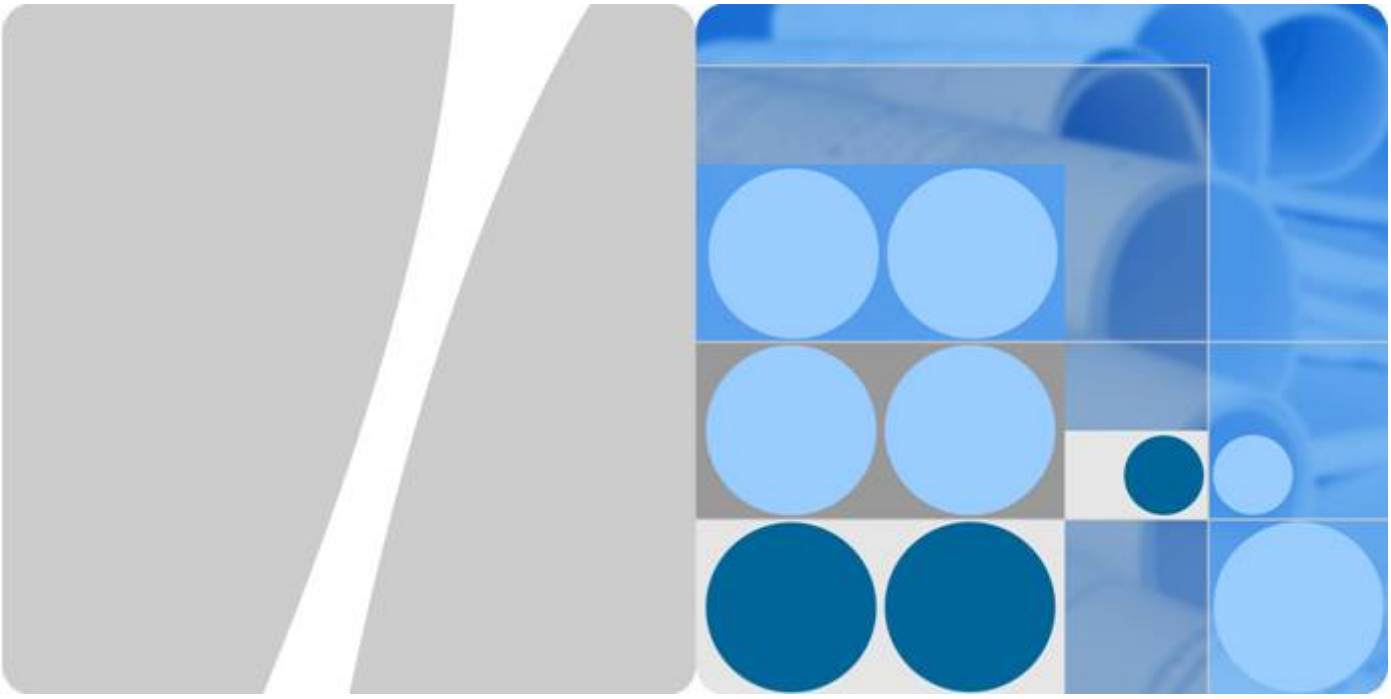


iManager U2000 Unified Network Management System

V100R002C01

Routine Maintenance

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

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

The intended audience of this document is the System Maintenance Engineer.

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) Based on Product Version V100R002C01

The fifth commercial release has the following updates:

Fixed some bugs.

Changes in Issue 04 (2010-09-24) Based on Product Version V100R002C01

The fourth commercial release has the following updates:

Fixed some bugs.

Changes in Issue 03 (2010-08-16) Based on Product Version V100R002C01

The third commercial release has the following updates:

Fixed some bugs.

Changes in Issue 02 (2010-07-16) Based on Product Version V100R002C01

The second commercial release has the following updates:

Fixed some bugs.

Changes in Issue 01 (2010-05-18) Based on Product Version V100R002C01

Initial field trial release.

Contents

Tables

1 Suggestions on Running Security

This topic describes the suggestions on running security. To ensure the normal running of the U2000, you need to follow the precautions for software and hardware operations.

Precautions for Hardware Operations

To make sure that the hardware operations are normal, note the following:

- Configure independent uninterrupted power supply (UPS) for the U2000 server. This can avoid some serious problems such as hardware damage, system restoration failure, and data loss caused by abnormal power failure. If the independent UPS cannot be configured for the U2000 server, normally shut down the U2000 application and then the database, before the administrator cuts the power upon a power cut notification.
- You need to follow the normal method to shut down the U2000 in any case. Do not run the halt command to power off the hardware or switch off. Otherwise, the system fails to be restored.
- To avoid network communication interruption, check the network communication status daily according to routine maintenance items.
- Removing network cables from the server is prohibited if the NMS is running. If you need to remove unwanted network cables, remove them after stopping NMS services.
- Keep the equipment room clean, dustproof and moistureproof.

Precautions for Software Operations

To make sure that the software operations are normal, note the following:

- Do not run the **reboot** or **init 6** command to restart the system. Do not press **Stop+A** to switch to **OK** prompt. Otherwise , a fault of the system occurs.
- After the system installation and configuration, do not install any patch for the system.
- Do not install any unnecessary software on the U2000 server.
- Do not enable irrelevant services or the Telnet authority and FTP authority of user root.
- Do not browse web pages on the U2000 server or set unnecessary shared paths. Make sure that the authority of the shared path is already set.
- Do not use other computers or laptop computers to access the same network as the U2000 server accesses. In this way, conflict of IP addresses and virus infection can be avoided.

- Classify authorities of the operating system (OS), database and U2000 passwords by level, and distribute the passwords to persons in charge of maintenance only. The administrator password should be controlled by the person in charge of maintenance only, based on strict management and well-defined power and responsibility.
- In the HA system, you can run the applications of the U2000 at only the primary site in normal cases. The secondary site is for backup. If you run the U2000 at both the primary and secondary sites, serious abnormality occurs.
- In the HA system, do not perform operations involving a large amount of data during the complete data synchronization between the primary and secondary sites. For example, do not search for trails, search for protection subnets, or query the networkwide alarms. Otherwise, the performance of the entire U2000 HA system is affected.
- Blades and slots of the shelf of the distributed system are in the one-to-one relationship.
- Regularly check and test the U2000 according to **2 Maintenance Item List** and record the results. Handle problems in time. For any problems that fail to be handled, contact the local office or customer service center of Huawei. For the contact methods, see **3 Obtaining the Technical Support**.

2 Maintenance Item List

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

NOTE

Refer to the related routine maintenance item list according to the system implementation scheme.

- Single-Server System (Windows), see **Table 2-1**.
- Single-Server System (SUSE Linux-distributed) , see **Table 2-2**.
- Single-Server System (Solaris), see **Table 2-3**.
- High Availability System (Windows), see **Table 2-4**.
- High Availability System (Solaris), see **Table 2-4**.
- High Availability System (SUSE Linux-distributed), see **Table 2-4**.

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

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

Maintenance Period	Routine Maintenance Task
	5.4 Checking the Logs of the SQL Server Database
	5.7 Checking the Running Status of the Anti-Virus Software
	5.8 Checking the Database Status
Monthly	6.1 Checking the User Configuration
	6.2 Backing Up System Files
	6.3 Viewing the Statistics of Alarms
	6.4 Checking the Server Time of the U2000
	6.5 Changing the Password of the Current User
	6.6 Releasing the Disk Space of the U2000 Server
Quarterly	7.1 Checking the Equipment Room Environment
	7.2 Checking the Power Supply of the U2000 Server
	7.3 Checking the Hardware and Peripherals of the U2000 Server

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

Maintenance Period	Routine Maintenance Task
Daily	4.1 Viewing Current Alarms
	4.2 Querying Security Logs
	4.3 Checking the Resource Usage of the U2000 Server
	4.4 Checking the Status of the Network Communication Between the U2000 and NEs
	4.5 Checking the Running Status of the Processes and Services of the U2000
	4.6 Checking the Server Status in the Distributed System
	4.8 Backing Up the U2000 Data
Weekly	5.1 Checking the Disk Status of the U2000 Server
	5.2 Checking the Disk Space of the U2000 Server
	5.3 Checking the Log Information of the OS
	5.5 Checking the Logs of the Sybase Database
	5.8 Checking the Database Status

Maintenance Period	Routine Maintenance Task
Monthly	6.1 Checking the User Configuration
	6.2 Backing Up System Files
	6.3 Viewing the Statistics of Alarms
	6.4 Checking the Server Time of the U2000
	6.5 Changing the Password of the Current User
	6.6 Releasing the Disk Space of the U2000 Server
Quarterly	7.1 Checking the Equipment Room Environment
	7.2 Checking the Power Supply of the U2000 Server
	7.3 Checking the Hardware and Peripherals of the U2000 Server

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

Maintenance Period	Routine Maintenance Task
Daily	4.1 Viewing Current Alarms
	4.2 Querying Security Logs
	4.3 Checking the Resource Usage of the U2000 Server
	4.4 Checking the Status of the Network Communication Between the U2000 and NEs
	4.5 Checking the Running Status of the Processes and Services of the U2000
	4.8 Backing Up the U2000 Data
Weekly	5.1 Checking the Disk Status of the U2000 Server
	5.2 Checking the Disk Space of the U2000 Server
	5.3 Checking the Log Information of the OS
	5.5 Checking the Logs of the Sybase Database
	5.8 Checking the Database Status
Monthly	6.1 Checking the User Configuration
	6.2 Backing Up System Files
	6.3 Viewing the Statistics of Alarms
	6.4 Checking the Server Time of the U2000

Maintenance Period	Routine Maintenance Task
	6.5 Changing the Password of the Current User
	6.6 Releasing the Disk Space of the U2000 Server
Quarterly	7.1 Checking the Equipment Room Environment
	7.2 Checking the Power Supply of the U2000 Server
	7.3 Checking the Hardware and Peripherals of the U2000 Server

Table 2-4 List of maintenance items for the High Availability System (Windows, Solaris and SUSE Linux-distributed system)

Maintenance Period	Routine Maintenance Task
Daily	4.1 Viewing Current Alarms
	4.2 Querying Security Logs
	4.3 Checking the Resource Usage of the U2000 Server
	4.4 Checking the Status of the Network Communication Between the U2000 and NEs
	4.5 Checking the Running Status of the Processes and Services of the U2000
	4.6 Checking the Server Status in the Distributed System
	4.7 Checking the Status of Data Replication Between the Primary and Secondary Sites in the Veritas High Availability System
	4.8 Backing Up the U2000 Data
Weekly	5.1 Checking the Disk Status of the U2000 Server
	5.2 Checking the Disk Space of the U2000 Server
	5.3 Checking the Log Information of the OS
	5.5 Checking the Logs of the Sybase Database
	5.8 Checking the Database Status
Monthly	6.1 Checking the User Configuration
	6.2 Backing Up System Files
	6.3 Viewing the Statistics of Alarms
	6.4 Checking the Server Time of the U2000
	6.5 Changing the Password of the Current User

Maintenance Period	Routine Maintenance Task
	6.6 Releasing the Disk Space of the U2000 Server
Quarterly	**7.1 Checking the Equipment Room Environment**
	7.2 Checking the Power Supply of the U2000 Server
	7.3 Checking the Hardware and Peripherals of the U2000 Server

3 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.

4 Daily Maintenance

About This Chapter

This topic describes how to perform daily maintenance. Through daily maintenance, you can collect the information about the running status and trend of the U2000 in real time. This helps you improve the efficiency of handling emergencies.

4.8 Backing Up the U2000 Data

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

4.1 Viewing Current Alarms

By viewing the current alarms, you can know the running status of the network. This helps during the network maintenance when you need to update the alarm information and take proper measures on time.

Procedure

1. Log in to the U2000 client.
2. Choose **Fault** > **Browse Current Alarm** from the main menu.
3. On the **Filter** tab, set filter criteria and click **OK**. The current alarm viewing window is displayed.

   NOTE

   If you already set the startup template for the current alarms, the alarms that meet the startup template criteria are directly displayed, without the displaying of the **Filter** dialog box.
4. Select an alarm. In the pane below, the details of the alarm and the handling suggestions are displayed.
5. **Optional:** Right-click an alarm in the query result list, and you can perform the following operations:
   - Choose **Memo** from the shortcut menu to set remarks for this alarm.
   - Choose **Acknowledge** from the shortcut menu to acknowledge the alarm.

     NOTE

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

   NOTE

   The operations that you can perform through the shortcut menus varies according to different alarms.
6. **Optional:** Select one or more uncleared alarms, right-click, and choose **Clear** from the shortcut menu. In the prompt that is displayed, click **Yes**.
7. **Optional:** Select the **Display latest alarms** check box to view the real-time alarms reported.
8. **Optional:** Click the buttons in the lower pane to perform the following operations:
   - Click **Template** to new, open, save as, or delete the alarm filtering template.
   - Click **Filter** to set filter criteria.
   - Click **Synchronize** to synchronize current alarms.
   - When the alarm that is reported from the equipment is changed, the **Refresh** button is marked by a red circle. You can click **Refresh** to refresh current alarms.
   - Click **Acknowledge** to acknowledge current alarms.
   - Click **Clear** to clear current alarms.

----End

Troubleshooting

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

4.2 Querying Security Logs

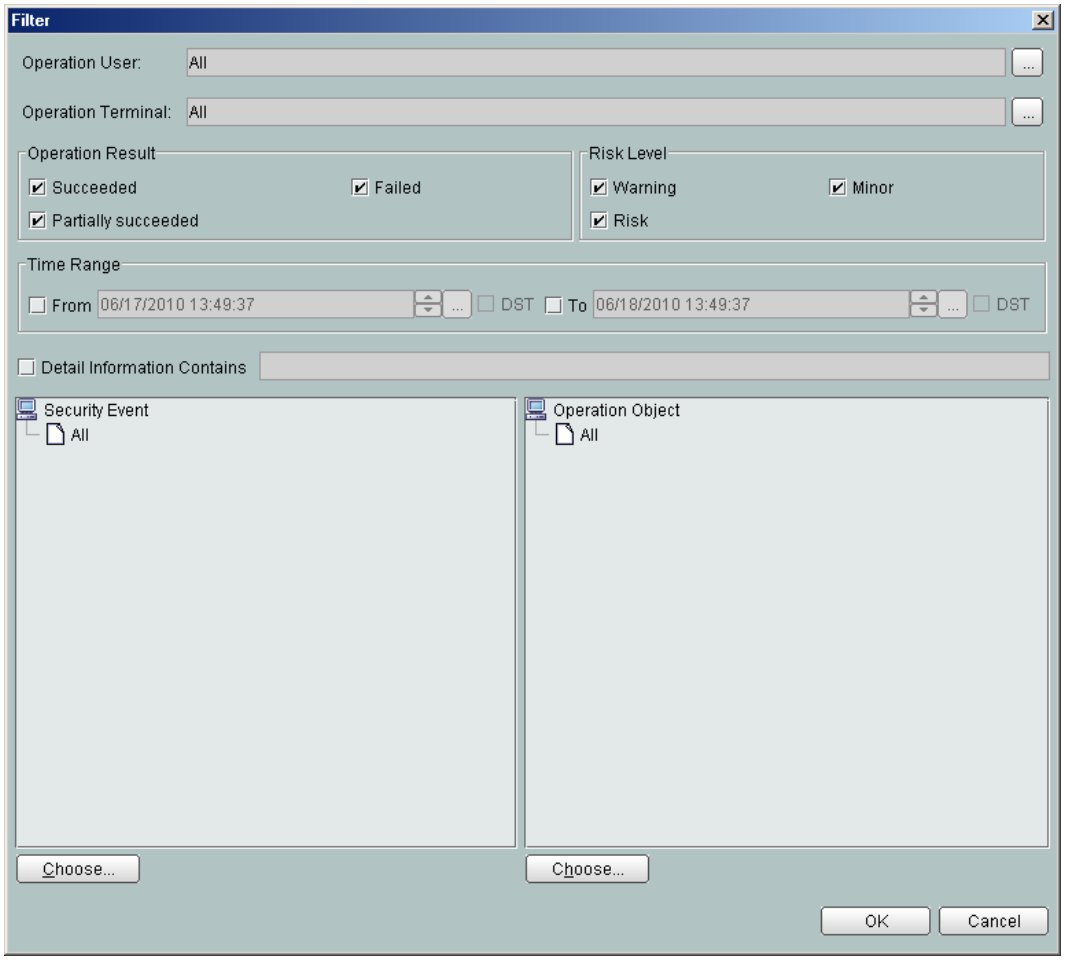
You can query security logs to know the security operations of the U2000.

Context

The statistical result is generated based on the existing data in the database. If the database is empty, there is no statistical result.

Procedure

1. Choose **Administration** > **Log Management** > **Query Security Logs** from the main menu.
2. In the **Filter** window, set the filtering conditions, and then click **OK**.



NOTE

You can query logs in the **Query Security Logs** window in the following ways:

- Click **Template Filter**, and then select **Open**. Select a template from the template list, and then click **Open** to use an existing template to query logs.
- Set the query conditions in the **Filter** window, and then click **OK** to query logs.

3 In the **Query Security Logs** window, double-click a record to view the log details.

- Click a field in the header of the query result table to sort the query results by field.
- A white upward triangular icon indicates that you can sort the results by field. A black upward triangular icon indicates that the results are sorted in the ascending order by field. The black downward triangular icon indicates that the results are sorted in the descending order by field.
- Click the **Device Name**, or **Access Method** field. Different from other table header fields, these fields are displayed in groups. Therefore, they are not sorted in alphabetic order.

4 Right-click in the query window and perform the following operations.

Operation Name	Operation Method
Details	Right-click a log in the window and choose **Details**, or double-click the log. **NOTE** The **Details** dialog box displays the time, risk level, or results of the operation that generates the log.
Save All Records	1. Right-click a log in the window and choose **Save All Records**. 2. In the **Save** dialog box, select the path to save records, and then click **Save**. **NOTE** The log records can only be exported as TXT, HTML, CSV, PDF or XLS files. The default file format is XLS file.
Save Selected Records	1. Right-click a log in the window and choose **Save Selected Records**. 2. In the **Save** dialog box, select the path to save records, and then click **Save**. **NOTE** The log records can only be exported as TXT, HTML, CSV, PDF or XLS files. The default file format is XLS file.

Operation Name	Operation Method
Save Appoint Records	1. Right-click a log in the window and choose **Save Appoint Records**. 2. In the **Save Appoint Record** dialog box, set the start row and end row of logs and the name of the file to be saved, and then click **OK**. **NOTE** In the **Save Appoint Records** dialog box, click ... on the right of **File name**. In the **Save** dialog box, select the path for saving the records. The log records can only be exported as TXT, HTML, CSV, PDF or XLS files. The default file format is XLS file.
Print All Records	1. Right-click a log in the window and choose **Print All Records**. 2. In the **Print** dialog box, set the print parameters, and then click **Print**.
Print Selected Records	1. Right-click a log in the window and choose **Print Selected Records**. 2. In the **Print** dialog box, set the print parameters, and then click **Print**.
Print Appoint Records	1. Right-click a log in the window and choose **Print Appoint Records**. 2. In the **Print Appoint Records** dialog box, set the start row and end row, and then click **OK**. 3. In the **Print** dialog box, set the print parameters, and then click **Print**.

----End

4.3 Checking the Resource Usage of the U2000 Server

This topic describes how to check the resource usage of the U2000 server. If the CPU usage, memory usage, disk usage or database usage exceeds a normal value, the system runs slowly. Therefore, you need to check the current running status of the U2000 server periodically, to find and solve the problem as soon as possible. This ensures the efficient running of the system.

Context

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

Procedure

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

2 Click the **Server Monitor** tab and view the information such as the CPU used rate, physical memory, used memory, and available memory of the server.

3 Click the **Hard Disk Monitor** tab and view the disk used rate.

4 Click the **Database Monitor** tab and view the data used rate and the log used rate.

----End

Reference Standards

Check Item	Standard
CPU Used Rate	Lower than 85%
Memory Usage	Lower than 95%
Disk Used Rate	Lower than 80%
Data Used Rate	Lower than 85%
Log Used Rate	Lower than 80%

Troubleshooting

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

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

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

Procedure

1 Log in to the U2000 client.

2 View the icons of device nodes in the navigation tree of the client.

----End

Reference Standard

In the device tree, if the icon of a device node is not gray, it indicates that the communication status is normal.

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

Troubleshooting

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

       NOTE

       If the ping fails, check whether the physical link of the network is abnormal.
    2. Right-click a device node and choose **Refresh Status** from the shortcut menu.

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

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

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

Procedure

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

  Check the process status in U2000 System Monitor client.

  1. Log in to the U2000 System Monitor client.
  2. Click the **Process Monitor** tab and view the running statuses of all processes on the U2000 server and of the **Database Server Process**.

  NOTE

  The Solaris OS also supports the function of checking whether the U2000 processes are started through the command line.

  # **su - nmsuser**

  $ **cd /opt/U2000/server/bin**

  $ **svc_adm -cmd status**

  After you run the preceding commands, the started processes are displayed.

- Do as follows in the High Availability System:
  - On the primary site, query the statuses of all the services and service groups of the U2000 through the VCS browser.
    1. Run the following command to log in to the graphical user interface (GUI) of the VCS Cluster Explorer:

       # **hagui &**

       NOTE

       In the Windows OS, choose **Start** > **Programs** > **Symantec** > **Veritas Cluster Server** > **Veritas Cluster Manager - Java Console** to start the VCS client.
    2. In the **Cluster Monitor** window, click **Click here to log in**.
    3. In the login dialog box, enter the user name and password of the VCS. Click **OK** to log in to the VCS.

       NOTE

       By default, the user of the VCS is **admin**, and the password is **password**.
    4. Access the **Cluster Explorer** window. For the service groups including ClusterService, AppService and VVRService, click the **Status** tab respectively to view the status.
  - Query the statuses of all services and service groups by using command lines on the primary site.
    1. Run the following command to view the statuses of all service groups in the VCS:

       # **hastatus -sum**

       The screen output is as follows:

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

A  Pri_master          RUNNING          0

-- GROUP STATE
-- Group           System             Probed    AutoDisabled
State

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

-- WAN HEARTBEAT STATE
-- Heartbeat       To                 State

L  Icmp             Sec_masterCluster  ALIVE

-- REMOTE CLUSTER STATE
-- Cluster         State

M  Sec_masterCluster RUNNING

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

N  Sec_masterCluster:Sec_master  RUNNING          0

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

O  AppService       Sec_masterCluster:Sec_master  Y     N
OFFLINE
```

2. Run the following command to view the statuses of all services in the VCS:

   # **hastatus**

   The screen output is as follows:

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

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

-------------------------------------------------------------------------
---
                NMSServer            localclus:Pri_master
```

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

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

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

NOTE

- If the northbound interface is enabled, the screen output contains the information of the corresponding resources, such as CorbaApp and SNMPApp.
- If the IPMP protection scheme is used, the screen output does not contain the information of the three resources, including webip, csgnic, and VVRServiceNIC.
- If the IPMP feature is enabled, the name of the Cluster service group is the same as the host name of the computer.
- To stop running the command, press the shortcut keys **CTRL+C**.

----End

Reference Standard

All the processes are in the running state and no process is restarted repeatedly.

In the High Availability System:

- If you use the VCS Cluster Explorer and all the service groups and services meet the standards in the following table, it indicates that the service groups and services of the HA System run normally.

Table 4-1 Standard statuses of services and service groups in VCS Cluster Explorer

Resource Group Name	Check Item	Reference Standard
AppService Group	Group Status on Member Systems	The status of the service group on the active site is **Online**.
	Resource Status	The status of each service is **Online on Pri_master**.
	Remote cluster	The status of system members is **Offline**.
ClusterService Group	Group Status on Member Systems	The status of each service on the active site is **Online**.
	Resource Status	The status of each service is **Online on Pri_master**.
VVRService Group	Group Status on Member Systems	The status of each service on the active site is **Online**.
	Resource Status	The status of each service is **Online on Pri_master**.

- If you use command lines to query the statuses of each service groups and services meet the standards in the following table, it indicates that the service groups and services of the HA System run normally.

Table 4-2 Query the standard statuses of services and service groups through command lines

Command	Check Item	Reference Standard
hastatus -sum	SYSTEM STATE	**System** is displayed as **RUNNING** on the active and standby site.
	GROUP STATE	The statuses of all the groups on the active site, including ClusterService, AppService, and VVRService, are **ONLINE**.
hastatus	resource	The statuses of all the services on the active site are **ONLINE**.

Troubleshooting

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

NOTE

The starting modes of a process include the following:

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

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

- Do as follows in the High Availability System:

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

  Contact the local office or Customer Service Center of Huawei according to the warranty.

4.6 Checking the Server Status in the Distributed System

This topic describes how to check the server status in the distributed system. A distributed system can run normally only when the master and slave servers are in the normal state. This topic describes how to check the statuses of the master and slave servers.

Prerequisite

The NMS Maintenance Suite must run in normal state.

Context

- Normally, the core processes of the U2000 server and the database server programs are running on the master server.
- Normally, the non-core processes of the U2000 server and the database client programs are running on the slave server.
- A distributed system, including the master and slave servers, provides network monitoring by using public network.

Procedure

1. Log in to the operating system as user root on the master server.
2. Log in to the client of the NMS Maintenance Suite on the master server.
3. Click the **Server** tab to check the statuses of the master and slave servers.

----End

Reference Standard

On the **Server** tab, both the master and slave servers are in **Connect** state.

Troubleshooting

If the master and slave servers are not in **Connect** state, it indicates that the master and slave servers are abnormal. In this case, contact the maintenance personnel of the equipment room to check the master and slave servers.

If the fault persists, contact Huawei technical support engineers.

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

This topic describes how to check the status of data replication between the primary and secondary sites in the Veritas High Availability System.

Context

NOTE

This operation is performed on the primary site.

Procedure

- In the Solaris or SUSE Linux OS:
  1. Log in to the operating system as user **nmsuser**.
  2. Open a terminal window, and run the following commands to switch to user **root**:

     $ **su**

     Password: *password_of_user_root*
  3. Run the following commands to check the status of data replication between the primary and secondary sites on the active site:

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

     The terminal displays:

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

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

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

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

   The terminal displays:

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

   NOTE

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

- In the Windows OS:

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

  C:\> **vxrlink -g** *datadg* **-i 5 status** *datarlk*

  The terminal displays:

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

  NOTE

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

----End

Reference Standard

The data replication status is normal in the case that the **Table 4-3** standard is complied with.

Table 4-3 Standard status of the data replication

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

Troubleshooting

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

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

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

4.8 Backing Up the U2000 Data

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

Context

- The backup mode of database is classified into the immediate backup and the timing backup. To reduce the workload for daily maintenance, it is recommended that you adopt the timing backup mode to back up the U2000 data periodically.
- It is recommended that you check the timing backup status weekly and make sure that the timing backup is enabled.
- It is recommended that you clear the data backup files periodically, which prevents the insufficiency of the disk space caused by a large number of backup files.

Procedure

1. Back up the U2000 data on schedule.

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

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

----End

Reference Standard

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

Troubleshooting

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

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

If the problem persists, contact the local office or Customer Service Center of Huawei according to the warranty.

5 Weekly Maintenance

About This Chapter

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

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

5.1 Checking the Disk Status of the U2000 Server

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

Procedure

- Do as follows in the Single-Server System (Windows):
  1. In the **My Computer** window, select a disk, right-click, and choose **Attribute** from the shortcut menu.
  2. In the dialog box displayed, click the **Tools** tab.
  3. In the **Check Error** area, click **Start Check**. Follow the prompts to check the disk status.
- Do as follows in the Single-Server System (SUSE Linux-distributed) and Single-Server System (Solaris):
  1. Log in to the operating system as user **nmsuser**.
  2. Open a terminal window, and run the following commands to switch to user **root**:

     $ **su**

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

     # **iostat -E**

     The terminal displays:

     ```
     sd1       Soft Errors: 0 Hard Errors: 0 Transport Errors: 0
     Vendor: HITACHI  Product: H101414SCSUN146G Revision: SA25 Serial No:
     0848E3PKSA
     Size: 146.80GB <146800115712 bytes>
     Media Error: 0 Device Not Ready: 0 No Device: 0 Recoverable: 0
     Illegal Request: 0 Predictive Failure Analysis: 0
     ```
- Do as follows in the High Availability System:
  - In the Solaris or SUSE Linux OS:
    1. Log in to the operating system as user **nmsuser**.
    2. Open a terminal window, and run the following commands to switch to user **root**:

       $ **su**

       Password: *password_of_user_root*
    3. Run the following commands on the master server of the primary and secondary sites:

       # **vxdisk list**

       The terminal displays:

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

NOTE

The equipment names in the DEVICE column may be different from those displayed on the terminal according to the actual situation of the workstation. The displayed number of columns is consistent with the number of disks.

- In the Windows OS, run the following commands on the master server of the primary and secondary sites:

  C:\> **vxdisk list**

----End

Reference Standard

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

1. After you run the **vxdisk list** command, the disk is in **online** state.
2. After you run the **iostat -E** command, if the **Hard Errors** information of the disk is **0**, it indicates that the physical status of the disk is normal.

Troubleshooting

If a disk fails, contact the equipment supplier to repair or replace the disk in a timely manner.

5.2 Checking the Disk Space of the U2000 Server

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

Context

NOTE

For the HA System, you need to check the disk space of the U2000 server on both the primary and secondary sites.

Procedure

- Do as follows in the Windows system:

  View the disk space of the server through U2000 System Monitor client or in the **My Computer** window. You need to view the disk space usage of the operating system, SQL server, and U2000 mainly.

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

  You can view the disk space of the server through U2000 System Monitor client or command lines. The following describes how to view the disk space by running a command.

  1. Log in to the operating system as user **nmsuser**.
  2. Open a terminal window, and run the following commands to switch to user **root**:

     $ **su**

     Password: *password_of_user_root*

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

df -k

----End

Reference Standard

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

Troubleshooting

If the disk space exceeds the standard value, you need to clear the space in time. For details, refer to **6.6 Releasing the Disk Space of the U2000 Server**.

5.3 Checking the Log Information of the OS

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

Procedure

- Do as follows in the Windows system:
  1. Choose **Start** > **Control Panel** > **Administrative Tools** > **Event Viewer**.
  2. In the window displayed, view the log information of events and check whether the information about the abnormal events that affect system running exists.

     NOTE

     For the method of using the Event Browser, refer to the Online Help of the operating system or the user manuals.
- Do as follows in the Single-Server System (SUSE Linux-distributed), Single-Server System (Solaris) and High Availability System:
  1. Log in to the operating system as user **nmsuser**.
  2. Open a terminal window, and run the following commands to switch to user **root**:

     $ **su**

     Password: *password_of_user_root*
  3. Run the following command to navigate to the directory where the log file is saved:
     - In the Single-Server System (SUSE Linux-distributed) and High Availability System (SUSE Linux-distributed): # **cd /var/log**
     - In the Single-Server System (Solaris) and High Availability System: # **cd /var/adm**
  4. Run the following command to view the log file of the operating system (the file name is started with **messages**):

     # **more messages***

----End

Reference Standard

- In the Windows system:

  The **Error** information is not displayed in **Event Viewer**.

- In the Single-Server System (SUSE Linux-distributed), Single-Server System (Solaris) and High Availability System:

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

  TIP

  Run the following command to quickly search the error information:

  # **grep error messages***

  If there is no error information, no information is displayed after the command is run.

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

Troubleshooting

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

5.4 Checking the Logs of the SQL Server Database

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

Procedure

Check the log files in the *SQL Server installation directory* **\MSSQL\LOG**.

Reference Standard

No error information appears in all of the files in the **\MSSQL\LOG** path.

Troubleshooting

Fix the system according to the errors in the log files. If the problem still persists, contact technical support engineers of Huawei for troubleshooting.

5.5 Checking the Logs of the Sybase Database

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

Procedure

1. Log in to the OS as user **nmsuser**.
2. Open a terminal window, and run the following commands to switch to user **root**:

   $ **su**

   `Password:` *password_of_user_root*
3. Run the following command to switch to the directory of the log files:

   # **cd /opt/sybase/ASE-15_0/install**

   NOTE

   The following uses Sybase 15.0 as an example.

4 Run the following commands to view the log files of the database:

more DBSVR.log

more DBSVR_back.log

----End

Reference Standard

No error information appears in the file.

TIP

Run the following command to quickly search the error information:

grep error DBSVR.log

grep error DBSVR_back.log

If there is no error information, no information is displayed after the command is run.

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

Troubleshooting

Fix the system according to the errors in the log files. If the problem still persists, contact technical support engineers of Huawei for troubleshooting.

5.6 Checking the Logs of the Oracle Database

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

Procedure

Check the log file *alert_U2KDB.log* in the **/opt/oracle/diag/rdbms/u2kdb/U2KDB/trace/**.

Reference Standard

No ORA-* information appears in the file.

Troubleshooting

Fix the system according to the errors in the log files. If the problem still persists, contact technical support engineers of Huawei for troubleshooting.

5.7 Checking the Running Status of the Anti-Virus Software

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

Procedure

Install the patches of the OS in time, search for viruses, and upgrade the anti-virus software regularly.

Reference Standard

No virus is found.

Troubleshooting

If any virus is found, clear it at once. If the troubleshooting fails, reinstall the OS.

5.8 Checking the Database Status

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

Context

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

Procedure

1. Log in to the U2000 System Monitor client.
2. Click the **Database Monitor** tab and the details of all the manageable databases are displayed in a list.
3. Select one database in the list, right-click, and choose **Refresh** from the shortcut menu to refresh all the information about the selected databases.

----End

Reference Standard

The databases run normally. For each database, the ratio of the used data space to the total data space is less than 85%.

Troubleshooting

If the log space of a database exceeds the standard value, dump the logs and clear the space in time. For details, refer to the related contents in chapter **Backing Up and Restoring the U2000 Database** of the administrator guide.

6 Monthly Maintenance

About This Chapter

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

6.1 Checking the User Configuration

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

Procedure

1. Log in to the U2000 as user **admin**.
2. Choose **Administration** > **NMS Security** > **NMS User Management** from the main menu.
3. In the **NMS User Management** window, choose **Users** from the navigation tree and then select a user node under the **Users** node to view the user attributes in the right pane.

----End

Reference Standard

No irrelevant user exists. The operation rights are set properly, and the password valid period is set.

Troubleshooting

- Assign user rights strictly according to the user group and operation set. Divide users with the same rights to a group, and avoid assigning rights to a single user. This reduces impact on the U2000 performance.
- Delete users who no longer use the device in time. Assign rights to users for maintaining a new device.
- Change the password at least quarterly.

6.2 Backing Up System Files

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

Procedure

- Do as follows in the Single-Server System (Windows) and High Availability System (Windows):
  1. Log in to the Windows OS as a user with the administrator rights.
  2. Back up the entire U2000 program directory, such as **D:\U2000** and **C:\HWENGR**.
  3. Back up the entire SQL Server database program directory, including the database running files in the SQL Server 2000 installation directory and the sqlserver dynamic link library (DLL) files in the **C:\WINDOWS\system32** directory.
  4. Back up the registry files.

     Choose **Start** > **Run** and enter **regedit**. In the window that is displayed, choose **File** > **Export**.
- Do as follows in the Single-Server System (Solaris) and High Availability System (Solaris):

1. Log in to the operating system as user **nmsuser**.
2. Open a terminal window, and run the following commands to switch to user **root**:

   > **su**

   `Password:` *password_of_user_root*
3. Run the following command to compress the system files, and then manually copy the system files to the specific storage device for backup:

   tar cvf *backup1.tar* **/opt/HWENGR**

   tar cvf *backup2.tar* **/opt/U2000**

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

   NOTE

   Here, *backup1.tar*, *backup2.tar* and *backup3.tar* are the names of compressed files. You can modify the names as required.

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

  1. Log in to the operating system as user **nmsuser**.
  2. Open a terminal window, and run the following commands to switch to user **root**:

     > **su**

     `Password:` *password_of_user_root*
  3. Run the following command to compress the system files, and then manually copy the system files to the specific storage device for backup:

     tar cvf *backup1.tar* **/opt/HWENGR**

     tar cvf *backup2.tar* **/opt/U2000**

     tar cvf *backup3.tar* **/opt/oracle**

     NOTE

     Here, *backup1.tar*, *backup2.tar* and *backup3.tar* are the names of compressed files. You can modify the names as required.

----End

6.3 Viewing the Statistics of Alarms

This describes how to collect and view the statistics of monthly alarms.

Procedure

1 Log in to the U2000 client.

2 Choose **Fault** > **Query Alarm Log Statistics** from the main menu.

3 In the **Statistic Filter** dialog box, set **Statistic Row** to **By month**. In the **Basic Setting** dialog box, select the **Occurrence Time Range** of alarms, and click **OK**.

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

4 According to the buttons at the bottom of the **Query Alarm Log Statistics** window, you can perform the following operations:

- Click **Template** to create, open, or save an alarm statistical template.

- Click **Statistic Filter** to set the statistical condition.
- Click **Refresh** to collect statistics on alarms again based on the current statistical condition.
- Click **Save As** to save the statistical result as a file.
- Click **Print** to print the statistical result in a specified medium.

----End

6.4 Checking the Server Time of the U2000

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

Procedure

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

     $ **su**

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

     # **date**

----End

Reference Standard

The server time is correct.

Troubleshooting

Check the running status of the NTP service. If the NTP service is abnormal, reconfigure the NTP service. For details, refer to the chapter **Configuring System NTP Solutions** of the commissioning guide.

6.5 Changing the Password of the Current User

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

Context

The new password must comply with the password policy.

Procedure

1. Choose **File** > **Change Password** from the main menu.
2. In the **Change Password** dialog box, set the new password for the current user.
3. Click **OK**.
4. In the dialog box, click **OK**.

----End

6.6 Releasing the Disk Space of the U2000 Server

This section describes how to clear the disk space. You need to clear the disk space to save resources.

Prerequisite

CAUTION

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

Procedure

- Do as follows in the Windows system:
  1. Log in to the Windows OS as a user with the administrator rights.
  2. Delete the useless and outdated alarm log files that are automatically dumped. The default directory is **installation path of the NMS\server\dump**

     NOTE

     You can compare the creation time and the modification time of a file with the current system time. If a file was created a long time ago and has not been used for a long time, it can be concluded that the file is outdated.
  3. Delete the useless and outdated abnormal event log files that are automatically dumped. The default directory is **installation path of the NMS\server\dump**.
  4. Delete the useless and outdated database backup files. The default directory is **installation path of the NMS\server\var\backup**.
  5. Delete the outdated and useless running log files. The default directory is **installation path of the NMS\server\log**.
  6. Delete other outdated and unnecessary files, such as the program installation files and patch installation files of earlier versions.
- Do as follows in the Single-Server System (SUSE Linux-distributed), Single-Server System (Solaris) and High Availability System:
  1. Log in to the OS as user **root**.
  2. Delete the useless and outdated alarm log files that are automatically dumped. The default directory is **installation path of the NMS/server/dump**.

3. Delete the useless and outdated abnormal event log files that are automatically dumped. The default directory is **installation path of the NMS/server/dump**.
4. Delete the useless and outdated database backup files. The default directory is **installation path of the NMS/server/var/backup**.
5. Delete the outdated and unnecessary running log files. The default directory is **installation path of the NMS/server/log**.
6. Delete other outdated and unnecessary files, such as the application installation files and patch installation files of earlier versions.

----End

7 Quarterly Maintenance

About This Chapter

This topic describes how to perform quarterly maintenance. Through quarterly maintenance, you can keep the equipment room environment of the U2000 in good condition to ensure the reliability of power supply and related hardware.

7.1 Checking the Equipment Room Environment

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

Procedure

1. Check the temperature, humidity, and dust-proof conditions of the equipment room.
2. Check the power supply system, air filter, fire alarm system, and lightning proof system.

----End

Reference Standard

Item	Index
Temperature	Range: 15°C-35°C
Humidity	Range: 30%-60%
Dust condition	Clear and spotless
Power supply	The power supply is normal, which ensures the normal running of the equipment in the equipment room.
Air filter	The air filter is clean and the cabinet is in good ventilation condition.
Fire alarm system	The fire alarm system works normally and can effectively sense the fire accident.
Lightning proof system	The lightning proof system works normally and can effectively prevent the lightning stroke.

Troubleshooting

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

7.2 Checking the Power Supply of the U2000 Server

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

Prerequisite

The U2000 server is powered on.

Procedure

1. View whether the power indicators of the server and monitor are normal.
2. If the server is configured with devices such as the disk array and storage device, view the power indicators of these devices.
3. Do as follows to view the information about the power supply faults in the logs recorded in recent days:
   - In the SUSE Linux OS:

     # **more** */var/log/messages*

     # **more** */var/log/warn*
   - In the Solaris OS:

     # **more** */var/adm/messages*

   Information similar to the following is displayed: If error or WARN is displayed, it indicates that the power supply is faulty.

   ```
   Jun 23 16:53:40 U2000Server rmclomv: [ID 632913 kern.error] Input power unavailable
   for PSU @ PS1.
   ```
4. Check the faults of the external power of the system.
5. Confirm that the power supply of the server is normal.

----End

Reference Standard

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

Troubleshooting

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

7.3 Checking the Hardware and Peripherals of the U2000 Server

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

Prerequisite

The U2000 server is powered on.

Procedure

1. Refer to the delivery manual of the server according to the server type to check the hardware of the server.

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

3 Check whether the CD/DVD-ROM runs normally.

----End

Reference Standard

In normal cases, the server and peripherals run normally and all indicators work normally.

Troubleshooting

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

A Abbreviations

C

CD-ROM	Compact Disc Read-Only Memory
CORBA	Common Object Request Broker Architecture
CPU	Central Processing Unit

D

DC	Data Center
DVD-ROM	Digital Video Disk Read-Only Memory

E

ECC	Embedded Control Channel

F

FTP	File Transfer Protocol

I

ID	Identity
IP	Internet Protocol

L

LOG	Call Logging

N

NE	Network Element
NMS	Network Management System
NTP	Network Time Protocol
R	
RVG	Replicated Volume Group
S	
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
T	
TFTP	Trivial File Transfer Protocol
U	
UPS	Uninterrupted Power Supply
V	
VCS	VERITAS Cluster Server
VVR	VERITAS Volume Replicator
VxVM	VERITAS Volume Manager