cannot be opened.	Rectify the fault with reference to **7.1.3.1 Prompting dopen: open '/opt/sybase/data/lv_LogDB_dev' in Logs**.
The log indicates **suspect**.	Rectify the fault with reference to **7.1.3.2 Prompt suspect in Logs**.
The log indicates the disk allocated for the database logs is full.	Rectify the fault with reference to **7.1.3.3 Disk of the Database Logs Is Full**.
In other cases.	Contact Huawei engineers for troubleshooting.

7.1.3.1 Prompting dopen: open '/opt/sybase/data/lv_LogDB_dev' in Logs

Symptom

In the single-server system, a message is displayed in the **$SYBASE/$SYBASE_ASE/install/DBSVR.log** indicating that the equipment file cannot be opened. The message displayed is as follows:

NOTE

The contents in **()** are explanations of the message.

```
00:00000:00001:2005/07/20 17:18:29.57 server  Activating disk 'LogDB_dev'.
00:00000:00001:2005/07/20 17:18:29.57 kernel  Initializing virtual device 13, '/
opt/sybase1192/data/lv_LogDBR6'
00:00000:00001:2005/07/20 17:18:29.57 kernel  dopen: open '/opt/sybase/data/
lv_LogDB_dev', No such file or directory
(The equipment file does not exist.)
00:00000:00001:2005/07/20 17:18:29.57 kernel  udactivate: error starting virtual
disk 13
(The equipment cannot be activated because the equipment file does not
exist.) ......
00:00000:00001:2005/07/20 17:18:46.38 kernel  udstartio: vdn 13 has not been set
up
(The equipment 13 is not activated.)
00:00000:00001:2005/07/20 17:18:46.40 server  Error: 840, Severity: 17, State: 1
(Error code)
00:00000:00001:2005/07/20 17:18:46.40 server  Device 'LogDB_dev' (with physical
name '/opt/sybase1192/data/lv_LogDB_dev', and virtual device number 13) has not
been correctly activated at startup time.  Please contact a user with System
Administrator (SA) role.
(The equipment cannot be started.)
00:00000:00001:2005/07/20 17:18:46.40 server  Unable to proceed with the recovery
```

```
of dbid <8> because of previous errors.  Continuing with the next database.
(The database cannot be restored because the equipment cannot be started.)
```

Possible Causes

The equipment file of the database is lost. The file may be deleted by mistake or lost due to the power failure.

Fault Diagnosis

To find the name of the database where the fault occurs, run the following commands as user **root**:

```
# su - sybase
$ isql -Usa -Psa's_password -SDBSVR
1> select name,status from sysdatabases
2> go
```

The terminal displays:

NOTE

Assume that the physical file of **LogDB** is deleted by mistake.

```
name                           status
 ------------------------------ ------
 Eml_multinesvrDB                   12
 FaultDB                            12
 LogDB                              76
 master                              0
 model                               0
 sybsystemdb                         0
 sybsystemprocs                      8
 tempdb                             12
```

The **status** value of **LogDB** is **76**, it indicates that the physical file of **LogDB** is deleted by mistake.

Procedure

1. To start the database, run the following commands as user **sybase**:

   ```
   $ cd /opt/sybase/ASE-*/install
   $ ./startserver -f ./RUN_DBSVR &
   $ ./startserver -f ./RUN_DBSVR_back &
   ```

2. To log in to the database, run the following command:

   ```
   $ isql -Usa -Psa's_password -SDBSVR
   ```

3. Run the following commands:

   ```
   1> sp_configure 'allow update', 1
   2> go
   1> update master..sysdatabases set status = 320 where name = 'database_name'
   2> go
   1> select name,status from sysdatabases
   2> go
   ```

   In the message displayed, if the **status** value of *database_name* to be restored is **320**, it indicates that the setting is successful.

4. Run the following commands:

   ```
   1> shutdown
   2> go
   ```

5. To start the database, run the following commands as user **sybase**:

```
$ cd /opt/sybase/ASE-*/install
$ ./startserver -f ./RUN_DBSVR &
$ ./startserver -f ./RUN_DBSVR_back &
```

6 To log in to the database, run the following command:

```
$ isql -Usa -Psa's_password -SDBSVR
```

7 Run the following commands:

```
1> dbcc dbrepair(database_name, dropdb)
2> go
```

8 Delete the database devices.

(1) To query the names of all the database devices in the database, run the following commands:

```
1> select name from sysdevices
2> go
```

The terminal displays:

NOTE

The following takes the unexpected deletion of the physical file of **LogDB** as an example.

```
name
 ------------------------------
 FaultDB_dev
 FaultDBlog_dev
 LogDB_dev
 LogDBlog_dev
 NAWdmNemgrDB_994_dev
 NAWdmNemgrDB_994log_dev
 NgwdmaNemgrDB_6154_dev
 NgwdmaNemgrDB_6154log_dev
 OAMSDB_dev
 OAMSDBlog_dev
 SchdDB_dev
 SchdDBlog_dev
 SecurityDB_dev
 SecurityDBlog_dev
 TNCOMMONDB_dev
 TNCOMMONDBlog_dev
 TNOTNDB_dev
 TNOTNDBlog_dev
 TopoDB_dev
 TopoDBlog_dev
 TransPerfDB_dev
 TransPerfDBlog_dev
 master
 mcdb_dev
 mcdblog_dev
 sysprocsdev
 tapedump1
 tapedump2
 tempdb_dev
 tempdblog_dev
```

(2) Find the names of the database devices to be deleted according to the message displayed.

The prefixes of the names of the database devices to be deleted are consistent with the name of the database to be restored. For example, the name of the database to be restored in this case is **LogDB**. Then, the names of the database devices to be deleted are **LogDB_dev** and **LogDBlog_dev**.

(3) To delete the database devices, run the following commands:

```
1> sp_dropdevice database_device_name
2> go
```

For example, the names of the database devices to be deleted in this case are **LogDB_dev** and **LogDBlog_dev**. Run the following commands:

```
1> sp_dropdevice LogDB_dev
2> go
1> sp_dropdevice LogDBlog_dev
2> go
```

9 Initialize the database. For the specific method, see the administrator guide for the corresponding version and solution.

10 Restore the database data. For the specific method, see the administrator guide for the corresponding version and solution.

----End

Suggestion and Summary

During routine maintenance, it is recommended that you comply with the precautions for the software and hardware operations mentioned in the suggestions on safe operations. In this way, you can avoid database exceptions caused by incorrect operations.

7.1.3.2 Prompt suspect in Logs

Symptom

In the single-server system, a message is displayed in the **$SYBASE/$SYBASE_ASE/install/DBSVR.log** indicating that the equipment file cannot be opened. The message displayed is as follows:

```
00:00000:00001:2005/07/20 17:33:25.71 server  Error: 926, Severity: 14, State: 1
00:00000:00001:2005/07/20 17:33:25.71 server  Database 'database_name' cannot be
opened.
An earlier attempt at recovery marked it 'suspect'.
Check the SQL Server errorlog for information as to the cause.
```

Possible Causes

The log contains **suspect**. Generally, this fault occurs because of the abnormal power failure of the server, or because the equipment file of the database is damaged or the database log is full but not cleared in a timely manner. Therefore, you need to rectify the fault manually.

CAUTION

If the **master** database is suspended, you need to re-install the database or seek advice from Sybase engineers.

Procedure

1 Log in to the operating system as user **root**.

2 To log in to the database as user **sa** , run the following commands:

```
# su - sybase
$ isql -Usa -Psa's_password -SDBSVR
```

3 To update the suspended database in the log, run the following commands:

```
1> sp_configure 'allow update', 1
2> go
1> update master..sysdatabases set status = -32768 where name = 'database_name'
```

```
2> go
1> shutdown SYB_BACKUP
2> go
1> shutdown
2> go
```

4 To restart the database server, run the following commands:

```
$ cd /opt/sybase/ASE-*/install
$ ./startserver -f ./RUN_DBSVR &
$ ./startserver -f ./RUN_DBSVR_back &
```

5 To log in to the database as user **sa** , run the following command:

```
$ isql -Usa -Psa's_password -SDBSVR
```

6 Run the following commands:

```
1> dump transaction database_name with no_log
2> go
1> sp_configure 'allow update', 1
2> go
1> update master..sysdatabases set status = 12 where name = 'database_name'
2> go
1> shutdown SYB_BACKUP
2> go
1> shutdown
2> go
```

7 To restart the database server, run the following commands:

```
$ cd /opt/sybase/ASE-*/install
$ ./startserver -f ./RUN_DBSVR &
$ ./startserver -f ./RUN_DBSVR_back &
```

8 To log in to the database as user **sa** , run the following command:

```
$ isql -Usa -Psa's_password -SDBSVR
```

9 Run the following commands:

```
1> use master
2> go
1> sp_dboption database_name,'trunc. log on chkpt.',true
2> go
1> use database_name
2> go
1> checkpoint
2> go
1> sp_configure 'allow update', 0
2> go
1> shutdown SYB_BACKUP
2> go
1> shutdown
2> go
```

10 Run the following commands to restart the database server. Then you can restore the database.

```
$ cd /opt/sybase/ASE-*/install
$ ./startserver -f ./RUN_DBSVR &
$ ./startserver -f ./RUN_DBSVR_back &
```

----End

7.1.3.3 Disk of the Database Logs Is Full

Symptom

In the single-server system, the database is started abnormally.

A message is displayed in the **$SYBASE/$SYBASE_ASE/install/DBSVR.log** indicating full log space of the database.

Possible Causes

The possible causes that result in full log space of the database are as follows:

- The log truncation is not set.
- The database is set to a small size.

Fault Diagnosis

To find the name of the database with full log space, do as follows:

1. Ensure that the U2000 application is closed and the database is started.
2. To search for the names of all the databases, run the following commands as user **root**:
   ```
   # su - sybase
   $ isql -Usa -Psa's_password -SDBSVR
   1> sp_helpdb
   2> go
   ```
3. To search for the name of the database with full log space, run the following commands:
   ```
   # su - sybase
   $ isql -Usa -Psa's_password -SDBSVR
   1> sp_helpdb database_name
   2> go
   ```
   In the message displayed, the number in the **free kbytes** column indicates the remaining space of the database log.

   NOTE

   - If the NMS of the Chinese version is installed, garbled codes may be displayed when you log in to the system by using the remote terminal login tool (CLI). Then, you need to set the encoding scheme of the remote terminal login tool to UTF-8.
   - If the remote terminal login tool does not support the ability to set the encoding scheme, log in to the system by using the GUI.
4. Find the name of the database with full log space according to the message displayed.

Procedure

1 Log in to the operating system as user **root**.

2 To log in to the database as user **sa**, run the following commands:

```
# su - sybase
$ isql -Usa -Psa's_password -SDBSVR
```

3 To update the suspended database in the log, run the following commands:

```
1> sp_configure 'allow update', 1
2> go
1> update master..sysdatabases set status = -32768 where name = 'database_name'
2> go
1> shutdown SYB_BACKUP
2> go
1> shutdown
2> go
```

4 To restart the database server, run the following commands:

```
$ cd /opt/sybase/ASE-*/install
$ ./startserver -f ./RUN_DBSVR &
$ ./startserver -f ./RUN_DBSVR_back &
```

5 To log in to the database as user **sa** , run the following command:

```
$ isql -Usa -Psa's_password' -SDBSVR
```

6 Run the following commands:

```
1> dump transaction database name with no_log
2> go
1> sp_configure 'allow update', 1
2> go
1> update master..sysdatabases set status = 12 where name = 'database_name'
2> go
1> shutdown SYB_BACKUP
2> go
1> shutdown
2> go
```

7 To restart the database server, run the following commands:

```
$ cd /opt/sybase/ASE-*/install
$ ./startserver -f ./RUN_DBSVR &
$ ./startserver -f ./RUN_DBSVR_back &
```

8 To log in to the database as user **sa** , run the following command:

```
$ isql -Usa -Psa's_password' -SDBSVR
```

9 Run the following commands:

```
1> use master
2> go
1> sp_dboption database_name,'trunc. log on chkpt.',true
2> go
1> use database_name
2> go
1> checkpoint
2> go
1> sp_configure 'allow update', 0
2> go
1> shutdown SYB_BACKUP
2> go
1> shutdown
2> go
```

10 Run the following commands to restart the database server. Then you can restore the database.

```
$ cd /opt/sybase/ASE-*/install
$ ./startserver -f ./RUN_DBSVR &
$ ./startserver -f ./RUN_DBSVR_back &
```

----End

7.2 SQL Server Database Troubleshooting

This topic describes how to troubleshoot the SQL Server database.

7.2.1 Failed to Re-install the SQL Server 2000 Database

Symptom

Re-installing the SQL server 2000 fails.

Possible Causes

The possible causes that result in the database re-installation failure are as follows:

- The path where the installation software package is located contains space, punctuations, or Chinese characters.
- The path where the database to be installed is located contains space, punctuations, or Chinese characters.
- The database is uninstalled incompletely. Therefore, junk files exist.
- The registry information is faulty or deleted incompletely.
- The computer is infected by viruses.
- The data files of database are deleted illegally.

Procedure

1. Ensure that the following paths do not contain any Chinese character:
   - The path where the installation software package is located
   - The path where the database to be installed is located
2. Ensure that the database is installed correctly according to the following method:
   (1) You need to stop the database server and exit the database service manager before uninstalling the Microsoft SQL Server 2000.
   (2) Click **Start** and choose **Control Panel**. The **Control Panel** window is displayed.
   (3) Double-click the **Add or Remove Programs** icon. The **Add or Remove Programs** window is displayed.
   (4) Select **Microsoft SQL Server 2000**, and then click **Change/Remove**.
   (5) Click **Yes**. A progress bar is displayed.
   (6) Perform the rest operations according to the prompts.
   (7) Delete the **MSSQL2000** folder in the installation directory of the database.
   (8) Delete the **Microsoft SQL Server** folder in the **Program Files** folder that is placed in the installation directory of the operating system.
   (9) Delete the **MSDesigners7** and **MSDesigners98** folders in the **Program Files\Common Files\Microsoft Shared** directory that is in the installation directory of the operating system.
   (10) Delete the following registry information.

   TIP

   For the method of opening the registries, see the *Windows Online Help*.

   a. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server
   b. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer
   c. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates\SQLServer 2000

d. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSSQLServer

e. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services \SQLSERVERAGENT

f. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services \MSSQLServerADHelper

3 After the preceding operations are performed, restart the operating system.

4 Ensure that the registries do not contain the **PendingFileRenameOperations** key value.

TIP

For the method of opening the registries, see the *Windows Online Help*.

5 **Optional:** For Windows HA system, ensure that the S disk for database data files is formatted.

6 Re-install the database.

7 If the database re-installation fails, the computer may be infected with viruses. Check for and remove the viruses by using the anti-virus software.

8 If the preceding procedure does not work, contact Huawei technical support personnel.

----End

7.2.2 How to Solve the Problem That an Attempt to Log In to the SQL Server Fails After the Windows Password Is Changed

Symptom

After the Windows password is changed, an attempt to log in to the SQL Server fails. How to solve this problem?

Possible Causes

The Windows password is different from the password of the SQL Server.

Procedure

1 Choose **Start** > **Aministrative Tools** > **Services**.

2 In the SQL Server services automatically started by Windows, right-click **MSSQLSERVER** , and then choose **Properties**. Click the **Log On** tab, select the account and change the password to the new one.

3 In the SQL Server services automatically started by Windows, right-click**SQLSERVERAGENT**, and then choose **Properties**. Click the **Log On** tab, select the account and change the password to the new one.

4 Right-click the service manager of SQL Server on the system tray of the desktop, start the **SQL Server** and **SQL Server Agent** services.

----End

7.2.3 Initializing the Database Fails

This topic describes how to troubleshoot the database initialization failure. On windows, locate and rectify the fault according to the system prompts or log information:

Current Symptom	Troubleshooting
If prompts are displayed in the DOS window, locate the fault according to the prompts.	If the following information is displayed, rectify the fault with reference to the corresponding solutions: ● **7.2.3.1 System Prompts login database failure** ● **7.2.3.4 System Prompts Incorrect Parameter of Java Virtual Machine**
If no prompt is displayed, locate the fault by querying the log information in the **nms\server\database\log** file.	If the following information is displayed, rectify the fault with reference to the corresponding solutions: ● **7.2.3.2 Prompt Failed to open the database 'xxDB' in Logs** ● **7.2.3.3 Prompt Cannot insert duplicate key in object 'TrailServiceType' in Logs**
In other cases.	Contact Huawei engineers for troubleshooting.

7.2.3.1 System Prompts login database failure

Symptom

On Windows, when the U2000 database is initialized, a message is displayed indicating **login database failure**.

Possible Causes

The possible causes that result in the database login failure are as follows:

- The alias of the database server is set incorrectly or is not set.
- The ODBC data source is configured incorrectly or is not configured.
- The database is not started.

Procedure

1 Check whether the database is started. If not, start it manually.

(1) Double-click the database icon on the taskbar of Windows. The **SQL Server Service Manager** window is displayed.

(2) Check whether the database server is started.

If **Start/Continue** is grayed out, it indicates that the database is already started. Otherwise, click **Start/Continue** to start the database server.

2 Check for and rectify the alias of the database server.

(1) Click **Start** and then choose **Programs** > **Microsoft SQL Server** > **Client Network Utility**. On the **Alias** tab page, view the alias of the database server.

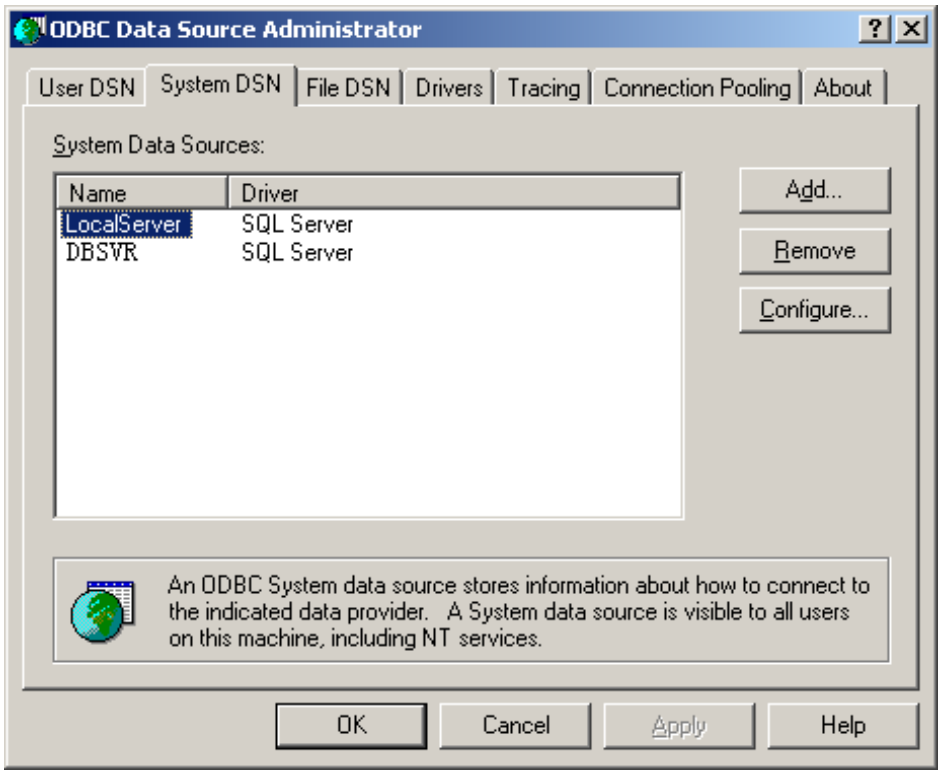
The **Server alias** should be **DBSVR**.

(2) Initialize the database again.

If the message indicating **login database failure** is displayed again, the ODBC data source may not be configured or configured incorrectly.

3 Check for and restore the configuration of the ODBC data source.

(1) Choose **Control Panel** > **Administrative Tools** > **Data Sources (ODBC)**.



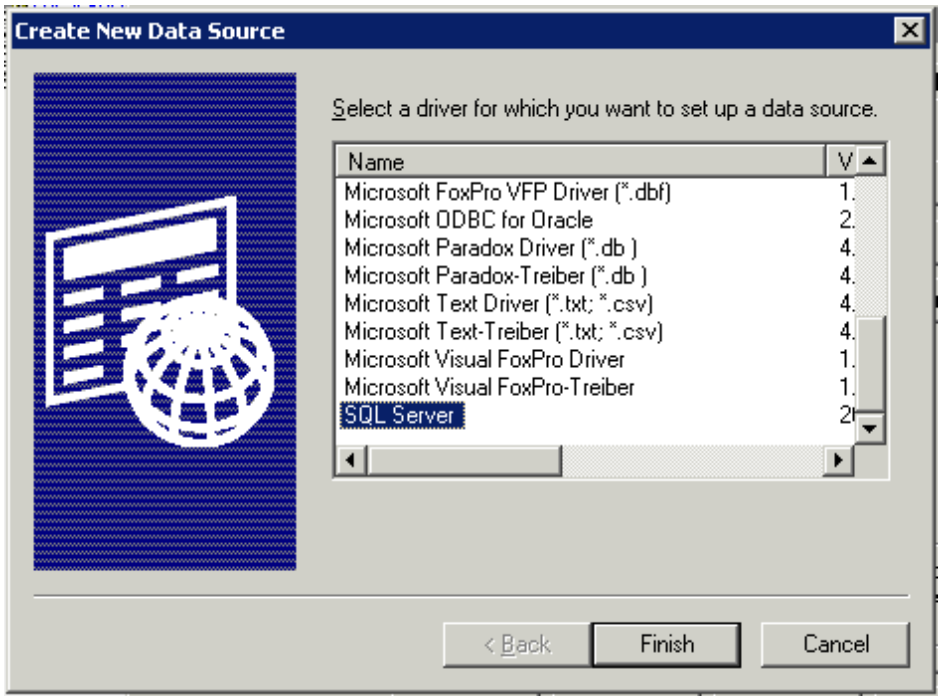
(2) On the **System DSN** tab page, view the configuration of **DBSVR**.

- If **DBSVR** already exists, select **DBSVR** and then click **Configure** to view the configuration items.
- If **DBSVR** does not exist, click **Add** to add **DBSVR**.

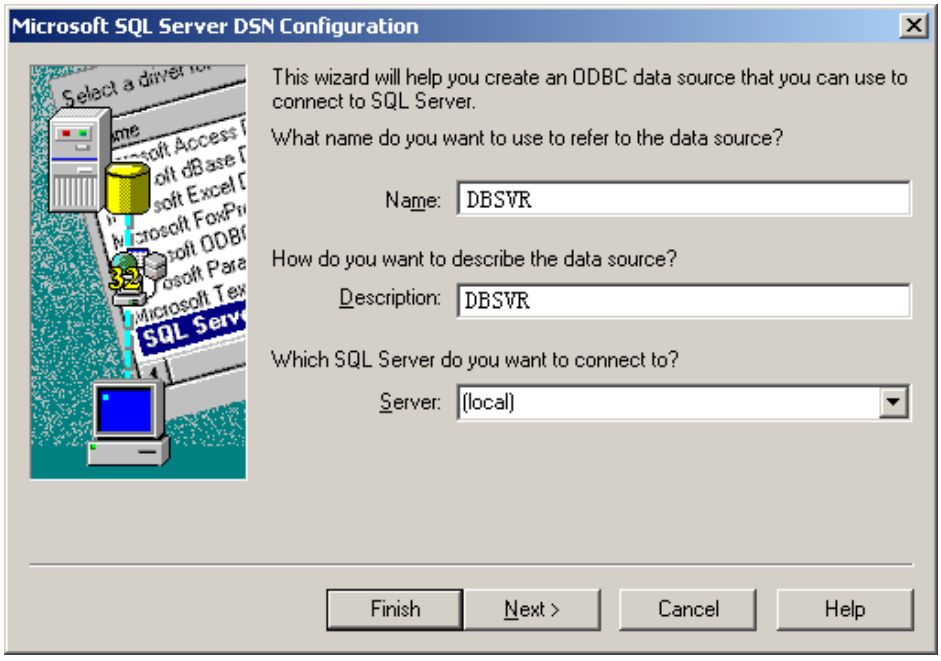
NOTE

Adding the **DBSVR** is considered as an example.

(3) On the **System DSN** tab page, click **Add**. In the **Create New Data Source** dialog box that is displayed, select **SQL Server**.

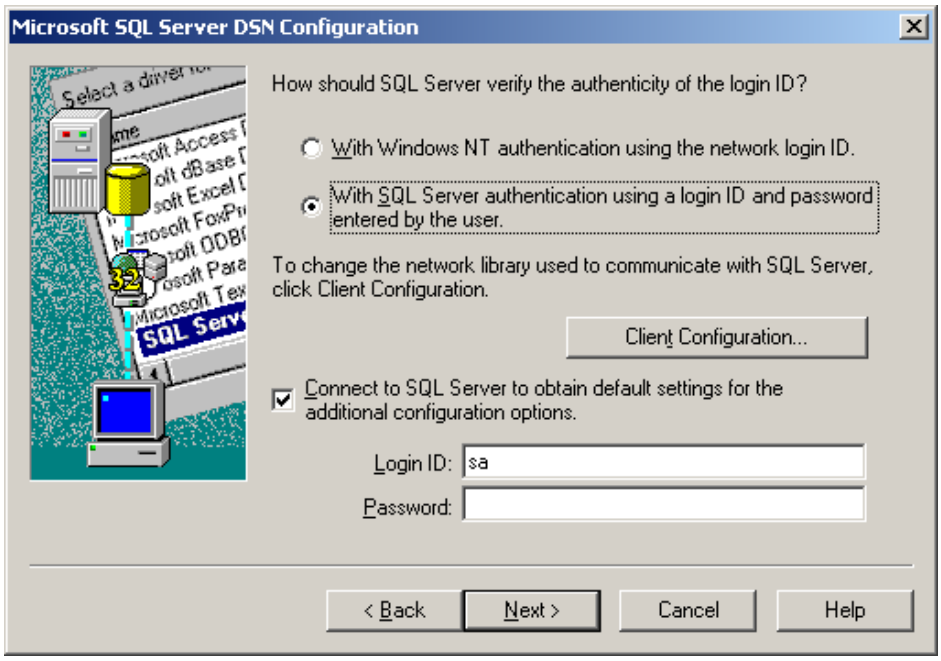


(4) Click **Finish**. In the **Microsoft SQL Server Configuration** dialog box displayed, enter the following information:



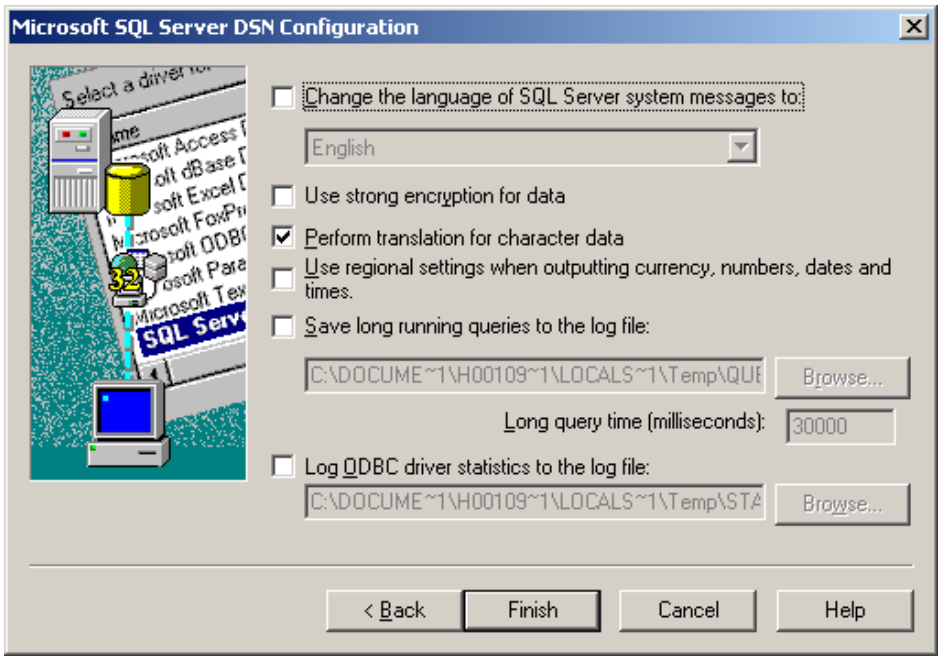
(5) Click **Next**. In the **Microsoft SQL Server Configuration** dialog box displayed, set the parameters as follows:

- Select the **With Windows NT authentication using the network login ID.** and **Connect to SQL Server to obtain default setting for the additional configuration options.** check boxes.
- In the **Login ID** field, enter the database user name **sa**. The **Password** is null. If a password is set, enter the password.

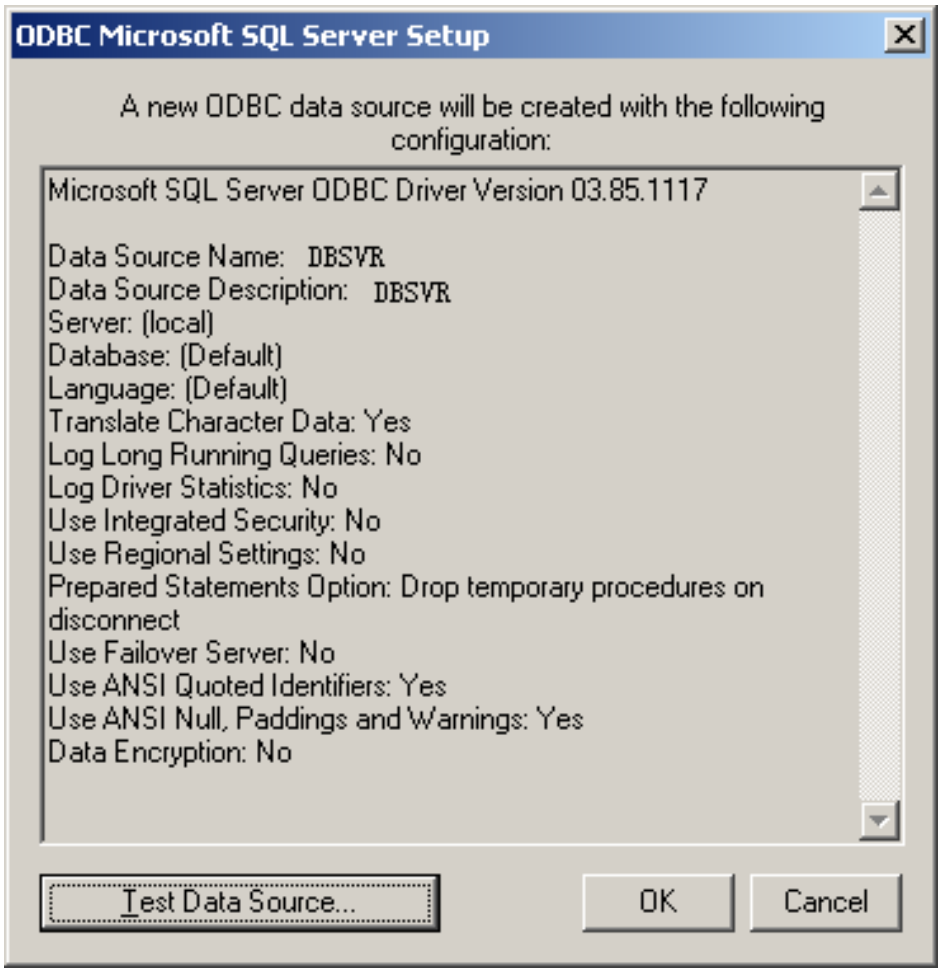


(6) Click **Next**. In the dialog box displayed, select **Change the default database to:** and then select **master** from the drop-down list.

(7) Click **Next**. In the dialog box displayed, the default settings are recommended.



(8) Click **Finish**. Then, **ODBC Microsoft SQL Setup** is displayed.



(9) Click **Test Data Source...**. Then, observe the information displayed on the screen. If **TEST COMPLETED SUCCESSFULLY!** is displayed, the U2000 application and the database server are connected.

(10) Initialize the database again.

----End

7.2.3.2 Prompt Failed to open the database 'xxDB' in Logs

Symptom

Database initialization fails. Check the logs in the **C:\HWENGR\logs\logsServer** directory and the following message is found:

```
2008-08-06_10:27:51(DBConnectionManager.getSingleConnection)    finish to
getSingleConnection
2008-08-06_10:27:51(CMSSQLConfig.mssqlSetDBOwner)    Begin to set database xxDB's
owner to NMSuser
2008-08-06_10:27:51(CMSSQLConfig.mssqlSetDBOwner)    ERROR:Set database xxDB's
owner to NMSuser failed
2008-08-06_10:27:51(CMSSQLConfig.mssqlSetDBOwner)    ERROR:java.sql.SQLException:
```

```
[Microsoft][ODBC SQL Server Driver][SQL Server] Failed to open the database 'xxDB',
because the file cannot be accessed, or the memory or the disk space is
insufficient. For details, see the SQL Server error logs.
......
```

Possible Causes

Certain database files were deleted or the disk space is insufficient.

Procedure

1. Check the disk space.
2. To delete the database manually, run the following commands:

   ```
   > isql -Usa -Psa's_password -SDBSVR
   1> drop database database_name
   2> go
   ```

   Deleting the **xxDB** database is considered as an example.

   ```
   > isql -Usa -Psa's_password -SDBSVR
   1> drop database xxDB
   2> go
   ```

3. Initialize the database again.

----End

7.2.3.3 Prompt Cannot insert duplicate key in object 'TrailServiceType' in Logs

Symptom

Database initialization fails. Check the logs in the **C:\HWENGR\logs\logsServer** directory and the following message is found:

```
2008-04-02_18:20:11(CServerConfig.RunCommand)    ERROR:Execute command failed
2008-04-02_18:20:11(CServerConfig.RunCommand)    ERROR:java.lang.Exception: MSSQL
bcp executes failed
2008-04-02_18:20:11(CServerConfig.LoadDataTable)    ERROR:Load data to
U2000DB.TrailServiceType from D:\U2000\server\database/staticdata/chinese
\TrailServiceType.dat failed
2008-04-02_18:20:11(CServerConfig.LoadDataTable)    ERROR:java.lang.Exception:
Failed to import the static data.
2008-04-02_18:20:11(CServerConfigManagement.loadAllStaticDatatable)    ERROR:load
static data failed
2008-04-02_18:20:11(CServerConfigManagement.loadAllStaticDatatable)
ERROR:java.lang.Exception: Failed to import the static data .
2008-04-02_18:20:11(CServerConfigManagement.InitializeDatabase)
ERROR:Initialize database failed
2008-04-02_18:20:11(CServerConfigManagement.InitializeDatabase)
ERROR:java.lang.Exception: Failed to import the static data.
2008-04-02_18:20:11(CServerConfigManagement.InitializeDatabase)    ERROR:Error
Message is Starting copy...
SQLState = 23000, NativeError = 2627
Error = [Microsoft][ODBC SQL Server Driver][SQL Server]Violation of UNIQUE KEY
constraint 'UQ__TrailServiceType__114A936A'. Cannot insert duplicate key in object
'TrailServiceType'.
SQLState = 01000, NativeError = 3621
Warning = [Microsoft][ODBC SQL Server Driver][SQL Server]The statement has been
terminated.
BCP copy in failed
```

Possible Causes

The character set used by the Microsoft SQL server database is not Chinese, while that used by the U2000 is Chinese.

Procedure

1. Run the following commands according to the command prompts:

```
> isql -Usa -Psa's_password -SDBSVR
1> sp_helpsort
2> go
```

The terminal displays:

```
Unicode 3.1 UTF-8 Character Set
```

NOTE

If **UTF-8** is displayed, it indicates that the character set used by the database is Chinese. Otherwise, the database needs to be installed again.

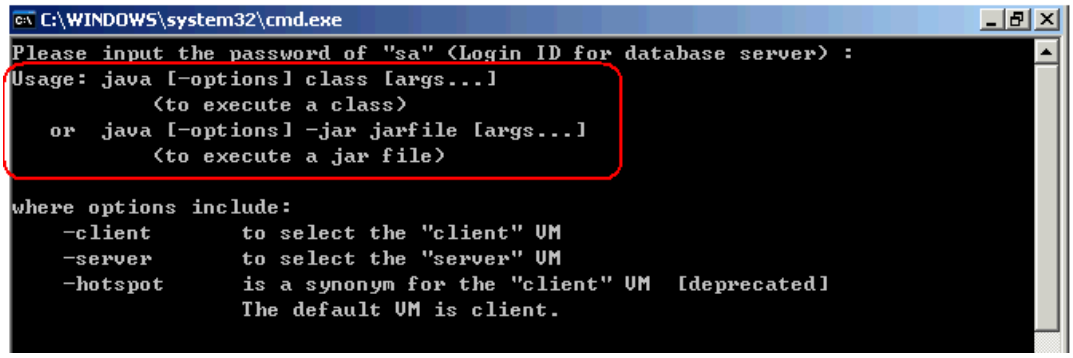
2. Initialize the database again.

----End

7.2.3.4 System Prompts Incorrect Parameter of Java Virtual Machine

Symptom

Database initialization fails. The following message is found:



Possible Causes

The symbol \ exists at the end of the value of the IMAP environment variable.

Procedure

1. Check for and restore the IMAP environment variable. For details, see **8.1.4 U2000 Environment Variable Is Set Incorrectly**.

2. Initialize the database again.

----End

7.2.4 Manually Backing up the Database Fails

Symptom

The backup file does not exist in the directory specified in the backup task.

The system prompts "Error Code: 1107329123. Failed to manually back up the database".

Possible Causes

The possible causes that result in the database backup failure are as follows:

- The database is not started.
- Full Disk Space.
- The password of user **sa** of the database is changed incorrectly.
- Another user has logged in to the NMS Maintenance Suite client.

Procedure

1. Ensure that the database is started.

   If the database icon in the Windows taskbar is displayed as  , it indicates that the database is started.

2. Check the disk space. For details, see **6.1.5 Operation Anomaly Caused by Insufficient Disk Space**.

3. Make sure that the password of user **sa** is changed according to the related operation guide. If the password is changed incorrectly, restore the previous configuration and then use the NMS Maintenance Suite to change the password again. For details, see "Changing the Password of the Administrator of the Database" in the *U2000 Administrator Guide*.

4. Ensure that all users have been logged out of the NMS Maintenance Suite client.

   ----End

7.3 Oracle Database Troubleshooting

This topic describes how to troubleshoot the Oracle database.

7.3.1 System Fails to Be Connected to the Oracle Database (Error Code: ORA-12541)

Symptom

The system displays an error message when being connected to the Oracle database.

```
ERROR:
ORA-12541: TNS:no listener
```

Possible Causes

- On the Oracle client, the listening port number set for the string in the **tnsnames.ora** file is incorrect.
- The listening service of the Oracle database is not started.

Procedure

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

   NOTE

   oracle is a user who manages the Oracle database.

2. To check the listening port number (default value: **1521**) set in the **tnsnames.ora** file on the Oracle client, run the following command:

```
$ more /opt/oracle/oradb/home/network/admin/tnsnames.ora
# tnsnames.ora Network Configuration File: /opt/oracle/oradb/home/network/admin/
tnsnames.ora
# Generated by Oracle configuration tools.

U2KDB =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = masterserver)(PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = U2KDB)
    )
  )
```

3. To view the listening service status of the Oracle database, run the following command:

```
$ lsnrctl status
...
STATUS of the LISTENER
------------------------
Alias           LISTENER
Version         TNSLSNR for Linux IA64: Version 11.1.0.7.0 - Production
Start Date      23-MAR-2010 10:16:36
...
```

   If **STATUS of the LISTENER** is displayed, it indicates that the listening service of the Oracle database has been started. If **STATUS of the LISTENER** is not displayed, run the following command to start the listening service of the Oracle database:

```
$ lsnrctl start
```

----End

7.3.2 Oracle Table Space Fails to Be Expanded (Error Code: ORA-01653)

Symptom

- The System Monitor displays a message indicating that the database space is full.
- View Oracle database logs, such as the **alert_U2KDB.log** in the **/opt/oracle/diag/rdbms/u2kdb/U2KDB/trace** path. The system displays a message indicating that the table space fails to be expanded. A sample message is as follows:

```
ORA-01653: unable to extend table SYS.T_SG1 by 4 in tablespace TBS_TEST
```

Possible Causes

- No space is available for table space expansion and the data file corresponding to table space is not automatically expanded.
- The data file is automatically expanded, but there is no space left in the file system where the data file is located.

Procedure

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

   NOTE

   oracle is a user who manages the Oracle database.

2. To connect to the Oracle database, run the following command:

   ```
   $ sqlplus / as sysdba
   ```

3. If there is remaining space in the file system where the data file is located, run the following command to modify the extended attributes of the data file.

   ```
   SQL> alter database datafile 14 autoextend on;
   ```

4. If no space is left in the file system where the data file is located, increase the size of the existing data file or add a data file for table space.

   - To increase the size of the existing data file, run the following command:
     ```
     SQL> alter database datafile 14 resize data_file_size;
     ```
     Here, *data_file_size* indicates the size of a data file, such as 500M.
   - To add a data file, run the following command:
     ```
     SQL> alter tablespace tbs_test add datafile 'data_file' size data_file_size;
     ```
     Here, *data_file* indicates the name of a data file, such as **/opt/oracle/data/test.dbf**; *data_file_size* indicates the size of a data file, such as 500M.

   ----End

8 U2000 Server Troubleshooting

About This Chapter

This topic describes how to troubleshoot the U2000 server.

8.1 Starting the U2000 Server Fails

Starting the U2000 server fails or certain processes of the U2000 are started repeatedly. On Solaris in the single server system, locate and rectify the fault according to the following sequence:

Sequence	Problem Location	Troubleshooting
1	Judge whether the fault is caused by the U2000 coredump.	Rectify the fault with reference to **8.1.1 Abnormal Termination of the Server Application**.
2	Locate and rectify the fault according to the following system prompts.	Locate and rectify the fault according to the following system prompts: ● **8.1.2 System Prompting Connection Failure to the Database** ● **8.1.3 Prompting Invalid License** ● **8.1.4 U2000 Environment Variable Is Set Incorrectly**
3	Restarting the U2000 server fails.	Contact Huawei engineers for troubleshooting.

8.1.1 Abnormal Termination of the Server Application

Symptom

The U2000 server application is terminated abnormally.

Possible Causes

The problem may be caused by the U2000 core dump.

Procedure

1 Check whether any file whose name starts with **core.** exists in the following directories.

On Solaris or SUSE Linux:

- **/opt/U2000**

- **/opt/U2000/server**
- **/opt/U2000/server/bin**

On Windows:

- **D:\U2000**
- **D:\U2000\server**
- **D:\U2000\server\bin**

NOTE

- In the case of the Solaris or SUSE Linux OS, the installation of the U2000 in the **/opt/U2000** path is taken as an example.
- In the case of the Windows OS, the installation of the U2000 in the **D:\U2000** path is taken as an example.

2 Collect the U2000 core dump file.

3 Send the collected core dump file to Huawei engineers for troubleshooting.

----End

8.1.2 System Prompting Connection Failure to the Database

Symptom

A message is displayed indicating that connecting to the database fails. In addition, the U2000 server cannot be started.

Possible Causes

- The database is not started.
- The communication connection between the database and the server is set improperly.
- The database password is illegally modified, which causes that the configuration file is damaged.
- Other problems regarding the database occur.

Procedure

- Check whether the database is started. If the database is not started, start the database manually.

  Check and start the database on Windows according to the following procedure:

  1. Double-click the database icon on the Windows taskbar.
     The **SQL Server Service Manager** dialog box is displayed.
  2. Check whether the database server is started.
     - If the **Start/Continue** option is grayed, it indicates that the database is started.
     - If the database is not started, click **Start/Continue** to start the database server.

       NOTE

       In the dialog box that is displayed, select the **Auto-start service when OS starts** option.

  Check and start the database on Solaris according to the following procedure:

  1. Log in to the operating system as user **sybase**.

NOTE

If you log in to the operating system as user **sybase** for the first time, a message is displayed asking you to set the password. For the system security, periodically change the password of user **sybase** by running the **passwd sybase** command. The password must contain a minimum of eight characters.

2. To check whether the database is started, run the following command :

```
$ cd $SYBASE/$SYBASE_ASE/install
$ ./showserver
```

Check whether the dataserver and backupserver processes are running. If these two processes do not exist, it indicates that the database process is not started. Start the database according to the following procedure:

3. To start the database, run the following commands:

```
$ cd /opt/sybase/ASE-*/install
$ ./startserver -f ./RUN_DBSVR
$ ./startserver -f ./RUN_DBSVR_back
```

4. To check whether the database process is running, run the following commands:

```
$ cd $SYBASE/$SYBASE_ASE/install
$ ./showserver
```

Check whether the dataserver and backupserver processes are running. If these two processes do not exist, it indicates that the database process is not started. If the database cannot be started, rectify the database fault with reference to **7.1.2 Starting the Sybase Database Fails**.

Check and start the database on SUSE Linux according to the following procedure:

1. Log in to the operating system as user **oracle**.

NOTE

If you log in to the operating system as user **oracle** for the first time, a message is displayed asking you to set the password. For the system security, periodically change the password of user **oracle** by running the **passwd oracle** command. The password must contain a minimum of eight characters.

2. To check whether the database is started, run the following command :

```
$ sqlplus / as sysdba
> select * from v$version;
```

The following is a display sample:

```
BANNER
--------------------------------------------------------------------------------
-------
Oracle Database 11g Enterprise Edition Release 11.1.0.7.3 - 64bit
Production
PL/SQL Release 11.1.0.7.3 - Production
CORE    11.1.0.7.3    Production
TNS for Linux: Version 11.1.0.7.3 - Production
NLSRTL Version 11.1.0.7.3 - Production
```

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

Otherwise, start the Oracle database.

3. To start the database, run the following commands:

```
> startup
```

The following is a display sample:

```
ORACLE instance started.

Total System Global Area 1610612736 bytes
Fixed Size                  2046264 bytes
```

```
Variable Size             385877704 bytes
Database Buffers         1207959552 bytes
Redo Buffers               14729216 bytes
Database mounted.
Database opened.
```

ORACLE instance started, **Database mounted**, and **Database opened** indicate that the Oracle DB is started properly.

- Check the communication connection between the U2000 and database.
  - On Windows, see **7.2.3.1 System Prompts login database failure** .
  - To log in to the Sybase on Solaris, run the following commands:

    ```
    # su - sybase
    $ cd /opt/sybase/OCS-*/bin
    $ ./isql -SDBSVR -Usa -Psa's_password
    ```

    If the following message is displayed:

    ```
    1>
    ```

    It indicates that communication between the U2000 and database is normal. Enter **quit** to exit the Sybase. If the preceding message is not displayed, you need to locate the fault of connection failure according to the log information and then rectify the fault.
  - To log in to the Oracle on SUSE Linux, run the following commands:

    ```
    # su - oracle
    $ sqlplus / as sysdba
    ```

    If the following message is displayed:

    ```
    SQL*Plus: Release 11.1.0.7.3 - Production on Mon Mar 8 15:37:13 2010

    Copyright (c) 1982, 2007, Oracle.  All rights reserved.


    Connected to:
    Oracle Database 11g Enterprise Edition Release 11.1.0.7.3 - 64bit
    Production
    With the Partitioning, Oracle Label Security, OLAP, Data Mining,
    Oracle Database Vault and Real Application Testing options

    SQL>
    ```

    It indicates that communication between the U2000 and database is normal. Enter **quit** to exit the Oracle. If the preceding message is not displayed, you need to locate the fault of connection failure according to the log information and then rectify the fault.
- The database user password is illegally modified, which causes that the configuration file is damaged.

  Re-set the database user password. For details, see *iManager U2000 Administrator Guide*.
- Other exceptions regarding the database.

----End

8.1.3 Prompting Invalid License

Symptom

A message is displayed indicating that the license of the U2000 is invalid. In this case, the U2000 cannot be started or certain functions cannot be used.

Possible Causes

- If the U2000 cannot start or certain functions cannot be used, the possible cause is that the license item is incorrect.

- If the time setting of the OS is incorrect, the license may also be invalid.

Procedure

- Check for and rectify the fault on Solaris or SUSE Linux according to the following precautions:
  1. Ensure that the date of the OS is the current date.
  2. A unique license file exists in the **/opt/U2000/server/etc/conf/license** directory.

     If more than one license files exist in the directory, you need to delete redundant license files manually.
  3. The NIC for the license application must be the same NIC that is actually used on the server.

     If the MAC addresses are different, you need to apply for a new license.
  4. The license file must be transferred in the ASCII format.

     TIP

     You can check the license file by running the **vi** command. If each line of the license file ends with the **^M** symbol, it indicates that the license file is uploaded in binary mode. You need to re-upload the license file.
  5. The authority of the U2000 is incorrect.
  6. The license file must comply with the U2000 version.
- Check for and rectify the fault on Windows according to the following precautions:

  NOTE

  Suppose that the U2000 is installed in the **D:\U2000** directory.
  1. Ensure that the date of the OS is the current date.
  2. A unique license file exists in the **D:\U2000\server\etc\conf\license** directory.

     If more than one license files exist in the directory, you need to delete redundant license files manually.
  3. The NIC for the license application must be the same NIC that is actually used on the server.

     If the MAC addresses are different, you need to apply for a new license.
  4. The license file must comply with the U2000 version.

----End

Suggestion and Summary

Do not modify the license file. Any modification made on the license file may result in the invalidity of the license.

8.1.4 U2000 Environment Variable Is Set Incorrectly

Symptom

A message is displayed indicating that the environment variable of the U2000 is set incorrectly.

Possible Causes

The environment variable is lost or modified.

Procedure

1. Check the environment variable of the U2000. Refer to *iManager U2000 Software Installation Guide* for the corresponding solution.
   - On Windows, right-click **My Computer** on the desktop and choose **Properties** from the shortcut menu. On the **Advanced** tab page, click **Environment variable** to query the value of **IMAP**, **IMAPROOT**, **OSSROOT**, and **NMSROOT** etc.
   - On Solaris or SUSE Linux, run the following command as user **nmsuser** to query the value. Take **IMAP** for a example.
     ```
     $ echo $IMAP
     ```
2. Check and rectify the environment variable of the U2000.
   - On Windows: Assume that the U2000 is installed in the **D:\U2000** directory. Then, **IMAP=D:\U2000\server\etc\conf**. Otherwise, re-set the environment variable of the U2000 manually.
   - On Solaris or SUSE Linux: Assume that the U2000 is installed in the **/opt/U2000** directory. Then, the value of the **$IMAP** is **/opt/U2000/server/etc/conf** by default. Otherwise, re-set the environment variable of the U2000 by running the following command as user **nmsuser**.
     ```
     $ IMAP=/opt/U2000/server/conf;export IMAP
     ```

----End

8.1.5 Startup Failure Because of the Authority Problem of the U2000 Installation Path

Symptom

After the U2000 Solaris workstation is restarted, the U2000 services fail to be started.

Possible Causes

This is caused by the authority problem of the U2000 installation path. You can change the owner of the U2000 installation path to solve this problem.

Procedure

1. Log in to the Solaris OS as the **root** user.
2. Change the owner of the U2000 installation path to **nmsuser**. Then, run the following commands in the CLI:
   ```
   # cd /opt
    # chown -R nmsuser U2000
   ```
3. Restart the U2000.

----End

8.2 Failure to Start Certain Processes of the U2000 Server

Symptom

On the System Monitor client, certain processes of the U2000 server are not running.

Possible Causes

- The server IP address is changed incorrectly. As a result, the configuration of IP addresses in certain processes is not refreshed accordingly.
- User **root** is used to start these processes but exits abnormally before the processes are started.
- These processes are not configured properly. For example, the NBI processes are not configured in advance.
- Licenses are not obtained for the relevant functions.
- Ports are occupied.
- On Windows OS, database software such as the Sybase client is installed on the U2000 server. An error occurs when processes access the database.

Procedure

1. On the System Monitor client, manually start the processes that are currently not started to check whether the failure recurs or whether relevant messages are displayed.
2. Restart the NMS and check whether the processes are started.
3. Check whether the server IP address is changed. If the IP address is changed, make sure that it is changed according to the related operation guide. If the IP address is changed incorrectly, restore the previous configuration and then change the IP address again. For details, see section "Changing the System IP Address and Host Name" in the *U2000 Administrator Guide*.

   NOTE

   In a Windows-based single-server system, you must synchronize the network configuration upon any changes on the network configuration of the U2000 server, as follows:

   On the **Server** tab page, right-click the server to be configured and choose **Synchronize the network configuration** from the shortcut menu. Click **OK**. Then, restart the OS.
4. Ensure that licenses are obtained for the relevant functions.
5. If user **root** is used to start these processes but exits abnormally before the processes are started, do as follows:
   (1) Start the processes as user **root** and exit after the processes are started.
   (2) Restart the OS.
6. If a process, such as the CORBA NBI process, fails to be started, check the NBI settings or re-configure the NBI.
7. Check whether the ports used by these processes are occupied.
8. If the server is switched off illegally or powered off or the database has been restored, it is recommended that you initialize the database and restore data. Then, restart the NMS server.
9. Uninstall the Sybase client if Windows OS is installed and database software such as the Sybase client are installed on the U2000 server.
10. If this issue persists after the preceding operations, contact Huawei engineers for help.

----End

Suggestion and Summary

- When changing the IP address, follow the related operation guide. Otherwise, the U2000 may malfunction.
- It is recommended that you start or stop the U2000 as user nmsuser.
- On Windows OS, do not install database software such as the Sybase client on the U2000 server.

8.3 Abnormal NMS Functions Due to Modified OS Time

Symptom

The modification made on the OS time results in the abnormal running of certain NMS functions.

Possible Causes

If the system time of the server is modified while the NMS is running, the whole system looks normal. Some functions based on timer principles, however, may be affected, such as the scheduled dump function of the security Daemon.

Procedure

- Shut down the NMS and the database, and then restart the server.

  NOTE

  Set the correct system time of the server when installing the NMS. Never modify it while the NMS is running. If needed, first exit the NMS server, then modify the system time and restart the NMS server.

----End

8.4 U2000 Runs Slowly

Response to certain operations on the U2000 is slow. For example, opening or closing a window takes more than three seconds.

Locate and rectify the fault according to the following sequence:

Sequence	Problem Location	Troubleshooting
1	Check whether the number of non-gateway NEs managed by the gateway NE exceeds the limit. Generally, each gateway NE is recommended to support a maximum of 50 non-gateway NEs (including the non-gateway NEs that use the extended ECC to connect to the gateway NE). If the number of non-gateway NEs exceeds 60, it is recommended that the number of gateway NEs be increased. Otherwise, ECC congestion may occur easily, which causes slow response to operations in the user interface.	Contact Huawei engineers for network division, ECC reconstruction, and DCN reconstruction.
2	Check whether a large number of abnormal events are reported to the U2000.	Rectify the fault according to the abnormal events.
3	Check whether the communication between the U2000 and gateway NEs is normal. If a large packet loss ratio (such as 40% or above) exists in the network, the data packets need to be retransmitted. In this case, the response speed to the commands that are delivered to the transmission equipment by the U2000 is greatly affected. Therefore, the response to the operations in the user interface is slow.	Restore the communication connection between the U2000 and gateway NEs. You can rectify the fault with reference to **5.3 A Large Number of Non-GNEs on the U2000 Are Disconnected**.
4	Check whether the operating system is normal. If the operating system runs at a low speed or crashes or is restarted frequently, the problem may be caused by exceptions of the operating system.	If the operating system runs abnormally, rectify the fault with reference to **6.1.1 Starting the Operating System Fails**.
5	Check whether the disk usage exceeds the limit. Normally, the disk space occupancy should be 80% or below.	If the disk space exceeds the normal value, rectify the fault with reference to **6.1.5 Operation Anomaly Caused by Insufficient Disk Space**.

Sequence	Problem Location	Troubleshooting
6	Check the hardware performance of the U2000 server.	Rectify the fault with reference to **6.1.6 Slow Running of the System Caused by Insufficient Memory** and **6.1.7 Slow Running of the System Caused by High CPU Usage**.
7	The preceding measures do not work.	Contact Huawei engineers for troubleshooting.

9 Faults of the U2000 Client

About This Chapter

This topic describes how to troubleshoot the faults of the U2000 client.

9.1 Starting the U2000 Client Fails

Symptom

A certain user double-clicks the shortcut icon of the U2000 client, but the login interface cannot be displayed.

Possible Causes

The possible causes that result in the U2000 client startup failure are as follows:

- The files of the operating system and client are abnormal.
- The shortcut icon on the desktop is not updated after upgrade.
- The virtual memory is not set. This may be caused by illegal installation of the U2000 client.

Procedure

1. If a prompt is displayed, locate and rectify the fault according to the prompt information.
2. Uninstall the U2000 client and then install it again. For details, see the installation guide for *iManager U2000 Client Installation Guide* .

----End

9.2 U2000 Client Login Failure

Symptom

The U2000 client fails to log in to the U2000 server after the user name and password are entered in the login interface.

Possible Causes

The possible causes that result in the U2000 client login failure are as follows:

- The U2000 server is faulty.
- When the server is installed in the Windows OS, the ODBC data source is configured incorrectly or not configured on the U2000 server.
- The network between the client and server is faulty.
- The port between the client and server is shielded by firewall or virus.
- The version of the client is inconsistent with that of the server.
- The communication protocol used by the client is inconsistent with that used by the server.
- The user that logs in to the client is locked. This may be caused by a number of failed login attempts.
- The number of clients allowed in the license is restricted.
- The client access control is set, and the IP address of the client is not in the permitted range.

- The setting of the system time of the client is incorrect.

Procedure

1. If a prompt is displayed, locate and rectify the fault according to the prompt information.
2. Check whether the server runs in the normal state. To be specific, ensure that the server runs in the normal state and the space of server disks is not full.
3. Choose **Help** > **About** on the U2000 server to check the number of clients allowed in the license.

   If the number of clients to log in exceeds the maximum number of clients allowed in the license, apply for a new license and update the U2000 license. For details, see the method in the installation guide for the corresponding version and solution.
4. If the U2000 server is installed in the Windows OS, check and restore the ODBC data source settings on the U2000. For details, see Step 3 in **7.2.3.1 System Prompts login database failure** .
5. Check whether the versions of the client and server are consistent. If the versions are inconsistent, replace the client with a version that is consistent with the server version, and then log in to the client again.
6. Check whether the communication protocols used by the client and the server are consistent. If the protocols are inconsistent, modify the protocols so that the protocols are consistent.

   TIP

   Log in to the **Sysmonitor Client** on the server, and choose **System** > **Communication Settings**. In the dialog box displayed, view the communication mode of the server.
7. Check the network between the client and server.

   Generally, the communication bandwidth between the client and server is at least 2 Mbit/s and the packet loss ratio is smaller than 0.1%.

   - To check the network between the client and server, run the following command on Windows:
     ```
     > ping -t IP_address_of_the_NMS
     ```
   - To check the network between the client and server, run the following command on Solaris:
     ```
     # ping -s IP_address_of_the_NMS
     ```
   - To check the network between the client and server, run the following command on SUSE Linux:
     ```
     # ping IP_address_of_the_NMS
     ```
8. Check whether the port between the client and server is shielded by firewall or virus. If the client installed on the computer where the server belongs can log in to the server, but other clients cannot log in, check the settings of the port and firewall.
9. Check whether the client access control is set.

   On the U2000, you can set the client IP addresses that can be accessed. If the IP address of a client is not in the permitted range, the client cannot access the server. For details, see "Setting the Access Control List" in the chapter "Security Management" of the *iManager U2000 Administrator Guide*.
10. If the number of failed login attempts by using the same user exceeds 3, the login authority of the user is locked.

    You can log in to the client again in 30 minutes (default) or unlock the user as another user that has the authority, such as user **admin**.

11 Check whether the system time is the current time. If not, modify the system time.

----End

9.3 The User Account for Logging In to the U2000 Client Is Locked

Symptom

When a user enters the user name and password in the login dialog box of the U2000 client, the system displays a message indicating that the user account is locked.

Possible Causes

A user tries to log in to the U2000 server using an invalid password for three times continuously.

Procedure

1 Check whether the user is an illegal user who wants to invade the U2000.

2 If the locked legal user is not user **admin**, the user account can be unlocked by user **admin**.

(1) Choose **Administration** > **NMS Security** > **NMS User Management** from the main menu.

(2) In the **Security Object** navigation tree, expand the **Users** node. Right-click a user and choose **Set Password**.

(3) In the **Set New Password** dialog box, enter the new password twice, and then click **OK**.

3 If the legal user forgets the password, user **admin** can initialize the database for the user.

(1) Choose **Administration** > **NMS Security** > **NMS User Management** from the main menu.

(2) In the **Security Object** navigation tree, click the **Users** node, and then click the **All User** tab.

(3) Right-click a locked user and choose **Unlock**.

4 If the locked user is user **admin**, the system automatically unlocks the user account after 30 minutes (default value).

----End

9.4 U2000 Client Runs Abnormally

Symptom

The U2000 client is started repeatedly and the operations are interrupted.

Possible Causes

The computer may be infected with viruses.

Procedure

1 Check for and remove the viruses with antivirus software.

2 Restart the U2000 client.

----End

9.5 U2000 Client Exits Abnormally Because of Inappropriate Input Method Editor Software

Symptom

In the case where **Intelligent ABC Input Method Editor** is used, a U2000 client exits abnormally and the GUI disappears.

Possible Causes

Certain software, such as **Intelligent ABC Input Method Editor**, conflicts with the Java Development Kit (JDK). Using these software may cause the core dump of the JDK, and as a result the U2000 client exits abnormally. This fault occurs due to a defect of the **Intelligent ABC Input Method Editor** software.

Procedure

1 Use another input software, such as **Google Pinyin Input Method Editor**.

2 Restart the U2000 client.

----End

9.6 The NE Manager GUI of Certain Equipment Is Displayed Abnormally on the U2000 Client

Symptom

On the U2000 client, the NE manager GUI of certain equipment is grayed out or displayed abnormally.

Possible Causes

For the NE manager of certain equipment such as the equipment of the PTN series, RTN series, NG WDM series, and SLM 3160 series, the browser settings result in abnormal display of the GUI.

Procedure

1 Check whether the browser settings comply with the standards. For the Windows OS, the default browser needs to be Microsft Internet Explorer; for the Solaris OS, the default browser needs to be Mozilla browser.

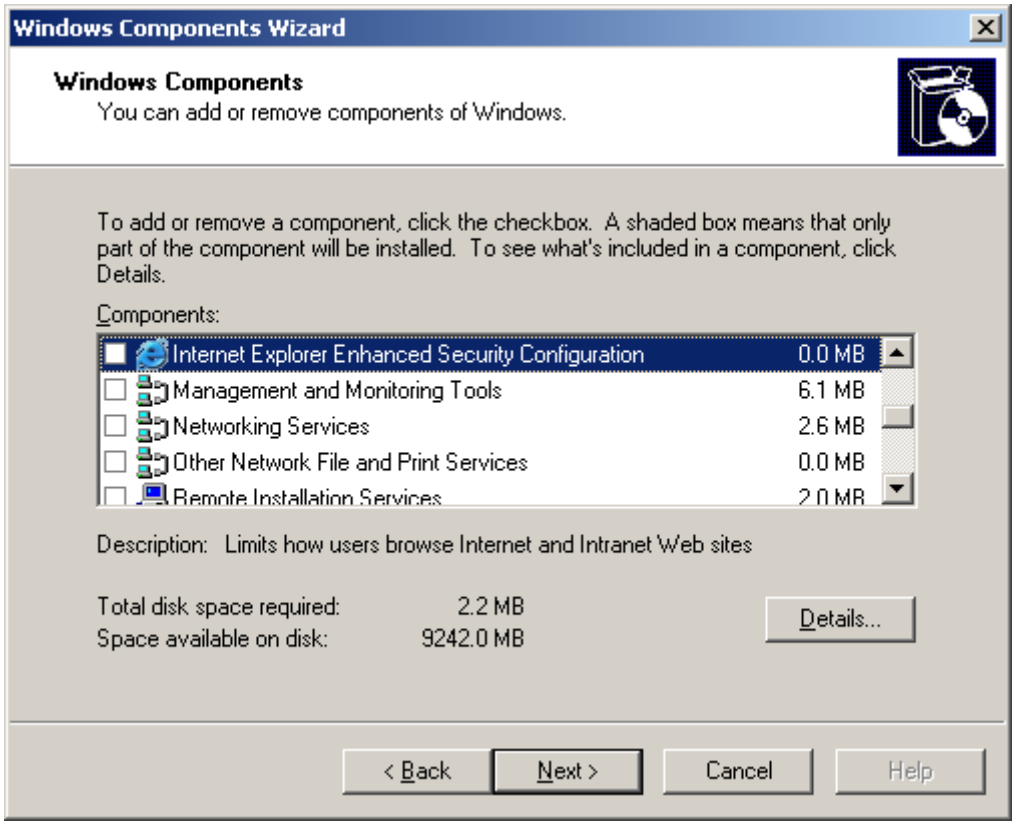
2 Check the version of Internet Explorer in the Windows OS. If the security level of Internet Explorer is set to high, the running of scripts is affected and the GUI becomes grayed out. To make the GUI display normally, you need to set the security level of the Internet Explorer to **Medium** or a lower level. In the Windows 2003 OS, the function of Internet Explorer enhanced security settings is installed by default. This function results causes the security level to remain high. Therefore, you need to cancel the function as follows:

(1) Choose **Start** > **Control Panel**. The **Control Panel** dialog box is displayed.

(2) Double-click the **Add or Remove Programs** icon. The **Add or Remove Programs** dialog box is displayed.

(3) Click the **Add/Remove Windows Components** icon. The **Windows Components Wizard**.

(4) Clear the selection of the check box to the left of **Internet Explorer Enhanced Security Configuration**.



NOTE

By default, the check box is selected, which indicates that the security level of the Internet Explorer is high.

(5) Click **Next**.

(6) Click **Finish**.

(7) Double-click the **Internet Explorer** icon on the desktop to open the Internet Explorer.

(8) Choose **Tool** > **Internet Options**.

(9) In the **Internet Options** dialog box, select **Security**. Then, move the slider to set the security level of Internet Explorer to **Medium** or a lower level.

(10) Click **Apply**.

(11) Click **OK**.

3 Check whether Internet Explorer is configured with the proxy server. If Internet Explorer is configured with the proxy server, cancel the proxy server or disable the connection to the U2000 server through the proxy server.

4 Check the installation directory of the U2000 client. The directory name contains only the letters, numbers, and underscores (_) and cannot contain the space or bracket.

----End

9.7 Connection Between the U2000 Client and Server that Are Running on the Same Machine Is Interrupted for a Short Period After a Network Cable Is Removed

Symptom

The U2000 client and server are running on the same machine. If a network cable is removed from the server, the U2000 client is disconnected from the server for a short period. On the U2000 client, a message is displayed as follows:

```
The server is disconnected. It is trying to reconnect...
```

Wait about five seconds. The connection then automatically recovers.

Possible Causes

When the U2000 client and server are running on the same machine, a network adaptor is selected as the communication link between the client and server. If a network cable is removed from the server, the connection between the client and server may be interrupted. This is because the client may currently use the network adapter that is connected to this network cable to communicate with the server.

Procedure

1 Wait about five seconds. The U2000 client automatically reconnects to the server.

----End

Suggestion and Summary

- This problem arises only when the U2000 client and the server are installed on the same machine. Using an independent remote client to log in to the U2000 server is recommended.
- After the NMS is restarted, do not remove any network cable at random. It is recommended that hardware be properly connected before the NMS is installed.

10 Veritas HA System Troubleshooting

About This Chapter

This topic describe how to troubleshoot the Veritas HA system.

10.1 Troubleshooting Policies for the Veritas HA System

This topic describes the confirmation of the faults that commonly occur in the Veritas high availability (HA) system and the troubleshooting policies.

10.1.1 Confirming the System Status

You need to check whether the HA system is in the dual-host state or in the healing state before you determine which fault recovery strategy to adopt.

NOTE

- If the server is configured with one network card, the **Host name** is the Host IP address of the master server. In this example, the **Host name** of the master servers are **129.9.1.1** and **129.9.1.2**.
- Run the following commands to check the RVG and replication status on Windows HA system:
  > **vradmin -g datadg printrvg datarvg**
  > **vxrlink -g datadg -i 2 status datarlk**

In a Normal State

Run the following command on the master server of primary site to check the system status:

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

The following information appears.

```
Replicated Data Set: datarvg
Primary:
  Host name:                    129.9.1.1
  RVG name:                     datarvg
  DG name:                      datadg
  RVG state:                    enabled for I/O
  Data volumes:                 1
  VSets:                        0
  SRL name:                     srl_vol
  SRL size:                     1.00 G
  Total secondaries:            1

Secondary:
  Host name:                    129.9.1.2
  RVG name:                     datarvg
  DG name:                      datadg
  Data status:                  consistent, up-to-date
  Replication status:           replicating (connected)
  Current mode:                 asynchronous
  Logging to:                   SRL
  Timestamp Information:        behind by 0h 0m 0s
```

Check whether the displayed information about the **Data status** is **consistent, up-to-date** and that of **Replication status** is **replicating (connected)**. If yes, it indicates that the replication relation between the active server and the standby server is normal.

In a Dual-Host State

Run the following command on the master server of primary site to check the system status:

```
# vradmin -g datadg repstatus datarvg
Replicated Data Set: datarvg
Primary:
Host name:         129.9.1.1
RVG name:          datarvg
DG name:           datadg
RVG state:         disabled for I/O
Data volumes:      1
SRL name:          srl_vol
SRL size:          1.00 G
Total secondaries: 1

Secondary:
Host name:         129.9.1.2<unreacheable>
RVG name:          datarvg
DG name:           datadg
Replication status: paused due to network disconnection
Current mode:      asynchronous
Logging to:        SRL
Timestamp Information: N/A
Config Errors:
129.9.1.2:         Pri or Sec IP not available or vradmind not running
```

Run the following command on the master server of secondary site to check the system status:

```
# vradmin -g datadg repstatus datarvg
Replicated Data Set: datarvg
Primary:
Host name:        129.9.1.2
RVG name:         datarvg
DG name:          datadg
RVG state:        enabled for I/O
Data volumes:     1
SRL name:         srl_vol
SRL size:         1.00 G
Total secondaries: 1
Config Errors:
129.9.1.1: Pri or Sec IP not available or vradmind not running
```

It indicates that the system is in the dual-host state.

Because of the following causes, the heartbeat connection between the primary and secondary sites is interrupted, the standby server is started, and the system is in the dual-host state:

- Corruption of the network card used for the communication between the two sites
- Fault in DCN between the primary and secondary sites
- Incorrect configuration of firewall between the primary and secondary sites

In the dual-host state, the following situation occurs on the client:

The NE users repeatedly force each other to log out. In this situation, where the server is in the dual-host state, shut down the U2000 applications on the primary site and connect to the secondary site.

When the primary site and the communication between the primary and secondary sites restore to normal, perform incremental or full synchronization on the site with updated data.

NOTE

- In the dual-host state, if the U2000 client connects to the secondary site, perform synchronization on the secondary site.
- In the dual-host state, if the U2000 client is still running on the primary site, perform synchronization on the primary site.

In a Healing State

Run the following command on the master server of primary and the secondary site to check the system status:

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

If the on-screen terminal output contains the **acting secondary** information as follows, it can be confirmed that the system is running in a healing status. No data is replicated. (Usually because the secondary site takes over forcibly, the network between the primary site and the secondary site returns to normal.)

```
Replicated Data Set: datarvg
Primary:
Host name:        129.9.1.2
RVG name:         datarvg
DG name:          datadg
RVG state:        enabled for I/O
Data volumes:     1
SRL name:         srl_vol
SRL size:         1.00 G
Total secondaries: 1

Primary (acting secondary):
Host name:        129.9.1.1
RVG name:         datarvg
DG name:          datadg
Data status:      consistent, behind
Replication status: logging to DCM (needs failback synchronization)
Current mode:     asynchronous
Logging to:       DCM (contains 0 Kbytes) (failback logging)
Timestamp Information: N/A
Config Errors:
129.9.1.1:        Primary-Primary configuration
```

10.1.2 Detailed Fault Recovery Strategies for HA System

This section describes the fault recovery strategies for different cases of the primary and secondary site status.

Procedure

- The network is disconnected and the system runs in a dual-host status.
  1. Restore network communication, the system changes from the dual-host state to the healing state. .
  2. Log in to the NMS Maintenance Suite client.
  3. Choose **Deploy** > **Force Active of Local Site** to restore data replication relations. The secondary site becomes the active site after the operation.
- The primary site is unavailable, and the secondary site is forced to take over.
  1. Log in to the NMS Maintenance Suite client.

2. Choose **Deploy** > **Force Active of Local Site** to restore data replication relations. The secondary site becomes the active site after the operation.

- The primary site is available, but the secondary site is unavailable.
  1. Recover the secondary site.
  2. Log in to the NMS Maintenance Suite client.
  3. Choose **Deploy** > **Force Active of Local Site** to restore data replication relations. The secondary site becomes the active site after the operation.
- If neither the primary site nor the secondary site is available, reinstall the system.

----End

10.1.3 Common Troubleshooting Solutions

This topic describes common troubleshooting solutions to the high availability (HA) system.

10.1.3.1 Logging In to the MSuite Client

This topic describes how to log in to the MSuite client.

Prerequisite

The MSuite server must be started.

Procedure

1. On a computer installed with the MSuite client, double-click the **U2000 NMS Maintenance Suite** shortcut icon on the desktop and then wait about one minute. The **Login** dialog box is displayed.

   NOTE

   - In Solaris OS, log in to the Java desktop system as user **nmsuser**. Otherwise, the **U2000 NMS Maintenance Suite** shortcut icon is not displayed on the desktop. To start the MSuite client by running commands, run the following commands as user **nmsuser**:
     ```
     cd /opt/U2000/engineering
     ./startclient.sh
     ```
   - In SUSE Linux OS, log in to GUI-based desktop system as user **root**. Otherwise, the **U2000 NMS Maintenance Suite** shortcut icon is not displayed on the desktop. To start the MSuite client by running commands, you need to run the following command as the **nmsuser** user:
     ```
     cd /opt/U2000/engineering
     ./startclient.sh
     ```

2. Set the login parameters.

   The login parameters are described as follows:

   - IP Address:
     - To log in to the local MSuite server, use the default IP address **127.0.0.1**.
     - To log in to the remote MSuite server, enter the IP address of the computer where the MSuite server is installed. If multiple IP addresses are configured for the computer, use the NMS application IP address.
   - Port No.: The default port ID is **12212**. There is no need to change the default value during login but ensure that the port is not occupied.
   - User Name: The default user name is **admin**.
   - Password: The default password is **admin**.

3. Click **Login**.

   NOTE

   - When you log in to the MSuite client, a progress bar is displayed showing the progress of querying components and instances. Wait until the operation is complete.
   - The MSuite works in single-user mode. Specifically, only one MSuite client can log in to the MSuite at one time.

----End

Exception Handling

If a dialog box is displayed during the login, indicating that network configuration information is inconsistent and re-synchronization is required after login, read through the message to learn the server that needs to be synchronized. Then, synchronize the network configuration, for details, see **10.1.3.2 Synchronizing Network Configurations**.

10.1.3.2 Synchronizing Network Configurations

This topic describes how to synchronize network configurations. When a network configuration of the NMS server changes, you need to synchronize the network configuration so that the IP addresses of the MSuite and server are synchronized. Otherwise, the system displays a failure message during the login to the MSuite client.

Prerequisite

- Ensure that the NMS server programs are already stop.
- Ensure that the database is running.
- In a high availability system, delete the high availability relationship between the primary and secondary sites. For details, see **10.1.3.4 Deleting the HA Relationship Between the Primary and Secondary Sites**. Then, log in to both the primary and secondary sites to synchronize network configurations.

Procedure

1. Log in to the MSuite client. For details, see **10.1.3.1 Logging In to the MSuite Client**.
2. On the MSuite client, click the **Server** tab.
3. Right-click the server whose network configuration needs to be synchronized and choose **Synchronize Network Configuration** from the shortcut menu. A dialog box is displayed for you to confirm the operation.
4. Click **OK**. A progress bar showing the synchronization progress is displayed.
5. When the system displays "Synchronize network configuration success", click **OK**.

----End

Follow-up Procedure

In a high availability system, reestablish the high availability relationship between the primary and secondary sites after synchronizing network configurations.

1. On the primary and secondary sites, do as follows to check whether the VCS service has been started:
   ```
   # ps -ef | grep had
   ```
   The following information is displayed:
   ```
   root  5852     1   0 07:14:51 ?           0:00 /opt/VRTSvcs/bin/hashadow
    root  5842     1   0 07:14:45 ?           1:36 /opt/VRTSvcs/bin/had -onenode
   ```
   NOTE

   If the displayed information contains **/opt/VRTSvcs/bin/hashadow** and **/opt/VRTSvcs/bin/had -onenode**, the VCS service has been started. If the VCS service has not been started, run the **hastart -onenode** command on the primary and secondary sites to start the VCS service.
2. Reestablish the high availability relationship between the primary and secondary sites. For details, see **10.1.3.3 Establishing the HA Relationship Between the Primary and Secondary Sites**.

10.1.3.3 Establishing the HA Relationship Between the Primary and Secondary Sites

This topic describes how to synchronize the primary and secondary sites. In a high availability system (Veritas hot standby), after installing the U2000 at the primary and secondary sites, synchronize the primary and secondary sites to configure the primary and secondary sites as an HA system.

Prerequisite

- All the MSuite servers on the servers of the primary and secondary sites must be started.
- The subsystems, deployed instances, and passwords of the administrator and NMS user of the database on the primary and secondary sites must be consistent.
- In a distributed system, the slave servers at the primary and secondary sites must be of the same quantity and correspond to each other.

Context

In a centralized system, log in to only the MSuite server at the primary site to perform the operation described in this topic. In a distributed system, log in to only the MSuite server of the master server at the primary site to perform the operation described in this topic.

Procedure

1. Log in to the MSuite client. For details, see **10.1.3.1 Logging In to the MSuite Client**.
2. Choose **Deploy** > **Synchronize Primary and Secondary Sites** from the main menu. The **Synchronize the primary and secondary sites** dialog box is displayed.
3. Enter the IP address of the remote server.

   NOTE

   Remote IP indicates the system IP address of the secondary site. In a distributed system, enter the system IP address of the secondary sitemaster server.
4. Click **OK**. A progress bar is displayed indicating the synchronization progress between the primary and secondary sites. Wait approximately 20 minutes until a dialog box is displayed indicating that the synchronization is completed.
5. Click **OK**. The synchronization between the primary and secondary sites is complete.
6. Run the following command repeatedly to check the status of data replication.
   - In Solaris or SUSE Linux OS, run the following command:

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

     A message similar to the following will be displayed:

     ```
     Replicated Data Set: datarvg
     Primary:
       Host name:                    129.9.1.1
       RVG name:                     datarvg
       DG name:                      datadg
       RVG state:                    enabled for I/O
       Data volumes:                 1
       VSets:                        0
       SRL name:                     srl_vol
       SRL size:                     1.00 G
       Total secondaries:            1

     Secondary:
       Host name:                    129.9.1.2
       RVG name:                     datarvg
       DG name:                      datadg
       Data status:                  inconsistent
       Replication status:           resync in progress (autosync)
       Current mode:                 asynchronous
       Logging to:                   DCM (contains 28742784 Kbytes)
     (autosync)
       Timestamp Information:        N/A
     ```

NOTE

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

- In Windows OS, run the following command:

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

  A message similar to the following will be displayed:

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

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

----End

Operations Through the CLI

On Solaris or SUSE Linux OS, if you fail to log in to the GUI desktop system, establish the HA relationship between the primary and secondary sites.

The operations in CLI mode are as follows:

On Solaris OS, run the following command as user **nmsuser**. On SUSE Linux OS, run the following command as user **root**.

```
cd /opt/U2000/engineering
./startclient.sh deploy -ip 127.0.0.1 -port 12212 -username admin -password admin
buildHA -secondaryip System IP address of the peer site
```

10.1.3.4 Deleting the HA Relationship Between the Primary and Secondary Sites

This topic describes how to delete the HA relationship between the primary and secondary sites. After the delete operation, the connection between the primary site and the secondary site is interrupted. In this manner, the HA system becomes two standalone sites. To delete the HA relationship between the primary and secondary sites, perform the following operations.

Prerequisite

The MSuite server on the primary and secondary sites must be started.

Procedure

1. Log in to the MSuite client. For details, see **10.1.3.1 Logging In to the MSuite Client**.
2. Choose **Deploy** > **Separate Primary Site from Secondary Site**. The **Separate Primary Site from Secondary Site** dialog box is displayed.
3. Click **OK**. The progress bar is displayed indicating the status of separating the primary and secondary sites. Wait until the dialog box is displayed indicating that the separation is complete.

4 Click **OK**.

----End

Operations Through the CLI

On Solaris or SUSE Linux OS, if you fail to log in to the GUI desktop system, delete the HA relationship between the primary and secondary sites through the CLI.

The operations in CLI mode are as follows:

On Solaris OS, run the following command as user **nmsuser**. On SUSE Linux OS, run the following command as user **root**.

```
cd /opt/U2000/engineering
./startclient.sh deploy -ip 127.0.0.1 -port 12212 -username admin -password admin
splitHA
```

Follow-up Procedure

After the active site and standby site are successfully separated, primary and secondary sites are two separate sites. To re-establish the HA system, you need to perform synchronization between the active site and standby site. For details, see **10.1.3.3 Establishing the HA Relationship Between the Primary and Secondary Sites**..

10.1.3.5 Configuring the Current Server as the Active Server Forcibly

This topic describes how to forcibly configure the current server as the active server. When the replication relations between the primary and secondary sites become abnormal or the high availability system is in the dual-active state, you can perform this operation to specify the active site and data replication direction to restore data replication relations.

Prerequisite

- The data replication relation between the primary and secondary sites must be abnormal.
- All the MSuite servers on the servers of the primary and secondary sites must be started.

Context

- Do not perform this operation if the HA system works in the normal state. Otherwise, an exception may occur in the HA system.
- Do not perform this operation if the resource group **AppService** at the primary and secondary sites are in the online process. Otherwise, an exception may occur in the HA system.
- If you log in to the MSuite server of the primary site to perform this operation, the primary site becomes the active site after the operation. If you log in to the MSuite server of the secondary site to perform this operation, the secondary site becomes the active site after the operation.

Procedure

1 Log in to the MSuite client. For details, see **10.1.3.1 Logging In to the MSuite Client**.

2 Choose **Deploy** > **Force Active of Local Site**.

3 Click **OK**. Then, the current server is configured to function as the active server.

----End

10.2 Veritas Troubleshooting Cases

This topic describes how to troubleshoot the Veritas.

10.2.1 Switching Between Primary and Secondary Nodes Fails

The switching between the primary and secondary sites in the HA system (Veritas hot backup) cannot be performed.

Locate and rectify the fault according to the following sequence:

Sequence	Problem Location	Troubleshooting
1	Check whether the HA system is in the normal state.	If the system is in the revertive state or dual-host state, you need to rectify the fault manually. For the specific method, see the troubleshooting chapters in the administrator guide for the corresponding version and solution.
2	Check whether the resources are abnormal.	Rectify the fault with reference to **10.2.5 Resource in the Frozen State** and **10.2.6 Resource in the Faulted State**.
3	Check whether the communication connection between the primary and secondary sites is normal.	Rectify the fault with reference to **10.2.4 Communication Between Primary and Secondary Sites Fails**.

Sequence	Problem Location	Troubleshooting
4	Check whether the data on the primary site is consistent with the data on the secondary site.	Rectify the fault with reference to **10.2.3 Data Replication Cannot Be Performed Between Primary and Secondary Nodes**.
5	The preceding measures do not work.	Contact Huawei engineers for troubleshooting.

10.2.2 Starting the U2000 HA System Fails

After the primary and secondary sites are restarted upon power failure, the U2000 HA system cannot be started.

Locate and rectify the fault according to the following sequence:

Sequence	Problem Location	Troubleshooting
1	Check whether the files of the operating system are normal.	Rectify the fault with reference to **6.1.1 Starting the Operating System Fails**.
2	Check whether the VCS is normal. Run the **hastatus -sum** command to query the status of the VCS. If the reported status of the VCS is **ADMIN**, it indicates that the VCS fails to be started.	Rectify the fault with reference to **10.2.9 Failed to Start the VCS Because of the Errors in the Configuration File**.
3	The preceding measures do not work.	Contact Huawei engineers for troubleshooting.

10.2.3 Data Replication Cannot Be Performed Between Primary and Secondary Nodes

The **vxrlink -g datadg -i 5 status datarlk** command is run on the primary server. After a certain period of time, however, the system still displays that substantive data is not synchronized.

Locate and rectify the fault according to the following sequence:

Sequence	Problem Location	Troubleshooting
1	Check whether the communication connection between the primary and secondary sites is normal.	Rectify the fault with reference to **10.2.4 Communication Between Primary and Secondary Sites Fails**.

Sequence	Problem Location	Troubleshooting
2	Check whether the HA system is in the normal state.	If the system is in the revertive state or dual-host state, you need to rectify the fault manually. See **10.1 Troubleshooting Policies for the Veritas HA System**.
3	The preceding measures do not work.	Contact Huawei engineers for troubleshooting.

10.2.4 Communication Between Primary and Secondary Sites Fails

Symptom

Data replication and switching cannot be performed between the primary and secondary sites.

Possible Causes

The possible causes that result in the communication failure between the primary and secondary sites are as follows:

- The network between the primary and secondary sites is unstable or a firewall exists.
- The IP addresses and gateways of the primary and secondary sites are set incorrectly.
- Replication link between the primary and secondary sites is interrupted.

Procedure

1. To check the communication status between the primary and secondary sites, run the following commands as user **root** on the primary site:

   ```
   # ping IP_address_of_the_secondary_site
   # ping IP_address_of_the_replication_NIC_on_the_secondary_site
   ```

   TIP

   Run **cat /etc/hosts | grep loghost** as user **root** on secondary site can query the *IP address of the Master NIC on the secondary site*.

   Generally, the bandwidth between the primary and secondary sites is at least 2 Mbit/s and the packet loss ratio is smaller than 0.1%.

2. Check whether replication NICs or the replication link functions properly.

3. Check whether all the ports used by the HA system are enabled.

   To query the service ports that are enabled in the system, run the following command as user **root**:

   ```
   # netstat -an
   ```

----End

10.2.5 Resource in the Frozen State

Symptom

A lock in red is displayed on a resource or resource group in the VCS Explorer.

Possible Causes

You may forget to restore the resource group after freezing it manually.

Procedure

1. In the VCS Explorer interface, right-click the resource group that is in the frozen state, and then choose **Unfreeze**.

----End

10.2.6 Resource in the Faulted State

Symptom

In the VCS Explorer, a cross in red is displayed for a certain resource. The resource is in the **Faulted** state.

Possible Causes

The resource is faulty. For example, the U2000 coredump occurs or processes or database processes are abnormal.

Procedure

1. Check whether the U2000 processes or database processes are normal.
2. Right-click the name of the resource that is in the **Faulted** state, and then choose **Clear Fault** to rectify the fault.
3. In the case of the primary server, right-click **AppService**, and then choose **Online**. The **AppService** resource group is in the **Online** state.

----End

Suggestion and Summary

If the U2000 still cannot work after the **Faulted** state of the resource is cleared, that is, the **AppService** resource group cannot enter the **Online** state on the primary server, contact the local office or customer service center of Huawei for troubleshooting.

10.2.7 Connection Failure Between the Rlink and the Remote Host

Symptom

In the console window, the following error message is displayed:

```
vxvm:vxrlink: ERROR: Unable to establish connection with remote host <remote_host>
```

Possible Causes

- The network connection between the primary site and the secondary site is torn down.
- The vradmind service process is stopped.

Procedure

- Check network connection between primary and secondary sites.

  Run the following command:
  ```
  # ping host_IP_address_of_the_master_server_on_the_secondary_site
  ```
  If each host can be pinged successfully, it indicates that network connection is normal. Otherwise, clear the network fault first.
- Check whether the vradmind process of the primary/secondary site is running.

  Run the following command:
  ```
  # ps -ef | grep vradmind
  ```

  The terminal displays:

  ```
  root   489     1  0 17:36:12 ?        0:00 /usr/sbin/vradmind
  root  9717  9662  0 18:08:46 pts/3    0:00 grep vradmind
  ```

  If **/usr/sbin/vradmind** is output, it indicates that the vradmind process is running. Otherwise, run the following commands to restart it:

  ```
  # cd /etc/init.d
  # ./vras-vradmind.sh start
  ```

----End

10.2.8 Abnormal Status of the Disk Volume

Symptom

Run the **vxprint -v** command to check the status of a disk volume, and the status of the data volume is not ACTIVE or ENABLED. Or run the **vxprint -l datarvg** command to check the status of datarvg, and the status of datarvg is RECOVER. Or run the **vxprint -l datarlk** command to check the status of datarlk, and the status of datarlk is RECOVER.

Possible Causes

The server is powered off abnormally or other abnormal operations are performed.

Procedure

1. Open a terminal window.
2. Run the following commands on the site on which the disk volume is abnormal:
   ```
   # vxrecover -g disk_group_name -sb
   # vxvol -g disk_group_name start volume_name
   ```

   NOTE

   You can run the **vxdg list** command to query the *disk_group_name*, and run the **vxprint -v** command to query the *volume_name*.
3. check whether the status of disk volume and data replication status is correct. If so, the recovery is successful.

----End

10.2.9 Failed to Start the VCS Because of the Errors in the Configuration File

Symptom

After the **hastatus -sum** is run, the state of the VCS is reported as ADMIN.

Possible Causes

The VCS startup failure may be caused by a power failure.

Procedure

1. To restore the VCS on the primary site, run the following command on the primary site as the **root** user:
   ```
   # hasys -force host name of the primary site
   ```
2. If starting the VCS on the secondary site fails, run the following command on the secondary site as the **root** user:
   ```
   # hasys -force host name of the secondary site
   ```

----End

10.2.10 Faults on the Active Site

Symptom

The NMS cannot be normally used.

Possible Causes

The NMS cannot be used because of the fault on the active site.

Procedure

- The connection between the client and server is torn down. In this case, the active site is unavailable. The NMS application processes are automatically switched to the standby site. Do as follows:
  1. Log in to the U2000 server on the secondary site through the client.
  2. Manage NEs through the U2000 server on the secondary site.
- On the client, the NEs on the NMS preempt the resource of each other. The server is in the dual-host state. Do as follows:
  1. Shut down the U2000 server on the primary site. For details, refer to the chapter "Shutting Down the U2000" of the *iManager U2000 Administrator Guide*.
  2. Log in to the U2000 server on the secondary site through the client.
  3. Manage NEs through the U2000 server on the secondary site.
- The damage of the NMS data results in the failure of the server. In this case, the primary and secondary sites are both unavailable. Do as follows:
  1. Recover the backup data of the U2000. For details, refer to the chapter "Backing Up and Restoring the U2000 Database" of the *iManager U2000 Administrator Guide*.

2. If there is no backup data, recover the data by using the script. For details, refer to the chapter "Backing Up and Restoring the U2000 Database" of the *iManager U2000 Administrator Guide*.

----End

10.2.11 Frequent Dual-Host State of the HA System

Symptom

The heartbeat between the primary and secondary sites is frequent interrupted, and the HA system is in the dual-host state. As a result, the U2000 cannot work normally.

Possible Causes

The instability of the data communication network (DCN) between the primary and secondary sites leads to the frequent interruption of heartbeat between the two sites. You can rectify the fault by modifying the timeout period of the heartbeat detection.

Procedure

1 To display the current heartbeat settings, run the following commands respectively on the primary and secondary sites:

```
# /opt/VRTSvcs/bin/hahb -display
```

2 To modify the heartbeat settings, run the following commands respectively on the primary and secondary sites:

```
# haconf -makerw
# /opt/VRTSvcs/bin/hahb -local Icmp AYARetryLimit
# /opt/VRTSvcs/bin/hahb -modify Icmp AYARetryLimit Retry_Limit -clus
Cluster_name_of_the_opposite_site
# haconf -dump -makero
```

NOTE

You can set the heartbeat settings according to the interruption time of the network between the primary and secondary sites. Besides an increase in Retry Limit (**AYARetryLimit**), you can set Interval (**AYAInterval**) and Timeout (**AYATimeout**) in this manner.

3 After the DCN becomes stable, you need to restore the heartbeat settings to the default value.

----End

Suggestion and Summary

Modifying the heartbeat settings applies to only the temporary avoidance of HA system problems caused by the DCN instability. Therefore, clear the instability of DCN communication between the primary and secondary sites in a timely manner, and restore the heartbeat settings to the default value.

11 Distributed System Troubleshooting

About This Chapter

This topic describes how to troubleshoot the distributed system.

11.1 Slave Server in the Disconnected State

Symptom

After logging in to the NMS Maintenance Suite, you find that the slave server is in the disconnected state.

Possible Causes

- The slave server is not started. The possible causes may be manual shutdown, abnormal power-off, and hardware fault.
- The NMS Maintenance Suite server of the slave server is not started or is started abnormally.
- The IP address used for connecting the slave server to the master server changes.
- The network between the slave server and the master server is faulty or the NIC of the slave server is faulty.

Procedure

1. Check whether the slave server is started successfully.

   If the slave server is started abnormally, check the server hardware, such as hard disk, CPU, memory, and card.

2. Check whether the NMS Maintenance Suite server of the slave server is started successfully.

   Run the following command as the **root** user on the slave server to check whether the NMS Maintenance Suite server is started:

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

   If **/opt/HWNMSJRE/jre_linux/bin/java -server** is displayed, it indicates that the NMS Maintenance Suite server is started. Otherwise, run the following commands to start the NMS Maintenance Suite server:

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

3. Check whether the IP address used for connecting the slave server to the master server changes.

   Run the **ifconfig -a** command as user **root** to check whether the displayed IP address is the same as the IP address in the server list of the NMS Maintenance Suite. If the IP addresses are different, right-click the server whose network configuration needs to be synchronized, and choose **Synchronize the network configuration**.

4. Run the **ping** ***Floating_IP_address_of_the_slave_server*** command as user **root** on the master server to check whether the network between the master and slave servers is normal.

   ----End

11.2 Other Faults on the Master Server

Symptom

Unrecoverable faults occur on the master server. You need to reinstall the master server.

Possible Causes

- The hard disk of the master server is faulty.
- The OS of the master server is faulty.
- A severe fault occurs on the file system of the master server. Consequently, the files on the master server are lost and reinstalling the NMS is required.

Procedure

1. Reinstall the master server where the faults occur.

   For details, refer to the *iManager U2000 Software Installation Guide* for the corresponding solution.

   NOTE

   During the installation, make sure that the IP address and host name of the reinstalled server are the same as those of the faulty master server.

2. Log in to the NMS Maintenance Suite client. Choose **System** > **Add the secondary server** to add the original slave servers again.

----End

11.3 Other Faults on the Slave Server

Symptom

Unrecoverable faults occur on the slave server. You need to reinstall the slave server.

Possible Causes

- The hard disk of the slave server is faulty.
- The OS of the slave server is faulty.
- A severe fault occurs on the file system of the slave server. Consequently, the files on the slave server are lost and reinstalling the NMS is required.

Procedure

1. Reinstall the slave server where the faults occur.

   For details, refer to the *iManager U2000 Software Installation Guide* for the corresponding solution.

   NOTE

   During the installation, make sure that the IP address and host name of the reinstalled server are the same as those of the faulty slave server.

2. On the NMS Maintenance Suite, choose **System** > **Add the secondary server** to connect the slave server to the master server to form a distributed system.

----End

12 NMS Maintenance Suite Troubleshooting

About This Chapter

This topic describes how to troubleshoot the NMS Maintenance Suite.

12.1 Troubleshooting the Inconsistency of the Instance Status

Symptom

How to troubleshoot the inconsistency of the instance status between the client of the NMS Maintenance Suite and the system monitoring client by refreshing the information on the network management system.

Possible Causes

The client of the NMS Maintenance Suite refreshes the instance status every several seconds. Therefore, the instance status between the client of the NMS Maintenance Suite and the system monitoring client may be inconsistent in a short time.

Procedure

1. On the client of the NMS Maintenance Suite, click the **Instance** tab.
2. Choose **System** > **Refresh the NMS Information**. You can also click the  shortcut icon to refresh the information on the network management system.

----End

A Obtaining the Technical Support

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

During the 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. You can also go to **http://support.huawei.com** to obtain the latest technical materials of Huawei.

Before seeking the technical support, collect the relevant information.